

**Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
January 4, 2016 / le 4 janvier 2016**

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse quotidienne peut également être accédée via [InfoMédia](#)

MINISTER / MINISTRE

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

OPERATION SYRIAN REFUGEES / OPÉRATION RÉFUGIÉS SYRIENS

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRE

INTERNATIONAL

MINISTER / MINISTRE

Public safety minister investigating case of 6-year-old on travel security list

The federal **public safety minister** says he'll investigate the case of a six-year-old Ontario boy whose name appears to be on a travel security risk list. **Ralph Goodale's** involvement in the matter comes after the boy's father tweeted a photo from Toronto's Pearson International Airport last week that appears to show his son's name, Syed Adam Ahmed, with a "DHP" or "deemed high profile" label and instructions on how to proceed before allowing the boy to check in. The father wrote: "Why is our (Canadian born) 6 year old on DHP no fly list? He must clear security each time. He is 6." His question was directed at Air Canada, the airline father and son were flying on Dec. 31 for their trip to the NHL Winter Classic in Boston. The boy's mother, Khadija Cajee, said the family has had to deal with the issue in the past. She says they've never been able to check their son in for flights online, and he needs special clearance every time they go to the airport. The boy and his father were both born in Canada, and Cajee's family came to the country from South Africa, fleeing apartheid, she said. Cajee doesn't know why her son is on the list, but she assumes he shares a name with someone who actually earned a place on it. [Canadian Press](#) (Cape Breton Post, The Telegram, The Guardian, Truro Daily News, Western Star, Prince Albert Daily Herald, Brandon Sun, Chronicle Journal), [CBC News](#), [CJAD 800 News](#), * [620 CKRM](#), * [Huffington Post](#)

Globe-trotting Mountie

An open letter to the **Minister of Public Safety** states, "Mr. (**Ralph**) **Goodale**, as a taxpayer of Canada, I demand this lunacy stop. As minister in charge of the RCMP, you have the ultimate responsibility to

compromise liberty. [Postmedia News](#) (Montreal Gazette, C1/Front, Ottawa Citizen, StarPhoenix, Edmonton Journal, Leader-Post)

* **Liberals will face tough choices on tech issues**

As Canada enters a new year with a new government, 2016 will be all about making tough choices on a wide range of technology law policies, including these eight issues that are sure to generate headlines.

1. How will Bill C-51 be revamped? Bill C-51, the Conservative government's anti-terrorism bill, emerged as a major political issue last year as many expressed concern over the lack of oversight and the implications for privacy and civil liberties. The Liberal government has committed to reforms, but has been generally coy about what those changes will be. New accountability mechanisms will undoubtedly feature prominently in any reform package, but the substantive amendments to the bill remain a mystery. 2. What to do about lawful access? The decade-long debate over lawful access, which establishes the rules under which law enforcement can access subscriber information, concluded last year with the passage of Bill C-13. The Privacy Commissioner of Canada remains critical of the legislation and the Supreme Court of Canada has ruled that subscribers have a reasonable expectation of privacy in that information. With law enforcement seeking new warrants to access subscriber data, the Liberals face tough policy choices in striking the privacy-security balance. [Toronto Star](#), S10

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

U.S. sees many benefits from free trade

One benefit of free trade is that it allows the United States to generate substantial economic gain from countries far smaller than our own. That lesson is lost on those who promote protectionism and trade wars, which unfortunately has started to include some Republicans. John Manzella, a noted author on global business, highlighted trade's benefits in a recent article reviewing the impact of the North American Free Trade Agreement, which has been in place for more than two decades now (...) Manzella noted \$658 billion worth of goods crossed the U.S.-Canada border last year (not including trade in services), making Canada the United States' largest trading partner despite having a population of just 35 million. Thus Canada, with only about 11 percent of the U.S. population, still accounts for 16.6 percent of all U.S. trade. [The Oklahoman](#)

US repeals meat labeling law after trade rulings against it

It's now harder to find out where your beef or pork was born, raised and slaughtered. After more than a decade of wrangling, Congress repealed a labeling law last month that required retailers to include the animal's country of origin on packages of red meat. It's a major victory for the meat industry, which had fought the law in Congress and the courts since the early 2000s. "U.S. exporters can now breathe a sigh of relief," said Republican Sen. Pat Roberts of Kansas, chairman of the Senate Agriculture, Nutrition and Forestry Committee. The longtime opponent of the labels helped add the repeal to a massive year-end spending bill. After the law was passed, Agriculture Secretary Tom Vilsack said the government immediately would stop requiring the labels. [Winnipeg Free Press](#) (2016-01-03)

* **DHS to Expand Drone Testing to Improve Border Protection**

Department of Homeland Security researchers are spearheading a push to better protect the nation's coasts and borders by consolidating research efforts and standardizing unmanned operations between two of its agencies. Threats from technologically adept "bad guys" and the challenges posed by very small aircraft like the gyrocopter protester Doug Hughes landed on the White House lawn and a quadcopter that crashed there just months earlier, are consuming greater attention at DHS, said Timothy Bennett, a program manager in the department's Science and Technology Directorate (S&T). "There's been a big push to increase our capabilities and our understanding of UAS systems," said Bennett. As a result, he said, DHS will combine two key testing programs and work to standardize and integrate the unmanned operations of Customs and Border Patrol (CBP) and the Coast Guard. S&T plans to combine and expand its successful Robotic Aircraft for Public Safety (RAPS) and the Robotic Aircraft for Maritime Public Safety (RAMPS) programs. [Inside Unmanned Systems](#)

* **Thousand Islands tourism survey: low Canadian exchange rate dampened business**

Today's News / Actualités
January 5, 2016 / le 5 janvier 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via [InfoMédia](#)

MINISTER / MINISTRE

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / CYBERSÉCURITÉ

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

OPERATION SYRIAN REFUGEES / OPÉRATION RÉFUGIÉS SYRIENS

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

Father of Canadian six-year-old on no-fly list: our family is not alone

The father of a Canadian six-year-old who was flagged as a potential travel threat says he has heard from at least a dozen other families struggling with the same issue. Syed Adam Ahmed's case drew national media attention after his father, Sulemaan Ahmed, tweeted to Air Canada on New Year's Eve, asking: "Why is our (Canadian born) 6 year old on DHP no fly list? He must clear security each time." The tweet, from the Toronto Pearson international airport, included a picture of the computer screen showing that his son had been given the "Deemed High Profile" designation (...). The Liberal government has committed to reviewing the issues related to the no-fly list – officially called the Passenger Protect Program – which was recently beefed up under controversial new anti-terrorism legislation passed last summer by the Conservative government of Stephen Harper. The Liberals have pledged to review and repeal problematic elements of that legislation. ***"That work is ongoing, and will include a public consultation process,"*** Goodale said in his statement. [Guardian UK](#)

Why your kid's name could put them on an airline security watchlist

improperly store secret files. A search warrant filed in provincial court alleges the actions of a man identified only as "Mr. Zawidski" violated a section of the federal Security Information Act that deals with wrongful communication of information. None of the allegations has been proven in court and Newton said he has received no indication that charges have been laid. [Hamilton Spectator](#)

Tech Law in 2016: Previewing Some of the Tough Policy Choices

An opinion piece by Michael Geist states "Technology law and policy continues to command the attention of the public and policy makers. My weekly technology law column (Toronto Star version, homepage version) notes that as Canada enters a new year with a new government, 2016 will be all about making tough choices on a wide range of technology law policies, including the following eight issues that are sure to generate headlines. 1. How will Bill C-51 be revamped? Bill C-51, the Conservative government's anti-terrorism bill, emerged as a major political issue last year as many expressed concern over the lack of oversight and the implications for privacy and civil liberties. The Liberal government has committed to reforms, but has been generally coy about what those changes will be. New accountability mechanisms will undoubtedly feature prominently in any reform package, but the substantive amendments to the bill remain a mystery. 2. What to do about lawful access? The decade-long debate over lawful access, which establishes the rules under which law enforcement can access subscriber information, concluded last year with the passage of Bill C-13. [michaelgeist.ca](#), [The Tyee](#)

Hugh Segal: If 'Canada's back,' we'll need a military

An opinion piece states "Whatever the trajectory, priorities or intensity of our new government's foreign policy, however the election of Oct. 19 is interpreted as a mandate for foreign policy change, no meaningful Canadian foreign policy can exist without a competent, well-resourced and multi-skilled armed forces. This is not about an obscure dialectic between those who prefer peacekeeping versus those who support combat capacity. Both preferences require a strong and capable armed forces... To the new government's credit, it has a rooted, practical and highly skilled brain trust in place to serve both the Prime Minister and the national interest. There's the new defence minister, who has outstanding battle theatre command credentials from several tours of duty in Afghanistan and as a commander of a reserve regiment. The Chief of Defence Staff has been in serious and complex operational command roles globally. The Chief Government Whip is a retired general staff officer who served in the field. The senior National Security Advisor to the Prime Minister is a former head of CSIS and deputy defence minister. Likewise, the Foreign Affairs minister has the legitimacy of long parliamentary service and the analytical mindset of a distinguished academic before entering public life. Like any compelling mix of outstanding assets, they prove nothing by their mere existence. How they combine to shape policy and priorities with the Prime Minister and cabinet is what will determine their success and impact. Still, with such qualified individuals in government, there is reason for optimism." [National Post](#)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Prince George baker Karl Haus sentenced for 'obsessive' gun collecting - Karl Haus is better known as the owner of Prince George's oldest bakery, the Pastry Chef

A Prince George baker known for his delicious flax buns and fresh loaves of rye was sentenced earlier this week after RCMP seized "an arsenal" of illegal weapons and ammunition from his home. Karl Haus is better known as the owner of Prince George's oldest bakery, the Pastry Chef, a downtown institution since 1955 that sells German pastries and breads. But Haus made headlines back in November 2013, after border officers at the International Mail Processing Centre in Toronto intercepted a suspicious package from Germany. The package turned out to contain prohibited weapons parts, so the Canada Border Services Agency (CBSA) brought in the RCMP and a joint investigative team was formed. When RCMP officers arrived to search Haus's Prince George home they uncovered 31,000 rounds of ammunition, several prohibited automatic weapons including a fully automatic M16 and a fully automatic AK 47, three hand guns, two of which were loaded, seven rifles, two morning stars, two shotguns, five 100-round capacity drum magazines, 50 assault rifle magazines, and four bulletproof vests. [CBC News](#)

Federal Court opens door for former KGB employee to rejoin family in Canada

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Thursday, January 07, 2016 6:00 PM
To: Today's News / Actualités (PS/SP)
Subject: (AMENDED) RT: CTV News - Power Play - Privacy Commissioner Daniel Therrien on CBSA's new passenger vetting system & potential privacy concerns - 17h20 ET - 2016-01-07

Categories: Red Category

Rough Transcript

Station: CTV News - Power Play
Time/Heure: 17h20 ET
Date: 2016-01-07

Summary: *CTV News' Power Play interviewed Privacy Commissioner Daniel Therrien on CBSA's new airline passenger vetting system and potential privacy implications.*

>> On: Welcome back. Fresh concerns that beefed-up surveillance of incoming air passengers could be used for racial profiling, to explain his concerns, we're joined by Canada's privacy commissioner, Daniel Therrien. Welcome to the show. Happy new year.

>> Thank you.

>> Don: What's caught your attention on this new vetting system of air travelers?

>> We're not saying of course, we're not saying that the border services agency is wrong to collect information about passengers. What caught our eye for some time is under an agreement with the United States, the border accord with the United States, Canada has undertaken to harmonize its screening rules. For passengers. And rather than to screen individuals bad on their own individual characteristics, to screen them based on scenarios or criteria and we don't know what the criteria are exactly] So we're not saying that there is discrimination, but we have asked the border services agency to let us know what the criteria are so that we can determine whether they are objective, whether they can lead to discrimination or other human rights violations. At this point, we say that this new system may create a risk. We're not saying there is discrimination. We would like evidence and what we're frankly concerned about quite a bit is that it's Ben about two years since this program has been in place and we have not still reived information about what the scenarios are.

>> Don: So help me understand what a scenario would be. Would a scenario be, sa na [unintelligible] [unintelligible] traveler coming into Canada had a history of visiting, say, Middle East countries, would that kind of scenario trigger something in Canada?

>> It might be but we haven't en them but it certainly would be logical to think that this might be a scenario that border services agency would look at. What's important to say as well is that this method is not used only for terrorism screening purposes but for criminality purposes so among the criteria or the scenario might be people who visit areas where drugs are manufactured, trafficked, et cetera.

>> Don: You're travelling in from the regions. Don't you have an expectation you're going to be red flagged because of what you have done and under those existing scenarios? I know you're saying you don't know what they are and that's what you want clarity on. But people must know that those scenarios would trigger things.

>> What we're saying is that of course it's legitimate for the government to screen people based on threat assessment. What we're saying is that these threat assessments cannot hinge only on criteria like nationality, country of embarkation, age, et cetera. It's absolutely

reasonable for the STE [unintelligible] to screen travelers but based on a matrix of factors which is not only nationality and age.

>> Don: Okay. What else beyond getting clarity on what scenarios you're looking at would you like to see addressed before you give this one your stamp of approval?

>> What's interesting as I was saying this new approach has been adopted following an agreement with the United States. On the American side, there is a review of the application of this approach, every quarter, so four times a year, by experts to determine that the scenarios in question, the criteria in question do not lead to human rights abuse, civil liberties abuse, et cetera interestingly enough, that kind of process is not occurring in Canada. The border services agency has told U th they intend to have a similar process. I think it would be a very good idea for them to undertake that.

>> Don: Have your U.S. counterparts seen the U.S. System does induce racial profiling, have they flagged that concern and as a result of that review, has that been verified?

>> I am not aware of at [unintelligible], no, such a finding has been made in the United States.

>> Don: I do want to get your thoughts quickly on the year ahead. Privacy issues continue to dominate, our privacy continues to erode. Where you see the flashpoivts [unintelligible] coming in 2016?

>> Well, I think there will continue to be issues around security, criminality, and privacy. So lawful access may be a theme, obviously the government has announced that it wants to introduce legislation to amend bill c-51 which was adopted last year. So the balance between security and privacy will absolutely continue to be a theme. On the private sector side, of course, there are many issues that will occur. The use of big data, whether or not consumers are able to consent to the uses that companies make of their information. So we intend to actually do quite a bit of work on that theme of the use of personal information by the private sector to ensure that privacy is respected. So on both fronts, the government front, the private sector front, we expect to be very busy this year.

>> Don: Yes, I imagine you have. Do they come to you and say we want to start bulletproofing this thing on privacy concerns, but I'm talking about bill C-51. Have you heard from them at all?

>> No, I have of course read about the commitments of the government to introduce legislation, but I have not been approached directly, no.

>> Don: We'll see if they do. All right, commissioner, thanks for coming in. Appreciate it.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Questions? Please contact us at PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Questions? Veuillez communiquer avec nous au PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Question Period Note / Note pour la Période des questions

Warrantless Access to Basic Subscriber Information

ISSUE: On November 25, 2015, at the Securetech conference in Ottawa, RCMP Commissioner Bob Paulson indicated that police need warrantless access to subscriber information to keep pace with online criminals.

PROPOSED RESPONSE:

- **Cyberspace provides tremendous benefits to Canadian's quality of life and to our national prosperity, but it also poses serious threats.**
- **Canadians are embracing the many advantages that the Internet offers, but along with this increased reliance on technologies comes vulnerability from cyber threats and cybercrime.**
- **Perhaps this is most evident in our efforts to combat child sexual exploitation over the internet, where perpetrators can exist in anonymity and timely access to evidence is crucial.**
- **The Government of Canada is committed to defending Canada's cyber security and protecting and advancing our national security and economic interests and to strengthen Canada's capacity to protect Canadians – individuals, industry and governments.**
- **The Government of Canada acknowledges the challenges currently being faced by law enforcement and national security agencies and is committed to working with them and other stakeholders to come up with appropriate solutions to ensure that they have the tools they need to conduct effective investigations and keep Canadians safe.**
- **Central to this work is the consideration of both keeping Canada safe and the personal privacy of Canadians.**

Warrantless Access to Basic Subscriber Information

BACKGROUND:

Canadians are increasingly using mobile phone networks, the internet, and other electronic means to communicate and execute transactions with each other. This has led to a significant gap between the technologies available for criminal exploitation and our means to enforce Canada's laws and keep Canadians safe.

Recently, the *Spencer* decision has impacted government and law enforcement's ability to initiate investigations. On June 13, 2014, the Supreme Court of Canada released its unanimous decision in *R. v. Spencer* dismissing the appeal and confirming the conviction of possession of child pornography. The Court disagreed with the trial judge and Saskatchewan Court of Appeal, both of which found that police obtaining basic subscriber information (BSI) did not breach Mr. Spencer's s. 8 *Charter* rights. The Court found that the police request for BSI in this case breached Mr. Spencer's s. 8 *Charter* rights; however, under s. 24 (2), the Court held that despite the breach, the evidence should be admissible and therefore upheld the conviction. The Court also upheld the Saskatchewan Court of Appeal's order of a new trial given the trial judge's error in interpreting the offence of making available child pornography under subsection 163.1 (3) of the *Criminal Code*. In its decision, the Court stated that where BSI can reveal a person's "personal choices or lifestyles," which may be compared to the "biographical core information" protected under s. 8 of the *Charter*, a reasonable law, warrant, or exigent circumstances are required for that information to be obtained lawfully. While concluding that the search was in violation of the *Charter*, the Court stated that nothing in the decision diminished the existing powers of the police to obtain BSI without a warrant in exigent circumstances, and that this information could also be provided pursuant to a reasonable law. Further, the Court confirmed the existing common law powers of police to make enquiries relating to matters that are not subject to a reasonable expectation of privacy. This decision came amid public concern that authorities were quietly gaining access to customer data with little oversight or independent scrutiny.

Until June 2014, Government and law enforcement agencies most frequently acquired BSI by requesting communications service providers to release BSI voluntarily under the *Personal Information Protection and Electronic Document Act (PIPEDA)* or by compelling the communications service providers to provide this information in the context of ongoing investigations pursuant to a court order. Basic Subscriber Information typically includes information such as an individual's name, address, telephone number, similar to in a phonebook, but may also include the individual's email address, IP address and/or local service provider identifier. With the latter of the identifiers being elements that have the potential to be used to develop more detailed portraits of individuals.

Most communications service providers and some other private businesses (e.g., banks and rental agencies) have interpreted the *Spencer* decision cautiously and broadly, and have ceased voluntarily providing any BSI.

As a result, Government and law enforcement agencies must now seek warrants (e.g., production orders) to obtain BSI, which has added a heavy administrative and financial burden to investigations and created challenges, including long delays or not pursuing the case at all, in some investigations where a warrant is required to obtain the information, but that same information is required to obtain the warrant.

Law enforcement agencies also continue to be confronted with the need for timely access to information to address child exploitation over the internet, including the identification of perpetrators over the internet. The securing of evidence required to combat these crimes has become more difficult and time consuming post-*Spencer*, and data retention times for internet service providers can be as little as seven days.

Currently, the Government is exploring options to address the *Spencer* decision to ensure that law enforcement and national security agencies have the tools they need to conduct effective investigations and to keep Canadians safe. The balance between both Canada's security and privacy for all Canadians will be a crucial factor as this work moves forward.

It is important to note that on December 2, 2015, the RCMP released their Cybercrime Strategy. The strategy builds on the findings of a report published by the RCMP in 2014, titled "Cybercrime: an overview of incidents and issues in Canada". The vision of the strategy is to reduce the threat, victimization and impact of cybercrime in Canada. It sets out an operational framework and an action plan to help the RCMP combat cybercrime.

CONTACTS:

Prepared by
[Redacted]

Tel. no.
[Redacted] (W)
[Redacted] (C)

Approved by
Monik Beauregard
SADM

Tel. no.
613-990-4976

Accès à l'information sans mandat abonné de base

SUJET : Le 25 novembre, 2015, à la conférence Securetech tenue à Ottawa, Le Commissaire de la GRC Bob Paulson a indiqué que la police a besoin d'accéder aux informations des abonnés sans avoir recours à un mandat et ce, afin de se maintenir au même niveau que les cybercriminels.

RÉPONSE SUGGÉRÉE :

- **Le cyberspace améliore grandement la qualité de vie des Canadiens et des Canadiennes et contribue à la prospérité nationale, mais il pose également de sérieuses menaces.**
- **Les Canadiens et les Canadiennes exploitent les nombreux avantages qu'offre Internet, mais ce recours accru aux technologies est accompagné d'une vulnérabilité aux cybermenaces et à la cybercriminalité.**
- **Cela est probablement le plus évident dans nos efforts de lutter contre l'exploitation sexuelle des enfants sur Internet. L'anonymat des auteurs de ce crime est assuré et l'accès en temps opportun aux éléments de preuve est essentiel.**
- **Le gouvernement du Canada est résolu à assurer la cybersécurité et à préserver et à renforcer la sécurité nationale et les intérêts économiques du pays ainsi qu'à renforcer la capacité du Canada à protéger les Canadiens et les Canadiennes, notamment les particuliers, l'industrie et le gouvernement.**
- **Le gouvernement du Canada est conscient des difficultés auxquelles sont confrontés les organismes d'exécution de la loi et les organismes de sécurité nationale et il est déterminé à collaborer avec eux et d'autres intervenants en vue de trouver des solutions appropriées pour veiller à ce qu'ils aient les outils qu'ils ont besoin pour mener des enquêtes efficaces et assurer la sécurité des Canadiens.**
- **La sécurité des Canadiens et la protection des renseignements personnels des Canadiens sont au cœur de ces travaux.**

Accès à l'information sans mandat abonné de base

CONTEXTE :

Les Canadiens utilisent de plus en plus les réseaux de téléphonie mobile, l'Internet et d'autres moyens électroniques pour communiquer et effectuer des transactions entre eux. Cela a mené à un important écart entre les technologies pouvant servir à des fins criminelles et les moyens dont nous disposons pour appliquer les lois du Canada et assurer la sécurité des Canadiens.

Récemment, la décision *Spencer* a eu des répercussions sur la capacité du gouvernement et des organismes d'application de la loi d'ouvrir des enquêtes. Le 13 juin 2014, la Cour suprême du Canada a rendu une décision unanime l'affaire *R. c. Spencer* dans laquelle elle a rejeté l'appel et elle a confirmé la condamnation pour possession de pornographie juvénile. La Cour n'était pas d'accord avec les conclusions du juge de première instance et la Cour d'appel de la Saskatchewan, qui avaient toutes les deux conclu que l'obtention par les policiers des renseignements de base sur les abonnés ne violait pas les droits de M. Spencer garantis à l'article 8 de la *Charte*. La Cour a conclu que, dans ce cas, la demande de policiers visant à obtenir des renseignements de base sur les abonnés violait les droits de M. Spencer garantis à l'article 8 de la *Charte*. Toutefois, en vertu du paragraphe 24(2), la Cour a statué que, malgré cette violation, les preuves devaient être admissibles et par conséquent elle a confirmé la condamnation. La Cour a aussi confirmé l'ordonnance de la Cour d'appel de la Saskatchewan de tenir un nouveau procès puisque le juge de première instance avait mal interprété l'infraction de distribution de pornographie juvénile aux termes du paragraphe 163.1 (3) du *Code criminel*. Dans sa décision, la Cour a indiqué que lorsque les renseignements de base sur les abonnés peuvent révéler les choix personnels ou le mode de vie d'une personne, ce qui peut être comparable aux renseignements biographiques de base protégés en vertu de l'article 8 de la *Charte*, une loi raisonnable, un mandat ou des circonstances contraignantes étaient nécessaires afin que cette information soit obtenue en toute légalité. Bien qu'elle ait conclu que la perquisition contrevient à la *Charte*, la Cour a affirmé qu'aucun élément de la décision ne portait sur les pouvoirs dont disposent les policiers pour obtenir sans mandat des renseignements de base sur les abonnés dans des circonstances contraignantes, et que cette information pourrait aussi être communiquée en vertu d'une loi raisonnable. De plus, la Cour a confirmé les pouvoirs actuels des policiers en common law de présenter des demandes au sujet d'affaires qui ne font pas l'objet d'une attente raisonnable en matière de vie privée. Cette décision a été rendue alors que dans l'opinion publique on s'inquiétait que les autorités obtiennent discrètement l'accès aux données des consommateurs, et ce avec peu de surveillance ou d'examen indépendant.

Jusqu'en juin 2014, le gouvernement et les organismes d'application de la loi obtenaient plus fréquemment les renseignements de base sur les abonnés en demandant aux fournisseurs de services de communications de communiquer volontairement cette information en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)* ou en incitant les fournisseurs de services de communication à fournir cette information dans le cadre d'enquêtes conformément à l'ordonnance d'un tribunal. En règle générale, les renseignements de base sur les abonnés incluent de l'information telle que le nom, l'adresse et le numéro de téléphone d'une personne, comme dans un bottin téléphonique, mais ils peuvent aussi inclure l'adresse courriel, l'adresse IP ou l'identificateur du fournisseur de services locaux de la personne. Ce dernier est un élément pouvant servir à obtenir un portrait plus détaillé de la personne.

La plupart des fournisseurs de services de communication et certaines autres entreprises privées (p. ex. banques et entreprises de location) ont interprété avec prudence et de manière assez large la décision *Spencer*, et ils ont cessé de fournir volontairement des renseignements de base sur les abonnés.

Par conséquent, le gouvernement et les organismes d'application de la loi doivent maintenant demander des mandats (p. ex. ordonnance de communication) pour obtenir des renseignements de base sur les abonnés, ce qui a ajouté un lourd fardeau administratif et financier aux enquêtes et créé des problèmes, notamment de longs délais ou l'abandon du cas, dans certaines enquêtes où un mandat est requis pour obtenir l'information, alors que la même information est nécessaire pour obtenir le mandat.

Les organismes d'application de la loi continuent aussi d'être confrontés au besoin d'avoir accès en temps opportun aux renseignements pour contrer l'exploitation d'enfants sur Internet, notamment à l'identification des auteurs de crimes sur Internet. L'obtention des preuves requises pour lutter contre ces crimes est devenue plus difficile et exige plus de temps depuis la décision *Spencer*, et la durée de conservation des données chez les fournisseurs de services Internet peut être aussi peu que sept jours.

À l'heure actuelle, le gouvernement étudie des options pour donner suite à la décision *Spencer* afin de veiller à ce que les organismes d'application de la loi et de sécurité nationale aient les outils dont ils ont besoin pour mener des enquêtes efficaces et assurer la sécurité des Canadiens. L'obtention d'un juste équilibre entre la sécurité du Canada et le respect de la vie privée pour tous les Canadiens sera un élément essentiel au fur et à mesure que ces travaux progresseront.

| | | | |
|--|--|---|----------------------------|
| CONTACTS : Préparé par : [Redacted] | Tel. no. [Redacted] (W) [Redacted] (C) | Approuvée par Monik Beauregard SADM | N° de tél. 613-990-4976 |
|--|--|---|----------------------------|

Today's News / Actualités
April 18, 2016 / le 18 avril 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS |
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

La majorité des ministres sont unilingues sur Twitter

La grande majorité des ministres libéraux ne respectent pas l'obligation de gazouiller dans les deux langues officielles, déplore l'impératif français. Selon une recherche menée par l'organisme, 23 des 31 ministres du cabinet Trudeau ne respectent pas la Loi sur les langues officielles sur leur compte Twitter. M. Perreault a rappelé qu'en février 2015, l'opposition libérale avait fait grand cas des rapports d'enquêtes préliminaires du commissaire aux langues officielles, Graham Fraser, qui rappelait que les ministres avaient l'obligation de communiquer avec le public en français, y compris par voie électronique, lorsqu'ils le font à titre de chef de leur ministère ou de représentant du gouvernement. L'ancien ministre conservateur John Baird avait d'ailleurs été un des ministres réprimandés par le commissaire Fraser, parce qu'il gazouillait trop souvent en anglais. Stéphane Dion, alors porte-parole libéral pour les langues officielles, avait fait parvenir une lettre au président du Conseil du Trésor de l'époque, Tony Clement,

RCMP misconduct cases jump 158% in single year

The number of misconduct investigations the RCMP launched into their own staff went up by 158 per cent in 2015 over the previous year, leaving 56 officers facing possible dismissal over allegations of serious misconduct. Details of the development are contained in a document posted to the RCMP website called Results and Respect in the RCMP Workplace. The document appears to be a means of updating the public on how the national police force has followed through on the findings and recommendations from the Mounties' Gender-Based Assessment and Gender and Respect Action Plan, in 2012 and 2013 respectively. In the introductory remarks, RCMP Commissioner Bob Paulson wrote that the purpose of the report is to "reassure and demonstrate to Canadians that purposeful and deliberate systems and processes have been deployed to change the inner workings — the guts of the organization as I've called it — in order to foster the culture change we are all seeking." Yet Paulson went on to caution that the culture change is slow. "While there is still work to do, change to the workplace, particularly cultural change, does not happen overnight, over a year or even over five years. Culture change occurs over a generation," wrote Paulson. The document appears to have been put together in some haste as it contained several typos and numerical errors when it was first posted. But it sheds some light on recent changes to the RCMP's internal disciplinary system. [CBC News](#)

Bow Island Mountie charged with sexual assault

A southern Alberta RCMP officer is accused of touching a woman in a sexual manner during a traffic stop search more than a year ago. Const. Elliot Teed of the Bow Island detachment was charged Monday with one count of sexual assault and two counts of breach of trust. Teed is expected to appear in Medicine Hat provincial court on May 4. Mounties say the charges stem from an RCMP investigation that was launched after a woman made a complaint on Feb. 16, 2015, about Teed's conduct during a traffic stop four days earlier on Bow Island, about 330 kilometres southwest of Calgary. The complainant alleged the officer touched her in a sexual manner during a physical search. As per standard RCMP practice, he has been suspended from duty since June and will remain off-duty until the charges have been resolved, at which point his duty status will be reviewed, police said. RCMP say an internal RCMP code of conduct investigation is also underway. [Calgary Herald](#); [CTV](#); [CBC](#); [Global](#); [Medicine Hat News](#); [Calgary Sun](#)

Car, train crash kills two young people west of Edmonton

How a car carrying two young people came to be in the path of a train west of Edmonton is still under investigation by RCMP. A 22-year-old man and 20-year-old woman in the car died at the scene last Tuesday. The railway crossing on Range Road 72 at Township Road 534 was "fully identified with train whistles activated," say police. The cause of the collision about 100 km west of Edmonton is still under investigation. Police are not releasing the victims' names or releasing any further information about the crash. [CBC](#)

Missing man found barricaded inside cabin, taken into custody

A missing man from Grand Falls-Windsor has been located by police, and has been taken into custody. Lee Wiseman, 38, was reported missing at 11 a.m. on Sunday, and the RCMP asked that the public be on the lookout for Wiseman's vehicle. Wiseman was located, police said, at 5 p.m. barricaded inside a cabin about 30 kilometres outside the central Newfoundland town. He was taken into custody hours later, at 11 p.m. Police said in a news release Tuesday that there was never a risk to the general public. [CBC](#)

BlackBerry Ltd Defends Against RCMP Decryption Claims

BlackBerry, defending itself against the RCMP decryption claims, has released a statement saying its focus has always been on protecting the privacy of its customers. Through this, it has tried to defend its core corporate and ethical principles. BlackBerry CEO John Chen highlighted that doing what is right for customers within legal and ethical boundaries has been the company's guiding principle. "We have long been clear in our stance that tech companies as good corporate citizens should comply with reasonable lawful access requests. I have stated before that we are indeed in a dark place when companies put their reputations above the greater good," Chen said in a blog post. Recently it was reported that the Royal Canadian Mounted Police (RCMP) got hold of BlackBerry's master encryption key and used it to intercept and decrypt about 1 million messages sent using BlackBerry's proprietary messaging technology. [Valuwalk](#)

Today's News / Actualités
April 18, 2016 / le 18 avril 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS |
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Wildfire forces evacuation of school in Maskwacis

The fires around Maskwacis have been contained. Two of them burning in that area. Students who were evacuated have now been allowed back. [CFCW](#)

Software flaws used in hacking more than double, setting record

The number of previously unknown software flaws used by hackers more than doubled last year, a new report says, in another sign of the increasing sophistication of cybercrime and online espionage. [Reuters](#) (Yahoo! News)

LAW ENFORCEMENT / APPLICATION DE LA LOI

(UPDATE): John Chen confirms BlackBerry cooperation in RCMP case, little else

BlackBerry CEO John Chen has posted a statement following press allegations that the Waterloo-based company may have provided the Royal Canadian Mounted Police with its global BlackBerry Internet Services (BIS) encryption key. In a post on the company's official blog, Inside BlackBerry, Chen neither confirmed nor denied the company's specific role in the RCMP's effort to dismantle two major Montreal-based mafia organizations. "We have long been clear in our stance that tech companies as good corporate citizens should comply with reasonable lawful access requests. I have stated before that we are indeed in a dark place when companies put their reputations above the greater good," starts Chen, referencing a 2015 post in which the CEO criticized companies like Apple for refusing to cooperate with law enforcement agencies. [Mobilesyrup](#); [CBC News](#); [Computer Dealer News](#); [Canadian Press](#) (Financial Post); [AFP](#) (Huffington Post); [Presse Canadienne](#) (Le Devoir)

Disciplinary hearing in RCMP graphic photo incident "adjourned indefinitely"

He's been suspended with pay for almost four years and it looks like that may be the case for one Coquitlam RCMP officer, indefinitely. The photos were an embarrassment to the Mounties. Corporal Jim Brown, in his RCMP-issued boots, was captured in bondage scenes with a woman. [CKNW](#)

Richmond Mountie faces assault charge

A Richmond Mountie has been charged after allegedly assaulting a man in a cell block. According to a Richmond RCMP news release on Friday, Const. Daryl Morrison is accused of assault causing bodily harm on April 4. Morrison was charged "following an investigation into his handling of a man" and, while the incident took place in a cell block, police didn't state whether the alleged victim was in custody at the time. [Richmond News](#)

Families want answers into unsolved homicides of their daughters

Two Manitoba families are demanding answers into two unsolved homicides on a remote First Nation. Both victims are from God's Lake First Nation located 550 kilometres northeast of Winnipeg. The families of 15-year-old Leah Anderson and 23-year-old Krystal Andrews protested outside RCMP headquarters on Portage Avenue, Monday. "We want to find out, ask the police what's being done. Is there DNA testing? Is there knocking on doors," said Justin Stevenson, Anderson's uncle. "Some of these families are hurting, they are crying, they want justice." Manitoba RCMP said both cases have remained active since day one, but will not speak publicly about the techniques or strategies used in the investigations. In an email to CTV News on Monday, Sgt. Bert Paquet said "each case has unique dynamics and investigators always consider a variety of avenues of investigation." RCMP said officers visit the community regularly and always try to keep relevant family members up to date, working with the goal of bringing them closure. [CTV News](#)

Moose Jaw man arrested after RV hits RCMP cruiser in Leduc

Leduc RCMP picked up a suspected drunk driver this morning---and the guy--was behind the wheel of an RV. Mounties say they saw the motorhome go through an intersection where a bunch of school kids had been waiting to cross. [CFW](#)

'I blame it on the meth': Travis Vader's sister offers glimpse into his past

Taped interviews with Bobbi-Jo Vader were played in court Monday, as part of her brother's double murder trial. She said Travis gave everything to his kids. The interviews with RCMP will be played in their entirety and Justice Denny Thomas will determine if they can be entered as part of the trial. In a taped interview on July 16, 2010, three days before Travis was arrested, Bobbi-Jo provided RCMP a look into her brother's life before he spiralled into despair. [Global News](#)

Today's News / Actualités
April 18, 2016 / le 18 avril 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS |
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

Quebec mom, son killed in Ecuador earthquake: relative

Two members of a Quebec family were among those killed during a massive earthquake in Ecuador on the weekend, a relative confirmed Monday. Guy Laflamme told Montreal radio station 98.5 FM his nephew's wife, Jennifer Mawn, and their son, Arthur Laflamme, were among the 350 reported dead after the roof of a residence collapsed on them. Laflamme said his nephew, Pascal Laflamme, and his family had moved to Ecuador not too long ago and that they liked travelling and working abroad. He said Pascal had been chatting on FaceTime with his father Real, who was in Quebec, when the earthquake hit Saturday night. "Everything was going well and from one moment to the next, everything started to shake, to vibrate," Laflamme said. "Pascal shouted, 'get out! get out! and all communication was cut off.'" The uncle said Pascal managed to get in touch later to confirm the deaths. Word of his son's death was sent by text first and a few hours after that, Pascal Laflamme managed to reach his father to also relate

command-and-control server located in Toronto, Ontario. A command and control server is a centralized computer that issues commands to a botnet and receives reports back from the co-opted computers. A botnet is a set of computers that have been compromised through the installation of malware and which can be instructed to send spam, install additional malicious programs, and/or steal passwords, among other illicit activity. The malware in this case was Win32/Dorkbot malware, which has infected more than one million personal computers worldwide by spreading through social networks, instant messaging programs, and USB flash drives... According to the CRTC, agencies from around the world, including the Federal Bureau of Investigation, Europol, Interpol, Microsoft Inc., the Royal Canadian Mounted Police (the "RCMP"), Public Safety Canada, and the Canadian Cyber Incident Response Centre, are working together on the investigation of Dorkbot. The warrant in Canada was granted by a judge of the Ontario Court of Justice and was carried out with assistance from the RCMP. No further details have been provided by the CRTC yet regarding the details of the warrant or the execution process. [Mondaq](#)

U.S. cyber soldiers hitting ISIS hard

The U.S. Cyber Command is taking the information security fight to ISIS hacking into the computers of individual fighters and interrupting the terror group's encrypted communications. The Daily Beast quoted three unnamed sources who gave a quick glance at Cyber Command's operation. American forces are implanting viruses and malware into computers used by specific ISIS members to pull out intelligence data on the organization's hierarchy leading to several being targeted and killed. Cyber Command is also working to disrupt ISIS' ability to communicate using encrypted devices. While unable to necessarily read what is being said, American forces are able to disrupt ISIS' ability to talk and thus coordinate its activities. [SC Magazine](#)

LAW ENFORCEMENT / APPLICATION DE LA LOI

BlackBerry CEO responds to critics' RCMP encryption key concerns

BlackBerry's CEO has responded to critics after it was revealed last week that the RCMP used a key to unlock approximately one million encrypted PIN-to-PIN messages sent between personal BlackBerry users since at least 2010. BlackBerry CEO John Chen published a blog post on the company's website Monday, noting that the company has always sought to "do what is right for the citizenry, within legal and ethical boundaries." "We have long been clear in our stance that tech companies as good corporate citizens should comply with reasonable lawful access," Chen said. "I have stated before that we are indeed in a dark place when companies put their reputations above the greater good." Chen said the company, headquartered in Waterloo, Ont., always strives to find a balance between "doing what's right" for the greater good, and protecting citizens' privacy. He pointed to an example from last November, when BlackBerry refused to give the Pakistan government access to its servers due to privacy concerns. He also pointed to a case from 2014, when the RCMP, with the help of BlackBerry, was able to intercept messages between suspected Montreal gang members, leading to dozens of arrests. "In the end, the case resulted in a major criminal organization being dismantled," he said. "Regarding BlackBerry's assistance, I can reaffirm that we stood by our lawful access principles. Furthermore, at no point was BlackBerry's (enterprise server) involved." Privacy experts expressed outrage last week, after news of the RCMP encryption key was revealed. [CTV News](#); [VICE News](#); [Motherboard](#); [Fiercemobile](#)

Teens warned about dangers of sexting from Crown prosecutor

A Crown prosecutor is cautioning teens to think twice before snapping an intimate photograph for themselves or a friend, even as a joke. Karen Lee, the lead counsel assigned to the internet child exploitation unit in New Brunswick, said many young people have no idea they're doing something illegal when they store those types of images on their phones and share them. Lee said the law is clear on what is considered a crime: it's illegal for anyone under 18 to take those kinds of photographs of themselves or other people. "The Criminal Code prohibits any sexualized image of a child, whether they be nude or in a sexualized situation, to be taken, possessed, looked at or shared," Lee said. "So for children, even just taking the photo is illegal, according to the Criminal Code." Lee said she sees these cases regularly in her job, particularly among young people. She said it has a lot to do with the technology and the ease with which people can not only take photos on their phones, but the illusion of privacy that comes with that technology. "It's become common," she said. Young people who share intimate photographs on

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Monday, April 18, 2016 12:50 PM
To: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Subject: CTV News: BlackBerry CEO responds to critics' RCMP encryption key concerns

Categories: Red Category

BlackBerry CEO responds to critics' RCMP encryption key concerns

CTV News

April 18, 2016 11:42AM ET

BlackBerry's CEO has responded to critics after it was revealed last week that the RCMP used a key to unlock approximately one million encrypted PIN-to-PIN messages sent between personal BlackBerry users since at least 2010.

BlackBerry CEO John Chen published a blog post on the company's website Monday, noting that the company has always sought to "do what is right for the citizenry, within legal and ethical boundaries."

"We have long been clear in our stance that tech companies as good corporate citizens should comply with reasonable lawful access," Chen said.

"I have stated before that we are indeed in a dark place when companies put their reputations above the greater good."

Chen said the company, headquartered in Waterloo, Ont., always strives to find a balance between "doing what's right" for the greater good, and protecting citizens' privacy. He pointed to an example from last November, when BlackBerry refused to give the Pakistan government access to its servers due to privacy concerns.

He also pointed to a case from 2014, when the RCMP, with the help of BlackBerry, was able to intercept messages between suspected Montreal gang members, leading to dozens of arrests.

"In the end, the case resulted in a major criminal organization being dismantled," he said. "Regarding BlackBerry's assistance, I can reaffirm that we stood by our lawful access principles. Furthermore, at no point was BlackBerry's (enterprise server) involved."

Privacy experts expressed outrage last week, after news of the RCMP encryption key was revealed.

Ann Cavoukian, Ontario's former Privacy Commissioner, said the fact that the key would have allowed the RCMP to read anyone's encrypted communications, not just the "bad guys," was "outrageous."

The issue of privacy and encryption made headlines earlier this year, when Apple opposed an order to help the FBI hack into an iPhone belonging to one of the San Bernardino shooters. In an open letter, Apple CEO Tim Cook said complying with the order would result in a new type of software that is "too dangerous to create."

Eventually, the FBI said it was able to hack into the phone without Apple's help.

This is not the first time Chen has commented on the issue of privacy.

In a blog post from last year, he noted that government officials have pleaded with technology companies for years to access criminals' encrypted data.

In the post, he appeared to allude to an example where Apple refused a lawful access request in an investigation of a known drug dealer, "because doing so would 'substantially tarnish the brand' of the company.

"At BlackBerry, we understand, arguable more than any other large tech company, the importance of our privacy commitment to product success and brand value: privacy and security form the crux of everything we do. However, our privacy commitment does not extend to criminals," he said in the post.

Link

Sent to: *!INTERNAL; RCMP Breaking News*

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Tuesday, April 19, 2016 8:55 AM
To: Cyber Security / Sécurité cybernétique (PS/SP)
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Follow Up Flag: Follow up
Flag Status: Completed

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique April 19, 2016 / le 19 avril 2016

Print Media / Médias en ligne

Alleged frat party attack spurs hacktivists

The hacker collective Anonymous has attacked Dalhousie University's website and crashed the Dalhousie Gazette news site to call attention to an alleged sexual assault at a fraternity house Halloween party last fall. Anonymous launched repeated denial-of-service attacks starting last week. On Friday, members of the group posted a video in which they named the alleged attacker and suggested a lack of action on the case could be due to potential ties between his family and the police. "We, as promised, waited patiently while the police gathered evidence," said the video, featuring a masked person speaking in a digitally disguised voice. "And now we can wait no longer." Dalhousie University spokesperson Brian Leadbetter, said the main Dalhousie website, dal.ca, was attacked April 1 and there were other attacks over the weekend. He confirmed their main website didn't go offline at any point last week. [Chronicle-Herald](#), A1 (2016-04-19)

BlackBerry CEO says co-operating with police a duty

The head of BlackBerry says tech companies have a duty to be "good corporate citizens" who co-operate with reasonable lawful requests from the police. The comments were in response to a story last week by Vice, which reported the RCMP intercepted and decrypted more than a million BlackBerry messages as part of an investigation between 2010 and 2012. The probe, dubbed "Project Clemenza," involved the killing of a Mafia crime family member. In a blog post Monday, BlackBerry (TSX:BB) chief executive John Chen said firms need to strike a balance between protecting the right to privacy and helping investigators apprehend criminals. Chen wrote that the world is a "dark place" when companies put their reputations above the greater good. He noted that the case resulted in a major criminal organization being dismantled. "For BlackBerry, there is a balance between doing what's right, such as helping to apprehend criminals, and preventing government abuse of invading citizen's privacy, including when we refused to give Pakistan access to our servers," Chen wrote. [ChronicleHerald](#), B3 (2016-04-19)

Online Media / Médias en ligne

Canada: Botnet Takedown: First Warrant Issued Under Canada's Anti-spam Law

Canada's anti-spam law ("CASL") outlines violations, enforcement mechanisms, and penalties aimed at protecting online consumers against spam, electronic threats, and misuse of digital technology. CASL's anti-spam rules came into effect on July 1, 2014. CASL's software update and installation rules came into effect on January 15, 2015. The latter rules are often referred to as malware/spyware computer program rules. Under these rules, CASL applies when a person, in the course of a commercial activity, installs or causes to be installed a computer program on any other person's computer system, unless the person has obtained the express consent of the owner or an authorized user of the computer system... On December 3, 2015, the CRTC announced that it served its first-ever warrant under CASL to take down a command-and-control server located in Toronto, Ontario. A command and control server is a centralized computer that issues commands to a botnet and receives reports back from the co-opted computers. A botnet is a set of computers that have been compromised through the installation of malware and which can be instructed to send spam, install additional malicious programs, and/or steal passwords, among other illicit activity. The malware in this case was Win32/Dorkbot malware, which has infected more than one million personal computers worldwide by spreading through social networks, instant messaging programs, and USB flash drives... According to the CRTC, agencies from around the world, including the Federal Bureau of Investigation, Europol, Interpol, Microsoft Inc., the Royal Canadian Mounted Police (the "RCMP"), Public Safety Canada, and the Canadian Cyber Incident Response Centre, are working together on the investigation of

Dorkbot. The warrant in Canada was granted by a judge of the Ontario Court of Justice and was carried out with assistance from the RCMP. No further details have been provided by the CRTC yet regarding the details of the warrant or the execution process. [Mondag](#) (2016-04-18)

U.S. cyber soldiers hitting ISIS hard

The U.S. Cyber Command is taking the information security fight to ISIS hacking into the computers of individual fighters and interrupting the terror group's encrypted communications. The Daily Beast quoted three unnamed sources who gave a quick glance at Cyber Command's operation. American forces are implanting viruses and malware into computers used by specific ISIS members to pull out intelligence data on the organization's hierarchy leading to several being targeted and killed. Cyber Command is also working to disrupt ISIS' ability to communicate using encrypted devices. While unable to necessarily read what is being said, American forces are able to disrupt ISIS' ability to talk and thus coordinate its activities. [SC Magazine](#) (2016-04-18)

BlackBerry CEO responds to critics' RCMP encryption key concerns

BlackBerry's CEO has responded to critics after it was revealed last week that the RCMP used a key to unlock approximately one million encrypted PIN-to-PIN messages sent between personal BlackBerry users since at least 2010. BlackBerry CEO John Chen published a blog post on the company's website Monday, noting that the company has always sought to "do what is right for the citizenry, within legal and ethical boundaries." "We have long been clear in our stance that tech companies as good corporate citizens should comply with reasonable lawful access," Chen said. "I have stated before that we are indeed in a dark place when companies put their reputations above the greater good." Chen said the company, headquartered in Waterloo, Ont., always strives to find a balance between "doing what's right" for the greater good, and protecting citizens' privacy. He pointed to an example from last November, when BlackBerry refused to give the Pakistan government access to its servers due to privacy concerns. He also pointed to a case from 2014, when the RCMP, with the help of BlackBerry, was able to intercept messages between suspected Montreal gang members, leading to dozens of arrests. "In the end, the case resulted in a major criminal organization being dismantled," he said. "Regarding BlackBerry's assistance, I can reaffirm that we stood by our lawful access principles. Furthermore, at no point was BlackBerry's (enterprise server) involved." Privacy experts expressed outrage last week, after news of the RCMP encryption key was revealed. [CTV News](#) (2016-04-18)

Cyber criminals shift sights from whole companies to individual employees

Every day, government agencies and private businesses are under threat from cyber criminals. While that is nothing new two recent industry reports show the tactics being used to attack them have changed, and technology alone is insufficient to stop the threat. "Every day millions of records are being stolen. It's happening right here, right now," said Ajay Sood, General Manager of FireEye Canada. "You can no longer use technology to meet this level of threat. FireEye, a security company headquartered in California that provides malware and network-threat protection systems for 4,400 customers in 67 countries (including 100 companies in Canada), released a report this year which showed businesses are swamped with alerts for security breaches — up to 17,000 each week. There's no system to rank or contextualize these breaches, which can leave major ones overlooked, and it can take up to 100 days to respond to serious breaches. FireEye's studies show that organizations can only manage to respond to 4 per cent of threat alerts and spend up to US\$1.2-million annually responding to inaccurate alerts... When asked to outline infrastructure and protocols that protect against cyber crime, **Mylène Croteau, a spokesperson for Public Safety Canada, said** in an email that the Government of Canada has a cyber crime Guide for Small and Medium Business that provides practical advice on how a business can protect itself and employees. In addition, it's the job of the **Canadian Cyber Incident Response Centre (CCIRC)** within **Public Safety Canada** to provide advice and support, **Croteau said. She** also explained that as part of **Canada's Cyber Security Strategy, the "Get Cyber Safe"** public awareness campaign is designed to help educate Canadians about internet security and how to keep themselves safe online. The website can provide information, **she** said on the most common threats and tips to help businesses protect themselves. From the IT department to counter-intelligence. In response, cyber security is no longer confined to the IT department; it has become a form of counter-intelligence. In 2014, FireEye acquired Mandiant, a security company that uses digital forensics. Today FireEye's 500 cyber-specialists worldwide include ex-military, computer scientists, and cryptographers who actively scour cyber networks for intelligence. The combination of local and global analytics and human and machine generated data is poured into their massive database to search for and take down malware to provide global coverage 24/7, Sood said. They're also working to plant operatives into cyber criminal terror cells in order to warn clients ahead of a cyber terror attack. [Yahoo! News](#) (2016-04-18)

Software flaws used in hacking more than double, setting record

The number of previously unknown software flaws used by hackers more than doubled last year, a new report says, in another sign of the increasing sophistication of cybercrime and online espionage. [Reuters](#) (Yahoo! News) (2016-04-18)

Insurers are 'vulnerable' to cyber attacks, says regulatory body

The IAIS, whose members are insurance market regulators based across the globe, said insurers face potential loss of confidential data, disruption of operations and reputational loss as a result of cyber risks. "The insurance sector is vulnerable to cyber incidents," the IAIS said in a new paper on cyber risk that it has opened to consultation. "Insurers collect, process, and store substantial volumes of data, including personally identifiable information. Insurers are connected to other financial institutions through multiple channels, including investment, capital raising, and debt issuance activities. Insurers execute mergers and acquisitions and other changes in corporate structure that may affect cybersecurity. Insurers outsource a variety of services, which may increase exposure to cyber risk." In its report the IAIS highlighted examples of cybersecurity weaknesses that regulators in the insurance sector have come across. It said insurers need to have oversight of the flow of data between their different "IT systems, applications, and components". It also flagged failings with "user privileges" extended to staff and said there needs to be "sufficient controls" on the access employees have to 'superuser' accounts. Insurers have to address cybersecurity "at all levels" of their organisation, the IAIS said. [Out-Law](#) (2016-04-19)

New cyber threats target Wairarapa

A Masterton business has the dubious distinction of being one of the first companies in Asia-Pacific to be targeted by a new type of cyber attack. Technology Solutions security expert Stephen Polley says cyber attacks on local businesses and individuals have been ramping up recently with crypto-ransomware incidents being reported in Wairarapa at a rate of about one a week. In a recent case a consultant with cyber security software provider ESET told Technology Solutions staff after finding malware detected on a Masterton business' computer that it was the first time they had seen this particular variant of the malicious software code in the Asia Pacific region. "To me it just highlights the fact that we are not to think that we're just small and out of the way. We're being specifically targeted as a town and a community," Polley says. A crypto-ransomware attack is when an attacker manages to infiltrate a computer system and encrypts all the valuable files. The owner then receives a note asking them to pay a ransom to get their files decrypted. [Stuff.co.nz](#) (2016-04-19)

Malware Based on JavaScript Attacks DNS Settings of Your Router

Trend Micro, a security firm, has revealed attack on the home routers which involves mobile website, malicious JavaScript, as well as mobile device like a smartphone. These types of attacks are happening after December 2015, and till now focuses on Japan, Taiwan and China. With United States being the fourth on attack list, hence be prepared for that. This new threat, namely JS_JITON, was first found in attacks toward December 2015-end, and hit its peak during February 2016 with more than 1,500 infections on daily basis. Meanwhile, it is still continuing infecting the devices till this day. As per report, a mobile website that is compromised may contain JavaScript, which then downloaded another JavaScript with DNS changing routines to the visiting mobile device. Despite the fact that the JavaScript could be downloaded on computer, the infection relies on the medium of the user - for instance, JS-JITONDNS merely infects the mobile devices causing DNS changing routine, while the JITON infection is activated only when the user have a ZTE modem. [SPAMFighter News](#) (2016-04-19)

Etude Check Point : Les attaques sur mobiles ont le vent en poupe

Durant Check Point Experience (CPX), la conférence annuelle européenne de la société, Check Point® Software Technologies Ltd. a dévoilé les principales familles de logiciels malveillants utilisés pour attaquer les réseaux des entreprises et les appareils mobiles dans le monde en mars 2016. Après son entrée dans le top dix en février 2016, l'agent mobile HummingBad est devenu le sixième type le plus courant d'attaque de logiciels malveillants dans le monde entier en mars. Il est également entré dans le top dix pour l'ensemble du premier trimestre 2016, malgré sa récente découverte en février. Les attaques contre les appareils mobiles Android utilisant cette famille de logiciels malveillants se développent donc très rapidement. Check Point a identifié 1 300 familles de logiciels malveillants uniques au cours de mars, soit une légère baisse par rapport au mois précédent prouvant que les cybercriminels n'ont pas besoin de développer de nouveaux logiciels malveillants pour lancer des attaques. Il leur suffit simplement de faire de petits changements dans les familles existantes pour permettre à la variante de contourner les mesures de sécurité traditionnelles. Des mesures avancées de prévention des menaces, telles que les solutions Check Point SandBlast et Mobile Threat Prevention, sont également nécessaires sur les réseaux, les postes et les appareils mobiles, pour stopper les logiciels malveillants à l'étape de pré-infection. [Global Security Mag](#) (2016-04-19)

G DATA Releases Malware Report for the Second Half of 2015

Today, global security firm, G DATA, released its H2 2015 Malware Report, which found that attacks by banking Trojans mainly targeted English-speaking countries, with 80% of all target sites located in the Anglophone region. The researchers also found a significant amount of attacks by banking Trojan, Dridex in particular. The criminals behind Dridex used spam email containing fictitious invoices or supposed tax refunds to lure recipients into their trap. The massive wave of attacks was averted by the unique G DATA BankGuard technology. "In the beginning of the second half of 2015, it initially appeared that attacks by banking Trojans had been significantly reduced," said Tim Berghoff, security evangelist, G DATA. "In fact, Swatbanker, a previously dominant Trojan, almost completely disappeared from the picture. However, in

December, our researchers found that Dridex was responsible for a huge wave of attacks through phishing emails, showing that banking Trojans are clearly still a major concern." [Virtual Strategy Magazine](#) (2016-04-19)

Python-Based Malware Infects European Companies

The use of Python means the PWOBot malware could easily be ported to different operating systems, says Palo Alto Networks. IT security researchers have discovered an unusual family of malicious code written entirely in the Python programming language, making it easy to port to different operating systems. The malware uses a modular design that allows it to carry out a selection of different attacks, including executing files, logging keystrokes, mining bitcoins using the affected system's CPU resources, executing arbitrary Python code and communicating with a remote server, according to Palo Alto Networks. [Tech Week Europe](#) (2016-04-19)

Android Users Warned Of New Mobile Malware Surge

Mobile users have again been warned against the risks of mobile malware as the number of attacks reaches a worrying high. Researchers at security firm Check Point found that malware variants such as HummingBad, Conficker and Sality made the first three months of 2016 a bad one for mobile users, but an encouraging time for cyber-criminals. Overall, Check Point identified 1,300 unique malware families during March, a slight decrease on the previous month, but an indication of the sheer scale of threats facing mobile users. However the firm found the UK was the 91st most attacked country globally during March (down from 74th in February), suffering more attacks than the USA (98th), but less than Germany (71st), Spain (52nd) and France (46th). [Tech Week Europe](#) (2016-04-19)

New CryptXXX Ransomware Locks Your Files, Steals Bitcoin and Local Passwords

CryptXXX is a new ransomware variant discovered during the past weeks, which, besides encrypting the user's data, is also capable of stealing Bitcoin from infected targets, along with passwords and other personal details, security researchers from Proofpoint have found. The first signs of the CryptXXX ransomware appeared towards the end of March. Security experts say the ransomware is distributed via Web pages that host the Angler exploit kit. This crimeware kit uses vulnerabilities to push the Bedep click-fraud malware on the users' systems. Bedep is also known for having "malware downloading" capabilities, so it will download the CryptXXX ransomware as a second-stage infection, dropping it as a delayed execution DLL, set to wait 62 minutes before launching. [Softpedia News](#) (2016-04-19)

Buffalo buffalo buffalo: malware that attacks malware

... Available at your nearest 'crimeware underground' system, Thanatos is a new strain of malware tooling that sports the ability to scan a target network for other malware. Reports suggest that Thanatos is offered at a price of \$1,000 per month or \$12,000 for a lifetime subscription. Named after the Greek god of death, Thanatos gets its ability to target other malware through the use of intelligent plugins. Thanatos effectively exhibits the characteristics of multi-staged malware tooling commonly found in Advanced Persistent Threat (APT) technology. Where this malicious software has power is in its ability to obliterate what we typically call 'low-level' attacks. Head of threat intelligence research at Cymmetria Nitsan Saddam writes on VentureBeat to explain that, "Thanatos uses 3-8 hardcoded flags to find malware by searching the host's task scheduler, services and registry. Once a suspicious signature is detected, Thanatos selectively uploads it to virustotal.com to make sure it's malicious and then erases it from the host. Another interesting feature is its ability to remove hooks placed by competing malware, in order to avoid data theft by other criminals." [SC Magazine](#) (2016-04-19)

New malware scam using Facebook Messenger

Digital security firm ESET is warning Facebook users of a common scam that sees attackers sending videos via Facebook Messenger through a user's friend list. ESET says by using the potential victim's current friend list to send the message, the hackers heavily increase their chances of successfully having the malware installed on their victims' computer. With the title "My first video", "My video", or "Private Video", the malicious link can also tag various people from a victim's friend list on a status and lures them into clicking on it. According to ESET, if a user falls for the scam, they will be re-directed to a fake YouTube website and let you know to install an extension to successfully load the content: "Sorry, if you don't install Video Play plugin, you will not be able to watch the video! Click 'Add Extension' to watch the video". "It's very concerning that this malicious link is targeting users directly through the messenger app, letting them think it is their friend sending a video," says Nick FitzGerald, senior research fellow at ESET. "Many users would think it is safe to click, but when the fake YouTube website comes up, they should not go any further," he warns. FitzGerald says if a victim clicks and installs the malicious plug-in, the browser they are using will become infected and continue to carry the infection with the same harmful content. [Security Brief New Zealand](#) (2016-04-19)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
April 20, 2016 / le 20 avril 2016

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse quotidienne
peut également être accédée via [InfoMédia](#)

MINISTER / MINISTRE

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / CYBERSÉCURITÉ

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS |
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRE

INTERNATIONAL

MINISTER / MINISTRE

*** RCMP misconduct cases more than double after new process implemented**

RCMP employee misconduct cases increased by 158 per cent last year — and the number of RCMP members facing dismissal more than quadrupled — after the force put a new investigation process in place. Overall, the federal law enforcement agency investigated a total of 741 cases. A report released last week says it's too soon to tell exactly why the number jumped, but suggests it's likely due to an increased emphasis on managers to deal with "unacceptable behaviour." The process has become more streamlined, the report says, allowing for matters to be dealt with within six months as opposed to 12-18 months under the old system, and has given managers and employees more flexibility in dealing with conduct issues. The number of members facing dismissal for serious misconduct increased 331 per cent, to 56 cases. "When appointed as RCMP Commissioner in late 2011, I was unequivocal in my pledge to transform the RCMP culture by focusing on accountability, leadership and addressing claims of harassment and bullying within the organization," Commissioner Bob Paulson says in the report's introduction. He says systemic transformation doesn't happen overnight, but it has been put into motion. The RCMP has been working to clean up its act following hundreds of allegations of workplace harassment. The RCMP is facing multiple lawsuits relating to harassment, gender discrimination and bullying. In February **Public Safety Minister Ralph Goodale** said he blasted Paulson over the

options than Glock handguns. "I am writing to again raise the issue of providing CEWs (Conducted Energy Weapons) to frontline officers," McCormack wrote in the letter, which was obtained by the Toronto Sun. "The time for action on this is now." We certainly can't wait for the next person to be shot by police and then pretend that it had nothing to do with politicians' refusal to provide officers with the tools they need. The time for action was actually in August 2013. Shortly after the streetcar shooting of Sammy Yatim resulted in second-degree murder charges being laid against Const. James Forcillo (he was later convicted of attempted murder), the provincial government cleared the way for Tasers to be issued to all officers - not just supervisors. "The use of CEWs has proven to result in fewer significant injuries to the public and police officers than many other use-of-force options," then-community safety minister Madeleine Meilleur said. [Toronto Star](#), A12; [Toronto Sun](#), A12

*** Self-reporting corporate misdeeds can be perilous**

The outcome of the cross-border foreign bribery investigation of Nordion (Canada) Inc. has fuelled the controversy regarding voluntary disclosure as the best alternative for a non-compliant company. "Self-disclosure was all the rage a few years ago, but companies and counsel in both the U.S. and Canada have become increasingly skeptical about the strategy in recent years," says Milos Bartuciski of Bennett Jones LLP in Toronto, who represented Nordion in Canada. The investigation centred around the activities of a Canada-based employee, Mikhail Gourevitch, in obtaining Russian government approval for the company's liver cancer treatment, TheraSphere. Gourevitch introduced Nordion to a Russian businessman whom the company retained to help with its efforts. It turned out that the Russian, without Nordion's knowledge, used some of his remuneration to bribe Russian government officials and kickback approximately \$100,000 to Gourevitch. Nordion's attempt to market its treatment in Russia ultimately failed. On uncovering the wrongdoing, Nordion acted promptly, spending some \$20 million on its internal investigation. "The facts in this case are very good from the company's point of view," says Riyaz Dattu of Osler, Hoskin Harcourt LLP in Toronto. "Nordion self-reported in both Canada and the U.S. as soon as it realized it had an issue, then fired Gourevitch and put remedial measures in place." The U.S. Securities and Exchange Commission imposed a US\$375,000 civil fine on Nordion for resolution of the U.S. anti-corruption proceedings. The RCMP, for its part, announced it would not pursue enforcement, reportedly for lack of evidence. [National Post](#), FP10

*** Inuit want exemption from Quebec's proposed long-gun registry**

Makivik Corp., representing Inuit in Nunavik, wants an exemption from Quebec's proposed long-gun registry, saying it treads on traditional hunting rights guaranteed under the James Bay and Northern Quebec Agreement. "Our rights and privileged exclusive rights are being diminished here," said Adamie Delisle Alaku, executive vice-president at Makivik. Bill 64, the Firearms Registration Act, would require that all firearms in Quebec be registered. On April 6, Makivik tabled a brief in the Committee on Institutions of the Quebec National Assembly itemizing their concerns over the bill. "We want an exemption because under the James Bay and Northern Quebec Agreement, which is a constitutionally protected agreement, we have rights," said Delisle Alaku. Under the proposed legislation each firearm would be assigned a unique number by the ministry, and owners would be required to "affix it to the firearm in the manner prescribed by government regulation." The penalty for failing to register a gun would be a fine ranging from \$500 to \$5,000. Makivik is requesting a full exemption from the bill for Nunavik Inuit until meaningful consultations take place. [CBC](#)

BlackBerry responds to police eavesdropping report

BlackBerry appeared to acknowledge it helped Canadian federal police crack a Montreal crime syndicate that had been using its messaging system, while insisting its smartphone security remains impenetrable. In a blog post, BlackBerry chief executive John Chen reiterated the company's long-held stance "that tech companies as good corporate citizens should comply with reasonable lawful access requests." The comments are the latest in a wider public discussion on how much access law enforcement officials should have to encrypted devices and how to balance security issues with user privacy rights. It was triggered when Apple recently refused an FBI request for access to the iPhone of San Bernardino mass shooters. Vice news and its sister publication Motherboard last week reported that BlackBerry may have helped Canadian federal police eavesdrop on BlackBerry so-called PIN-to-PIN messages sent between members of a suspected criminal organisation in Montreal. It was revealed that the Royal Canadian Mounted Police (RCMP) had obtained BlackBerry's global cryptographic key,

allowing the agency to read all messages sent between BlackBerry smartphones. This provoked a reaction from Prime Minister Justin Trudeau calling for better oversight of Canadian security and intelligence agencies. The RCMP said it had intercepted and decrypted more than one million BlackBerry messages in connection with its investigation, which began in 2010. [The Star Online](#), [Tech Times](#)

Speeding, drugs, theft among concerns conveyed to Kamloops RCMP

She has lived on MacKenzie Avenue in Kamloops for 43 years and has seen it all. On Tuesday night, she asked the 12 Mounties in front of her to visit her home. "I'd like to invite anybody to come and sit in my kitchen and watch what goes on in my neighbourhood," she said. "I'll make coffee or whatever. I watched a drug deal go down just before I came here — and the speeding is atrocious." The North Kamloops resident, who declined to give her name to *KTW*, was one of 22 residents on McArthur Island for the first of two Kamloops RCMP public forums this week. A second forum will take place Thursday at 7 p.m. at the Hal Rogers Centre in Sahali's Albert McGowan Park. The MacKenzie Avenue resident told RCMP Supt. Brad Mueller she has given scads of information to Mounties over the years, yet the nefarious activity in the area persists, including three fatal crashes and the still-unsolved 2006 murder of Henry Vandenberghe. "One drug house burned down," she said. "And that was a blessing." Tuesday night's meeting was the first such gathering to be held by the local RCMP since 2012 and was being held to explain to the public how police operations work and to solicit feedback from those served by the 130 officers in the city. [Kamloops This Week](#), [CFJC Today](#) (2016-04-19)

Policing committee to be considered

A new policing committee could be on the horizon for St. Albert. Coun. Bob Russell promised during his byelection campaign last June to pursue the creation of a policing committee to give the community a voice. On Monday a motion for city administration to work with the RCMP and the solicitor general on the establishment of such a committee and to bring back a bylaw or terms of reference for council's consideration was unanimously passed. Russell said a policing committee can serve an active function, and his suggestion was not meant to be a criticism of the St. Albert RCMP. "There are many areas where we can be of some help," he said, noting he's served on similar committees in the past. Russell said that the committee would have a voice to represent citizens, but would leave the day-to-day policing to the RCMP. He disputed a staff report that suggested an additional city employee would be needed to co-ordinate such a committee. [St. Albert Gazette](#)

RCMP overcome hockey hijinks to take charity title

The Cold Lake RCMP beat up on Cold Lake Fire-Rescue in the first annual charity hockey game to benefit Cold Lake Victim Services. The RCMP, sporting uniforms designed to mimic their ceremonial dress, jumped out to a 6-0 lead after the first two periods. The fire department finally found the back of the net in the third period, scoring two goals before the antics took over. Looking for an advantage, the fire department started playing with an extra man on the ice, and even brought out two extra pucks in an effort to close the gap. Despite playing disadvantaged, the RCMP took the trophy with an 8-6 victory. Both teams spent a significant amount of time playing pranks on their opponents. The RCMP blasted the firefighters with large water guns, and Staff Sgt. Jeremie Landry threatened to arrest Fire Chief Jeff Fallow. The fire department attacked the RCMP with water pistols of their own, and enticed the officers with donuts and Timbits attached to the end of a fishing rod. Cold Lake Mayor Craig Copeland, who coached the fire department team, was impressed with the ability of the police force. "The RCMP is a stacked team, they've been training all year round and we're in tough tonight," he said. "They're really good. They've got some players who've played junior hockey." Copeland was happy with the community's support. [Cold Lake Sun](#)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Locked Up And Alone

The average stay in solitary confinement for an inmate in 1999 at the Saskatoon jail: 17.5 days. The average stay during a three-month period 15 years later: 37 days. The increased use in jails not only in Saskatoon but across the province, revealed in a Ministry of Justice snapshot of data, is being strongly criticized by the head of the John Howard Society of Saskatchewan. "I'm concerned that even after the

Question Period Note / Note pour la Période des questions

BLACKBERRY COOPERATION WITH POLICE

ISSUE: RCMP technology in relation to lawfully obtaining evidence

PROPOSED RESPONSE:

- **Our government knows that it is not only possible but necessary to keep Canadians safe while at the same time defending their rights and freedoms, and we are working to ensure that the appropriate balance is achieved.**
- **I can assure Canadians that all police investigations in this country are governed by the law and the Charter and are subject to appropriate judicial processes.**
- **Court orders must be limited, specific and proportionate to the seriousness of the criminality under investigation.**
- **While it would be inappropriate for me to comment about a company's direct interaction with foreign law enforcement agencies, I can say that we expect Canadian companies to adhere to the laws of those countries.**
- **Soon, in our upcoming national security consultations, Canadians will have an unprecedented opportunity to provide advice on what laws and practices are reasonable and appropriate in these matters.**

On warrantless access to subscriber data:

- **In its June 2014 decision, the Supreme Court was clear that there is a reasonable expectation of privacy under s.8 of the *Charter* with respect to Basic Subscriber Information. Police must obtain a judicial authorization to obtain basic subscriber information such as a customer's name, address and phone number from telecommunications companies when this information allows for a link between a person's identity and their online activities.**
- **The decision also recognized some narrow exceptions for emergency situations.**

BLACKBERRY COOPERATION WITH POLICE

BACKGROUND:

BlackBerry media article (June 9, 2016)

On June 9, 2016, the CBC published an article regarding BlackBerry's lawful assistance to police investigations, such as the production of readable data (potential digital evidence) found on lawfully seized digital devices. The CBC article also included commentary from the University of Toronto's Citizen Lab, which stated in the article that BlackBerry Ltd. is allowing foreign police to bypass Mutual Legal Assistance Treaties (MLATs).

RCMP involvement

While the recent article did not explicitly mention the Royal Canadian Mounted Police (RCMP), it did refer to Canadian law enforcement in general. Moreover, previous media articles on this topic have referenced BlackBerry's assistance to the RCMP, specifically in connection with a high profile court case in Quebec involving organized crime (Project Ciemenza). In the recent article and in past media coverage, BlackBerry Ltd. has publicly defended its lawful assistance to priority criminal investigations when supported by reasonable, lawful access requests.

As Canada's national police force, the RCMP uses various technical investigative methods to lawfully obtain evidence in order to safeguard Canadians and conduct priority criminal investigations. The use of any investigative tools by the RCMP is governed by the law, including the Charter, and subject to appropriate judicial processes. By law, court orders must be limited and specific to the criminality under investigation, and can only be obtained if the statutory requirements are met. In general and to safeguard investigative techniques from criminal exploitation, the RCMP does not comment on specific investigative methods, tools and techniques outside of court.

The RCMP has a positive working relationship with Blackberry Ltd., which has been established for more than 10 years. The two organizations have regular communications on items of mutual interest. Blackberry Ltd. has supported and continues to support law enforcement in Canada under various court orders. It is the RCMP's experience that they are cooperative and comply with court orders, where possible. Where technically able to do so and under court order, Blackberry Ltd. provides support to law enforcement agencies globally in those jurisdictions where they have a presence or through MLAT requests.

Mutual Legal Assistance Treaties (MLATs)

Canada's MLAT provisions fall under the purview of the Minister of Justice. Mutual Legal Assistance is the formal process by which countries share evidence and provide other types of assistance to one another to advance criminal investigations and prosecutions. It is for Blackberry, as a private company and in consultation with their legal counsel, to determine whether and how it will provide assistance to foreign police agencies.

CONTACTS:

Submitted by:
Prepared by
Chris Lynam, Director, Strategic
Policy and Planning Directorate,
Specialized Policing Services

Tel. no.
613-843-4494

Approved by:
Deputy Commissioner,
Peter Henschel,
Specialized Policing Services

Tel. no.
613-843-4494

COOPÉRATION DE BLACKBERRY AVEC LA POLICE

SUJET : Technologie de la GRC et obtention légale d'éléments de preuve

RÉPONSE PROPOSÉE :

- **Le gouvernement sait qu'il est non seulement possible mais nécessaire d'assurer la sécurité des Canadiens tout en défendant leurs droits et libertés. Nous veillons à maintenir un juste équilibre entre les deux.**
- **Je peux assurer aux Canadiens que toutes les enquêtes policières menées au Canada sont régies par la loi, ce qui comprend la Charte, et qu'elles sont assujetties aux processus judiciaires applicables.**
- **Les ordonnances des tribunaux doivent être limitées, spécifiques et adaptées à la gravité du crime visé par l'enquête.**
- **Je dois m'abstenir de faire tout commentaire sur les interactions directes d'une entreprise avec des services de police étrangers, mais je peux affirmer que nous nous attendons à ce que les entreprises canadiennes respectent les lois de ces pays.**
- **Les prochaines consultations sur la sécurité nationale offriront aux Canadiens une occasion sans pareille de se prononcer sur les lois et les pratiques jugées raisonnables dans ce genre d'affaires.**

Au sujet de l'accès sans mandat aux renseignements sur les abonnés :

- **Dans une décision rendue en juin 2014, la Cour suprême a clairement statué qu'aux termes de l'art. 8 de la *Charte* une attente raisonnable en matière de respect de la vie privée protège les renseignements sur les abonnés. La police doit demander une autorisation judiciaire pour obtenir d'une entreprise de télécommunications des renseignements sur un abonné, tels son nom, son adresse et son numéro de téléphone, si ces renseignements permettent d'établir un lien entre l'identité de l'abonné et ses activités en ligne.**
- **Par ailleurs, la Cour reconnaissait dans sa décision des exceptions bien précises pour les situations d'urgence.**

COOPÉRATION DE BLACKBERRY AVEC LA POLICE

CONTEXTE :

Article sur BlackBerry (9 juin 2016)

Le 9 juin 2016, la CBC a publié un article sur l'aide légitime apportée par BlackBerry dans les enquêtes policières, notamment la production de données lisibles (éléments de preuve potentiels) trouvées dans des appareils numériques saisis légalement. L'article de la CBC renfermait aussi un commentaire du Citizen Lab de l'Université de Toronto selon lequel BlackBerry permet ainsi aux services de police étrangers de faire fi des traités d'entraide juridique.

Rôle de la GRC

Même si dans l'article récent on ne mentionnait pas explicitement la Gendarmerie royale du Canada (GRC), on faisait référence à la police au Canada en général. De plus, des articles précédents sur le sujet ont fait mention de l'aide offerte par BlackBerry à la GRC, plus précisément en lien avec un procès fortement médiatisé au Québec concernant le crime organisé (projet Clemenza). Dans le récent article et d'autres reportages dans les médias, BlackBerry Ltd. a défendu publiquement l'aide légitime apportée aux enquêtes criminelles prioritaires lorsqu'elles sont appuyées par des demandes d'accès légitimes raisonnables.

En tant que police nationale, la Gendarmerie royale du Canada utilise divers moyens d'enquête techniques pour obtenir légalement des éléments de preuve afin de protéger les Canadiens et d'effectuer des enquêtes criminelles prioritaires. L'utilisation d'outils d'enquête par la GRC est régie par la loi, ce qui comprend la Charte, et assujettie aux processus judiciaires applicables. Conformément à la loi, les ordonnances des tribunaux doivent être limitées et spécifiques au crime visé par l'enquête, et elles peuvent uniquement être obtenues si elles respectent les exigences de la loi. En général et afin d'empêcher les criminels d'exploiter les techniques d'enquête, la GRC ne fait aucun commentaire sur des outils, des méthodes et des techniques d'enquête en particulier en dehors des tribunaux.

La GRC entretient depuis plus de dix ans une relation de travail positive avec BlackBerry Ltd. Les deux organisations communiquent régulièrement sur des questions d'intérêt commun. BlackBerry Ltd. a appuyé et continue d'appuyer les services de police au Canada conformément à diverses ordonnances des tribunaux. Selon l'expérience de la GRC, l'entreprise est prête à coopérer et respecte les ordonnances des tribunaux, dans la mesure du possible. Lorsqu'elle a les moyens techniques de le faire et sur ordonnance du tribunal, BlackBerry Ltd. fournit un soutien à des organismes d'application de la loi étrangers dans les territoires où elle est présente ou aux termes de demandes en vertu de traités d'entraide juridique.

Traités d'entraide juridique

Au Canada, les dispositions des traités d'entraide juridique relèvent de la ministre de la Justice. L'entraide juridique est le processus officiel au moyen duquel un pays transmet des éléments de preuve et fournit d'autres types d'aide à un autre pays pour faire avancer des enquêtes ou des procès criminels. Il revient à BlackBerry, à titre d'entreprise privée et en consultation avec son conseiller juridique, de déterminer si et de quelle façon elle fournira de l'aide à des services de police étrangers.

CONTACTS:

Préparée par :
Chris Lynam, directeur,
Planification et Politiques
stratégiques, Services de police
spécialisés

Tél. : 613-843-4494

Approuvée par :
S.-comm. Peter Henschel,
Services de police spécialisés

Tél. : 613-843-4494

QUESTION PERIOD NOTE

Date: June 10, 2016
Classification: UNCLASSIFIED
Branch / Agency: RCMP

Question Period Note / Note pour la Période des questions

CANADIAN POLICE INVESTIGATIVE TOOLS AND TECHNIQUES

ISSUE: RCMP technology in relation to lawfully obtaining evidence

PROPOSED RESPONSE:

- **Canadian police investigations are governed by the law, including the *Charter*, and are subject to appropriate judicial processes.**
- **Court orders must be limited and specific to the criminality under investigation, and can only be obtained if the statutory requirements are met.**
- **While it would be inappropriate for me to comment about a company's direct interaction with law enforcement agencies around the world, I can say that we expect Canadian companies to adhere to the laws of those countries where applicable.**

Page 32
is a duplicate
est un duplicata

Rowe, Melissa (PS/SP)

From: Miller, Kevin (PS/SP)
Sent: Monday, June 20, 2016 6:06 PM
To: Bardsley, Scott (PS/SP); Brien, Dan (PS/SP); Peirce, Hilary (PS/SP)
Cc: Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP); Duval, Jean Paul (PS/SP); Croteau, Mylène (PS/SP)
Subject: Fw: [REDACTED]

Thanks Scott, we will follow up and coordinate in the morning.

Kevin

Kevin K. Miller
Communications Manager | Gestionnaire de Communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-949-9741
Fax | Télécopieur : 613-954-6048
Email | Courriel : kevin.miller@canada.ca

From: Media Relations / Relations avec les médias (PS/SP) <ps.mediarelations-relationsaveclesmedias.sp@canada.ca>
Sent: Monday, June 20, 2016 5:28 PM
To: Duval, Jean Paul (PS/SP); Miller, Kevin (PS/SP); Malik, Zarah (PS/SP); Levert, Jean-Philippe (PS/SP); Martel, Karine (PS/SP); MacLean, Megan (PS/SP); Croteau, Mylène (PS/SP); Baker3, Ryan (PS/SP)
Subject: FW: [REDACTED]

From: Bardsley, Scott (PS/SP)
Sent: June 20, 2016 5:28:30 PM (UTC-05:00) Eastern Time (US & Canada)
To: Media Relations / Relations avec les médias (PS/SP)
Cc: Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP); Brien, Dan (PS/SP); Peirce, Hilary (PS/SP)
Subject: [REDACTED]

Dear PS Media Relations,

[REDACTED] from the Toronto Star is working on a piece on encryption/lawful access based on an ATIP of the Minister's briefing materials and has asked MO to see if he could receive a briefing on the current law and policy in these areas. Could you please either arrange a briefing or a written reply?

I've sent him the following on the Minister's views:

Minister Goodale encourages and welcomes public debate on these important issues. Canadians need to reflect on this new and emerging area of law, privacy and crime prevention.

The government is constantly updating its policies and tools because of ever-changing technologies. Public Safety, the RCMP, academics and others continue to study these complicated questions.

We are committed to keeping Canadians safe while respecting their rights and freedoms, including their privacy rights. That commitment includes holding broad public consultations on national security issues.

Scott

PS: The Minister also touched on these issues directly in a recent speech:

“We need a thoughtful discussion about the legal framework that applies to new technologies. On the issue of encryption, for example, is absolute privacy the only "public good" that needs to be safeguarded, or is there a point at which criminal or terrorist investigations should be properly and lawfully assisted? And if so, where?”

Scott

Scott Bardsley

Press Secretary | Attaché de presse

Office of the Minister of Public Safety and Emergency Preparedness

Cabinet du ministre de la Sécurité publique et de la Protection civile

scott.bardsley@canada.ca | 613-998-5681

s.19(1)

Rowe, Melissa (PS/SP)

From: Miller, Kevin (PS/SP)
Sent: Tuesday, June 21, 2016 5:12 PM
To: Baker3, Ryan (PS/SP)
Cc: Duval, Jean Paul (PS/SP)
Subject: FW: [REDACTED]

Hi Ryan, wanted to give you an update on this call.

We have reached out to the reporter to try and get an exact sense of what he is looking for. We are waiting on the reporter to call-back to obtain more clarity.

JP spoke to Scott earlier today to provide an update, so MO is aware of our approach. We will provide an update as we keep moving on this call.

Thanks,
Kevin

From: Media Relations / Relations avec les médias (PS/SP)
Sent: Monday, June 20, 2016 5:29 PM
To: Duval, Jean Paul (PS/SP); Miller, Kevin (PS/SP); Malik, Zarah (PS/SP); Levert, Jean-Philippe (PS/SP); Martel, Karine (PS/SP); MacLean, Megan (PS/SP); Croteau, Mylène (PS/SP); Baker3, Ryan (PS/SP)
Subject: FW: [REDACTED]

From: Bardsley, Scott (PS/SP)
Sent: June 20, 2016 5:28:30 PM (UTC-05:00) Eastern Time (US & Canada)
To: Media Relations / Relations avec les médias (PS/SP)
Cc: Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP); Brien, Dan (PS/SP); Peirce, Hilary (PS/SP)
Subject: [REDACTED]

Dear PS Media Relations,

[REDACTED] from the Toronto Star is working on a piece on encryption/lawful access based on an ATIP of the Minister's briefing materials and has asked MO to see if he could receive a briefing on the current law and policy in these areas. Could you please either arrange a briefing or a written reply?

I've sent him the following on the Minister's views:

Minister Goodale encourages and welcomes public debate on these important issues. Canadians need to reflect on this new and emerging area of law, privacy and crime prevention.

The government is constantly updating its policies and tools because of ever-changing technologies. Public Safety, the RCMP, academics and others continue to study these complicated questions.

We are committed to keeping Canadians safe while respecting their rights and freedoms, including their privacy rights. That commitment includes holding broad public consultations on national security issues.

Scott

PS: The Minister also touched on these issues directly in a recent speech:

"We need a thoughtful discussion about the legal framework that applies to new technologies. On the issue of encryption, for example, is absolute privacy the only "public good" that needs to be safeguarded, or is there a point at which criminal or terrorist investigations should be properly and lawfully assisted? And if so, where?"

Scott

Scott Bardsley

Press Secretary | Attaché de presse

Office of the Minister of Public Safety and Emergency Preparedness

Cabinet du ministre de la Sécurité publique et de la Protection civile

scott.bardsley@canada.ca | 613-998-5681

Today's News / Actualités
August 16, 2016 / le 16 août 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS |
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

Trudeau says rights must be balanced with security in battling terrorism

An alleged terrorist plot in Ontario that created anxieties over police monitoring of suspects hasn't shaken Prime Minister Justin Trudeau's emphasis on balancing civil liberties with public safety. In his first reaction to an alleged plot that led to the death of Aaron Driver in Strathroy, Ont., Trudeau said Tuesday that balancing individual rights with keeping Canadians secure from bombing threats has to be handled with care. "Canada is a country that values its freedom (and) its basic charter rights," he said during a stop in Bridgetown, N.S., for an infrastructure announcement. "All Canadians expect their government to do two things: to keep Canadians safe and to defend and uphold the values and rights that all Canadians hold dear." "Getting that balance right isn't always easy in the challenging situation we now live in but it's

unsure whether Driver had died as a result of his own bomb or police bullets but the father said the autopsy had put that question to rest. "It was the police officer's bullet that killed him," the father told the National Post. "The bomb that exploded he could have walked away from with minor to severe injuries they said." [National Post](#); [CBC News](#); [Canadian Press](#) (London Free Press, Kingston Whig-Standard, CTV News); [Radio-Canada](#)

Crime in Canadian cities: 'Perceptions do not necessarily match the reality,' pollster says

The statistics say Saskatoon, Regina and Edmonton have the most severe crime but Canadians believe Winnipeg, Toronto and Montreal are the most dangerous cities, according to a new poll from Mainstreet Research. "The results paint an interesting portrait of how we see each other," Mainstreet president Quito Maggi said in a release. "Perceptions do not necessarily match the reality of crime and safety." Ottawa was perceived as the safest city of 15 included in the poll, followed by Charlottetown and Moncton. According to Statistics Canada, however, the cities with the least severe crime last year were Quebec City, Toronto and Ottawa, respectively. Canada's biggest city had the biggest perception-reality gap - despite having the second-lowest crime severity index, Toronto was perceived as the second most dangerous city, behind only Winnipeg. And Manitoba's capital, despite its unsafe reputation, had less severe crime than Vancouver, Edmonton, Regina and Saskatoon. [CBC News](#)

Cybersécurité: les chefs de police réclament l'accès légal aux mots de passe

Les chefs de police canadiens réclament une loi pour contraindre les gens à révéler leurs mots de passe aux forces de l'ordre avec l'approbation d'un juge. L'Association canadienne des chefs de police (ACCP) a adopté une résolution incitant le gouvernement à prendre des mesures législatives pour faciliter l'obtention de preuves électroniques. L'ACCP estime que les criminels ont de plus en plus recours au chiffrement pour dissimuler leurs activités illicites en ligne. Le commissaire adjoint de la Gendarmerie royale du Canada (GRC), Joe Oliver, a déclaré qu'aucune loi canadienne ne contraignait actuellement le détenteur d'un mot de passe à le révéler aux policiers dans le cadre d'une enquête. Lors d'une conférence de presse mardi, M. Oliver a soutenu que les criminels, qu'ils soient membres de la mafia ou pédophiles, bénéficiaient d'un anonymat quasi absolu en ligne. Cette résolution de l'ACCP survient alors que le gouvernement fédéral entame ses consultations en matière de cybersécurité, notamment par rapport à l'équilibre entre les besoins des policiers et les libertés fondamentales. Ces consultations se poursuivront jusqu'au 15 octobre. [Presse canadienne](#) (L'Actualité) ; [Canadian Press](#) (CTV News, News 1130, iPolitics); [CHED 630 AM](#)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Severe summer storm in the Prairies causes more than \$48 million in insured damage

Insurance Bureau of Canada (IBC) reports a severe storm that swept through Alberta, Saskatchewan and Manitoba during the second week of July has resulted in more than \$48 million in insured damage according to Catastrophe Indices and Quantification Inc. (CatIQ). From July 8 - 11, a low pressure system caused severe thunderstorms in the Prairies. The storms produced strong winds, hail, lightning, heavy rainfall, and funnel clouds. This system also caused significant flooding in Estevan, SK and produced a brief tornado touchdown in Humboldt, SK on July 10. [Insurance Bureau of Canada News Release](#) (Montreal Gazette)

B.C. Hydro concerned earthquakes from fracking could damage Peace River dams

Internal documents show B.C. Hydro officials have had concerns since at least 2009 that earthquakes triggered by fracking are a potential risk to its Peace River dams. The electricity-generating dams in northeastern B.C. include one of the largest earth dams in the world, the W.A.C. Bennett Dam, as well as the smaller Peace Canyon Dam, and the \$9-billion Site-C dam, which is under construction. The Crown agency has not discussed the issue publicly. But as a result of its concerns, B.C. Hydro worked out an agreement, possibly as early as 2014 with the B.C. Oil and Gas Commission (BCOGC), to create five-kilometre buffer zones around dams where no new fracking and drilling rights are issued, according to a report released today from the Canadian Centre for Policy Alternatives, a left-wing think-tank. [Financial Post](#)

I am thankful this situation did not escalate to an attack and was mitigated immediately. Although there may be many solutions to homegrown extremism, the most effective one is having a true and powerful counter-narrative. One example of such a narrative is the Ahmadiyya Muslim Youth Association, which is known for giving back to society through blood drives, food drives, city cleanups and much more. These counter-narratives will help put an end to homegrown extremism and continue to make Canada great..."
Winnipeg Free Press

Broadcast media / Médias télédiffusés :

The Ontario provincial police released a statement today saying a gunshot wound killed ISIS supporter Aaron Driver. Driver was killed in the southwestern Ontario city of Strathroy on August 10. It was the result of an RCMP investigation into a national security threat. (CBC News, 10:00ET, 12:00ET; CTV 12:30ET)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CBSA Proposes Amendments to NEXUS and Other Trusted Traveler Programs

The Canada Border Services Agency ("CBSA") recently announced that it was proposing changes to its Trusted Traveller Programs ("TTPs"), which include CANPASS, Free and Secure Trade ("FAST"), and NEXUS. In furtherance of this proposal, CBSA intends to amend the Presentation of Persons (2003) Regulations (the "POP Regulations"), which were implemented under the Canadian Customs Act. A summary of these proposed amendments appears below. Lexology

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Cybersécurité: les chefs de police réclament l'accès légal aux mots de passe

Les chefs de police canadiens réclament une loi pour contraindre les gens à révéler leurs mots de passe aux forces de l'ordre avec l'approbation d'un juge. L'Association canadienne des chefs de police (ACCP) a adopté une résolution incitant le gouvernement à prendre des mesures législatives pour faciliter l'obtention de preuves électroniques. L'ACCP estime que les criminels ont de plus en plus recours au chiffrement pour dissimuler leurs activités illicites en ligne. Le commissaire adjoint de la Gendarmerie royale du Canada (GRC), Joe Oliver, a déclaré qu'aucune loi canadienne ne contraignait actuellement le détenteur d'un mot de passe à le révéler aux policiers dans le cadre d'une enquête. Lors d'une conférence de presse mardi, M. Oliver a soutenu que les criminels, qu'ils soient membres de la mafia ou pédophiles, bénéficiaient d'un anonymat quasi absolu en ligne. Cette résolution de l'ACCP survient alors que le gouvernement fédéral entame ses consultations en matière de cybersécurité, notamment par rapport à l'équilibre entre les besoins des policiers et les libertés fondamentales. Ces consultations se poursuivront jusqu'au 15 octobre. Presse canadienne (L'Actualité) ; Canadian Press (CTV News, News 1130, iPolitics); CHED 630 AM

Largest ransomware-as-service scheme pulls in US\$195,000 a month: Report

Canadians are among those who have fallen victim to a global ransomware-as-a-service scheme which targeted tens of thousands of users in 201 countries and territories in July alone, according to security researchers. The researchers at Check Point Software and IntSights Cyber Intelligence of Israel released a report Tuesday saying the service, which it calls Cerber, is currently running 161 active campaigns with a total estimated profit of US\$195,000 last month alone. In July an estimated 150,000 devices were infected. Each day an average of eight new campaigns on average are launched, Check Point says. The biggest percentage of victims so far are in South Korea (29 per cent), the U.S. (14 per cent), Taiwan (9 per cent) and China (eight per cent). However, Check Point says there's evidence to support the developer's claim that Americans are among the top people willing to pay up. IT World Canada

Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
August 17, 2016 / le 17 août 2016

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse quotidienne
peut également être accédée via [InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS |
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRE

INTERNATIONAL

MINISTER / MINISTRE

**Goodale contradicted over detainee claim: 17 responded to minister's request for details on why
detention was unfair**

Advocates for a group of hunger-striking immigration detainees were shocked Monday to hear **Public Safety Minister Ralph Goodale** say none had replied to his request for details of why their detention was unfair. In fact, 17 of 50 detainees in two Ontario jails who ended a hunger strike in July responded to **Goodale's** invitation conveyed to them by Canada Border Services Agency officials. Syed Hussan, a member of the End Immigration Detention Network, told the Star that many wrote **Goodale** to make their individual case, and others did not. "Many of the detainees refused to participate. They didn't know what it was for. They didn't know it came from **Goodale's** office," Hussan said, adding many felt that, "the onus is not on the detainee to prove why he shouldn't be in there. "The onus is on the government to explain why someone is in prison without trial or charges, in the case of the people we work with, mostly for two-plus years." Scott Bardsley, a spokesman for **Goodale**, told the Star Tuesday that the minister was not fully briefed with the latest information on the hunger strikers' file prior to a news conference in Laval, Que., Monday. [Toronto Star](#), A11

incident is also ongoing. (...) Aaron Driver's father has said his son was a troubled child but appeared to have turned his life around after converting to Islam. But then the father said CSIS contacted him in January 2015 about disturbing posts his son had made on social media. Canadian Press (Red Deer Advocate, A8, Winnipeg Sun, Ottawa Sun, Toronto Sun, Times Colonist, Edmonton Sun, Calgary Sun, Daily Gleaner, Times & Transcript, CTV News); * Presse canadienne (Le Droit) ; * Radio-Canada

*** Les chefs de police réclament l'accès légal aux mots de passe**

Les chefs de police canadiens réclament une loi pour contraindre les gens à révéler leurs mots de passe aux forces de l'ordre s'ils ont obtenu l'approbation d'un juge. L'Association canadienne des chefs de police (ACCP) a adopté une résolution incitant le gouvernement à prendre des mesures législatives pour faciliter l'obtention de preuves électroniques. L'ACCP estime que les criminels ont de plus en plus recours au chiffrement pour dissimuler leurs activités illicites en ligne. Le commissaire adjoint de la Gendarmerie royale du Canada (GRC), Joe Oliver, a déclaré qu'aucune loi canadienne ne contraignait actuellement le détenteur d'un mot de passe à le révéler aux policiers dans le cadre d'une enquête. Lors d'une conférence de presse mardi, M. Oliver a soutenu que les criminels, qu'ils soient membres de la mafia ou pédophiles, bénéficient d'un anonymat quasi absolu grâce à des outils en ligne qui camouflent leur identité, de même que leurs communications. «Les victimes dans l'espace numérique sont réelles, a rappelé M. Oliver. Les lois du Canada et sa capacité à maintenir l'ordre doivent suivre le rythme de l'évolution technologique.» Cette résolution de l'ACCP survient alors que le gouvernement fédéral entame ses consultations en matière de cybersécurité, notamment par rapport à l'équilibre entre les besoins des policiers et les libertés fondamentales. Ces consultations se poursuivront jusqu'au 15 octobre. La Presse Canadienne (Le Quotidien, 17, Le Soleil); Canadian Press (Times & Transcript, Calgary Herald, National Post, Ottawa Citizen, Leader-Post, Edmonton Journal, Waterloo Region Record, Toronto Star, Hamilton Spectator, Edmonton Sun, Toronto Sun, Cape Breton Post, Chronicle-Herald, The Telegram, The Guardian)

*** Calgary police push for right to access digital passwords**

Calgary police are supporting calls for a new law that would force civilians to hand over electronic passwords to investigators with a judge's permission. Calgary police Chief Roger Chaffin was among those at the Canadian Association of Chiefs of Police who voted Tuesday to ask for legal means to obtain such digital evidence, saying it would help law enforcement keep pace with cybercrime. But civil liberties advocates say such a law would be highly problematic, and might even clash with the Charter of Rights and Freedoms. "When the chiefs of police want this sort of self-incrimination and openness, will it apply to them as well?" said Rocky Mountain Civil Liberties Association director Sharon Polsky, insisting it would be "flagrantly in violation" of Canadians' privacy rights. Current laws don't allow police to compel someone to give them a password. Deputy Chief Sat Parhar, who was in Ottawa with Chaffin to vote on the resolution, said the new legislation would be a guide for law enforcement, outlining when it is and isn't OK to access certain data. "There's a rule book, the rule book is the criminal code," said Parhar. "We're just saying this needs to be represented in the rule book. You don't want the police doing things without some sort of guidance through the law." Calgary Herald, A1

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Up to 47,000 houses face flood risk**

The Insurance Bureau of Canada wants a new deal for people who live in the riskiest, most flood-prone areas. On Tuesday, the association that represents most insurance companies in the country told the legislature's climate change committee it wasn't fair for taxpayers to keep subsidizing people who live in floodplains or along coastal areas. "I hate to say this, but in the industry we now call water the new fire," said Amanda Dean, a vice-president with the bureau. Thanks to torrential downpours, flooding has become the biggest insurance claim in recent years, outstripping the former number 1 claim, for fire damage. Over the last 20 years, property claims have doubled in New Brunswick, most of them due to water damage. Across Canada, annual insured losses from catastrophic events are now close to \$1 billion, with 2013 the high-water mark, when insurers paid out a record-high \$3.2 billion. In June, the association submitted a proposal for a national flood strategy to Ottawa. It spent more than \$1 million mapping out areas in Canada that are prone to flooding from rivers, and is about to do the same for

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Wednesday, August 17, 2016 8:40 AM
To: Cyber Security / Sécurité cybernétique (PS/SP)
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique August 17, 2016 / le 17 août 2016

Print Media / Médias imprimés

Les chefs de police réclament l'accès légal aux mots de passe

Les chefs de police canadiens réclament une loi pour contraindre les gens à révéler leurs mots de passe aux forces de l'ordre s'ils ont obtenu l'approbation d'un juge. L'Association canadienne des chefs de police (ACCP) a adopté une résolution incitant le gouvernement à prendre des mesures législatives pour faciliter l'obtention de preuves électroniques. L'ACCP estime que les criminels ont de plus en plus recours au chiffrement pour dissimuler leurs activités illicites en ligne. Le commissaire adjoint de la Gendarmerie royale du Canada (GRC), Joe Oliver, a déclaré qu'aucune loi canadienne ne contraignait actuellement le détenteur d'un mot de passe à le révéler aux policiers dans le cadre d'une enquête. Lors d'une conférence de presse mardi, M. Oliver a soutenu que les criminels, qu'ils soient membres de la mafia ou pédophiles, bénéficient d'un anonymat quasi absolu grâce à des outils en ligne qui camouflent leur identité, de même que leurs communications. «Les victimes dans l'espace numérique sont réelles, a rappelé M. Oliver. Les lois du Canada et sa capacité à maintenir l'ordre doivent suivre le rythme de l'évolution technologique.» Cette résolution de l'ACCP survient alors que le gouvernement fédéral entame ses consultations en matière de cybersécurité, notamment par rapport à l'équilibre entre les besoins des policiers et les libertés fondamentales. Ces consultations se poursuivront jusqu'au 15 octobre. [La Presse Canadienne](#) (Le Quotidien, 17, Le Soleil); [Canadian Press](#) (Times & Transcript, Calgary Herald, National Post, Ottawa Citizen, Leader-Post, Edmonton Journal, Waterloo Region Record, Toronto Star, Hamilton Spectator, Edmonton Sun, Toronto Sun, Cape Breton Post, Chronicle-Herald, The Telegram, The Guardian)

Calgary police push for right to access digital passwords

Calgary police are supporting calls for a new law that would force civilians to hand over electronic passwords to investigators with a judge's permission. Calgary police Chief Roger Chaffin was among those at the Canadian Association of Chiefs of Police who voted Tuesday to ask for legal means to obtain such digital evidence, saying it would help law enforcement keep pace with cybercrime. But civil liberties advocates say such a law would be highly problematic, and might even clash with the Charter of Rights and Freedoms. "When the chiefs of police want this sort of self-incrimination and openness, will it apply to them as well?" said Rocky Mountain Civil Liberties Association director Sharon Polsky, insisting it would be "flagrantly in violation" of Canadians' privacy rights. Current laws don't allow police to compel someone to give them a password. Deputy Chief Sat Parhar, who was in Ottawa with Chaffin to vote on the resolution, said the new legislation would be a guide for law enforcement, outlining when it is and isn't OK to access certain data. "There's a rule book, the rule book is the criminal code," said Parhar. "We're just saying this needs to be represented in the rule book. You don't want the police doing things without some sort of guidance through the law." [Calgary Herald](#), A1

Fighting crime in the digital age

An opinion piece states, "This week, top police officials from coast to coast have descended on our nation's capital for the 111th annual Canadian Association of Chiefs of Police conference. The topic that will shape their discussion, Public Safety in a Digital Age: Real Victims - Real Crime, is timely, given that we're at an important societal juncture. So much of our daily lives now take place online: our wealth passes through jurisdictions in the form of ones and zeros; the most intimate details of our lives, whether they are held by government or industry, rest on servers located somewhere around the globe; and our critical infrastructure, whether it is managed by the public or private sector, is operated digitally. Given the recent media coverage of data breaches and many people's personal experiences with fraudulent phishing schemes, it's understandable that we, as consumers and citizens, want to erect the highest walls possible around our valuable digital assets. This is a natural human reaction, but it isn't a realistic societal response, given the magnitude of our online world." [National Post](#), A8

Online Media / Médias en ligne

Ottawa announces public consultation on cyber security strategy

The federal government has started a three-month public consultation on updating its cyber security strategy, asking security pros and citizens for input on how it should not only strengthen the national IT systems and critical infrastructure in the private sector but also help businesses and residents. **Public Services Minister Ralph Goodale said Tuesday** the consultation, which ends Oct. 15, will help identify gaps and opportunities, bring forward new ideas to shape Canada's renewed approach to cyber security and capitalize on the advantages of new technology and the digital economy. [IT World Canada](#)

Public Safety Canada launches public consultation on cybersecurity landscape

Public Safety Canada (PSC) has launched a public consultation on the "evolving cybersecurity landscape." On Tuesday, the federal government launched the Consultation on Cyber Security to help identify gaps and opportunities, bring forward new ideas to shape Canada's renewed approach to cybersecurity and capitalize on the advantages of new technology and the digital economy, PSC said in a statement. From now until Oct. 15, PSC will be leading the consultation by engaging stakeholders and Canadians on the trends and challenges of cybersecurity, as well as on new initiatives under consideration which will strive to build Canada's resilience, capability and innovation in cybersecurity, the department said. Topics of the consultation include: the evolution of the cyber threat; the increasing economic significance of cybersecurity; the expanding frontiers of cybersecurity; and Canada's way forward on cybersecurity. **"Canadians spend more time online than people in any other country," said Ralph Goodale, Minister of Public Safety and Emergency Preparedness, in the statement. "We need to get really good at cybersecurity – across our personal, business, infrastructure and government sectors – so we can take full advantage of the digital economy, while protecting the safety and security of Canadians, and selling our valuable cyber skills and products into a booming market throughout the rest of the world."** [Canadian Underwriter](#)

Canadian Police Lobbies for Law That Would Force People to Reveal Passwords

Royal Canadian Mounted Police (RCMP) Assistant Commissioner Joe Oliver told Canadian press in a conference on Tuesday that his institution asked government officials for a law that would allow police officers to force crime suspects to reveal passwords for devices and online accounts. The RCMP official claims a spike in the number of cases where criminals employ encryption to protect sensitive and possibly incriminating data. RCMP officials are trying to criminalize situations where suspects refuse to cooperate. The proposal the RCMP made involves oversight, with a judge approving in situations where RCMP officers can force citizens to reveal passwords. [Softpedia News](#); [CanTech Letter](#); [Motherboard](#)

Hacking group auctions 'cyber weapons' stolen from NSA

A mysterious online group called the Shadow Brokers claims to have infiltrated an elite hacking unit linked to the National Security Agency and stolen state "cyber weapons", and is now auctioning them off to the highest bidder. The stolen malware is said to belong to Equation Group, a sophisticated hacking team believed to be operated by the NSA. So far, the Shadow Brokers have only released a few taster files and images of the cache, but security researchers said they appear to be legitimate. The leak, announced in broken English by the group in a series of posts on Twitter, Tumblr, Pastebin and Github, was accompanied by claims that the group was in possession of state-sponsored "cyber weapons". Kaspersky Lab, the security company that first exposed Equation Group's cyber-espionage in 2015, has published a detailed blogpost showing a "strong connection" between the files found in the leak and their earlier findings about Equation Group. Kaspersky has found encryption algorithms among more than 300 files in the Shadow Brokers' cache used in a way that has only been seen before in Equation Group malware. [The Guardian](#); [Threat Post](#); [Ars Technica](#); [Softpedia News](#)

Snowden Claims Russia is Behind NSA Hack

Former NSA contractor Edward Snowden has claimed that the Kremlin is most likely behind the recent cyber-attack on what is thought to be an NSA C&C server, and is using the data as leverage against a possible retaliation for the state-sponsored campaign against the Democrat party. The 'group' known as Shadow Brokers went public earlier this week with a treasure trove of "cyber weapons" it said belong to the Equation Group – outed last year by Kaspersky Lab as probably being baked by the NSA. Now Snowden has taken to Twitter to reveal what he believes happened – namely that the state-backed Shadow Brokers accessed a "staging server" belonging to the NSA, where it found the binaries it is now trying to 'sell'. [Info Security Magazine](#); [Fortune](#); [Engadget](#); [RT](#)

#Shadowbrokers hack could be Russia's DNC counter-threat to NSA

One of the most interesting hacks in recent memory is almost certain to be a compromise of infrastructure operated by an ultra-elite hacking group thought to be the United States' National Security Agency. The breach involves the public release of more than 300 files that showcase a host of exploits against companies including Cisco and Fortinet, plus tools known to be part of the National Security Agency's arsenal. Initial analysis by the likes of Kaspersky Labs, NSA whistleblower Edward Snowden, and a host of independent security researchers shore up claims by a hacking group calling itself Shadow Brokers that the exploits and toolsets it hopes to auction for millions of dollars in Bitcoins are legitimate Equation group weaponry. Kaspersky Labs last year revealed the Equation group to be almost certainly a

state-sponsored actor and, according to deep analysis of its activities, highly likely to be a wing of the National Security Agency given a series of very striking operational and technical similarities. It is a group that until February last year had conducted global hacking campaigns of the highest sophistication in complete stealth including interdiction attacks and persistent hard disk firmware re-writing using a suite of unique malware families. Its attacks had gone unnoticed for more than 14 years. Now the same Kaspersky Labs analysts who revealed Equation group confirm it has been compromised in the Shadow Brokers breach. [The Register](#)

The Shadow Brokers NSA hack claim unlikely say experts

The claim by the hacking group the Shadow Brokers that it has pilfered surveillance tools from another group, allegedly associated with the National Security Agency (NSA), is being called bogus by security experts. [SC Magazine](#)

How Cyberattacks on Critical Infrastructure Could Cause Real-Life Disasters

In October 11, 2012, then Secretary of Defense Leon Panetta warned of the impending dangers of a digital Pearl Harbor, a cyberattack that targeted critical infrastructure and caused real, physical damage. Since then, others have sounded the alarm bells of a cyberattack on infrastructure. Yet, other than the Stuxnet attack on an Iranian nuclear power plant, and a blackout enabled by a malware infection in Ukraine, there are very few examples of cyberattacks whose effects have spilled beyond the digital world. Security experts seem to agree that the threat is real—though highly misunderstood—and yet squirrels cause far more problems to the energy grid than hackers. But the fact that infrastructure attacks don't seem to happen very often doesn't mean they are not possible. Critical infrastructure, many agree, is highly vulnerable. [Motherboard](#)

Largest ransomware-as-a-service scheme pulls in US\$195,000 a month: Report

Canadians are among those who have fallen victim to a global ransomware-as-a-service scheme which targeted tens of thousands of users in 201 countries and territories in July alone, according to security researchers. The researchers at Check Point Software and IntSights Cyber Intelligence of Israel released a report Tuesday saying the service, which it calls Cerber, is currently running 161 active campaigns with a total estimated profit of US\$195,000 last month alone. In July an estimated 150,000 devices were infected. Each day an average of eight new campaigns on average are launched, Check Point says. The biggest percentage of victims so far are in South Korea (29 per cent), the U.S. (14 per cent), Taiwan (9 per cent) and China (eight per cent). However, Check Point says there's evidence to support the developer's claim that Americans are among the top people willing to pay up. [IT World Canada](#); [The Merkle](#); [Graham Cluley News](#)

US Dept of Energy spends \$34m on securing the smart grid

The US Department of Energy (DOE) has awarded \$34 million in funding to projects aimed at securing the smart grid. In total, 12 projects have been accepted as part of the Obama Administration's focus on energy-based infrastructure and the Office of Electricity Delivery and Energy Reliability's Cybersecurity of Energy Delivery Systems (CEDs) program. The DOE says the projects will aim to enhance the "reliability and resilience" of US smart grids through "innovative, scalable, and cost-effective research." The main focus, however, is on security -- and how to keep core infrastructure and electrical grids as safe as possible from outside intrusion. [ZDNet](#); [The Register](#)

Researchers Developed a System to Find Zero-Day Exploits

Researchers from Arizona State University created a way that makes gathering data from dark net markets and forums easy, and it helps identify new emerging cyber threats as they are released. The system utilizes search engines and dark net sites through the Tor network, and the researchers say they have found 30 marketplaces, and over 20 forums where black hat hackers reside. The system automatically gathers data from the sites and utilizes multiple information mining and machine learning techniques to organize the data that is collected. [The Merkle](#)

Pokémon Go 'App' Hides Nasty Ransomware Surprise

Security researchers have discovered new ransomware masquerading as a Pokémon Go app which also creates a backdoor in the victim's machine as well as attempting to spread itself via removable media. The malware itself is an updated version of the Hidden Tear open source initiative, according to Lawrence Abrams at Bleeping Computer. Discovered by researcher Michael Gillespie impersonating a Windows Pokemon Go app, the ransomware scans a victim's drive and encrypts any file with a certain extension – as per usual. However, there are some features which demand further attention. [Info Security Magazine](#); [SC Magazine](#)

New Vawtrak Trojan variant leverages SSL pinning, HTTPS

A new variant of the Vawtrak banking Trojan uses HTTPS to secure its command and control communications, and it includes support for SSL certificate pinning to evade detection in enterprise environments. As researchers continue to discover more about the deployment of new features in Vawtrak, the Trojan's developers continue to add new security features to the sophisticated malware platform. Vawtrak's incorporation of SSL certificate pinning, reported by Fidelis Cybersecurity, follows the recent PhishLabs' report that Vawtrak developers had added a domain generation algorithm (DGA) to the Trojan that is marketed as crimeware as a service and sold privately to malicious actors. [Tech Target](#)

Hacker puts source code of HL7 software vendor PilotFish up for sale on dark web

Security firm InfoArmor discovered that a cybercriminal placed the source codes to all PilotFish Technology software for sale on the dark web. PilotFish develops legacy standards, systems and technology software, including middleware to integrate disparate systems and HL7-supported medical devices. The threat actor, called 'batwhatman,' is offering the source codes on the underground marketplace called AlphaBay, which is on the TOR network and actively used by cybercriminals to sell illegal goods and services like stolen digital data. Currently, the marketplace has over 90,000 members. [Health Care IT News](#)

Data Of Nearly 900,000 At Risk In Latest Cyber Attack

Valley Anesthesiology and Pain Consultants, a large practice with more than 300 providers serving multiple hospitals across the greater Phoenix region, has suffered a cyber attack affecting 882,590 patients. The incident also affects all current and former employees and providers, the number of which was not disclosed. [Information Management](#)

Trojan affecting TeamViewer comes knocking on European and US doors

Another backdoor Trojan, BackDoor.TeamViewer.ENT.1, has been detected installing legitimate TeamViewer components on infected machines to spy on users. Doctor Web researchers discovered the malware has been in development since 2011 and regularly releases modified versions of it. The backdoor is distributed under the name SpyAgent. [SC Magazine](#)

Super-Sophisticated Spyware Spotted After 5-Year Run

Symantec and Kaspersky Lab last week separately announced the discovery of a highly sophisticated advanced persistent threat that had eluded security researchers for at least five years. A previously unknown group called "Strider" has been using Remsec, an advanced tool that seems to be designed primarily for spying. Its code contains a reference to Sauron, the main villain in The Lord of the Rings, according to Symantec. The APT spyware is called "ProjectSauron" or "Strider" in Kaspersky's report. The malware has been active since at least October 2011, Symantec said. It obtained a sample after its behavioral engine detected it on a customer's systems. Kaspersky found out about ProjectSauron when its software caught an executable library registered as a Windows password filter loaded in the memory of a Windows domain controller. The library had access to sensitive data in cleartext. [Tech News World](#)

Brazil Hit With a Second Major Banking Trojan Attack

Brazil is seeing its second major banking Trojan campaign in two weeks. IBM X-Force has discovered a new version of Zeus Sphinx, a sophisticated malware campaign now targeting the online banking and Boletto payment services of three of the top Brazilian banks, and one bank in Colombia, according to its configuration file. The criminals are likely trying to capitalize on the Olympic games in Rio, first with Zeus Panda, which targeted 10 local banking and payment industry targets in Brazil. Now, a fresh version of the Zeus Sphinx malware has been uncovered; it adapts social engineering injections to manipulate users in each targeted bank. [Info Security Magazine](#); [SC Magazine](#)

Operation Ghoul targets Middle East engineers, industrial players

Researchers have uncovered a wave of attacks against industrial and engineering companies in the quest for cash. According to Kaspersky, sensitive corporate financial data is the top target of the threat actors behind the campaign "Operation Ghoul," which operates primarily in the Middle East but is known to attack companies worldwide. The researcher's report, published on Wednesday, says that cyberattackers are using spear phishing as the main technique to infiltrate company servers. [ZDNet](#); [Threat Post](#)

Hackers only need 5 minutes to forge a phishing scam and 25 minutes to break into systems – Report

How long do you think it may take cybercriminals to hack into your computer? According to a new report by cloud-based cybersecurity firm Duo Security, it may take less than half an hour for hackers using phishing email campaigns to access systems and steal sensitive information. Duo Security collected data from 400 organisations using its free web-based tool Duo Insight, which allows internal IT teams to test employee response by sending out phishing campaign simulations. The firm said that of the 11,542 users who received such phishing emails, 31% clicked on links that could have potentially compromised systems via malware or virus attacks. [International Business Times](#)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Sent to: !Cyber Security Media Summary Dist List #1; !Cyber Security Media Summary Dist List #2; !Cyber Security Media Summary Dist List #3; !Cyber Security Media Summary Dist List #4

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Friday, September 09, 2016 8:44 AM
To: Cyber Security / Sécurité cybernétique (PS/SP)
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique September 9, 2016 / le 9 septembre 2016

Print Media / Médias imprimés

National security review tries to tackle needs of law enforcement in digital world

The Liberal government is taking another crack at making it easier for police and spies to gain "lawful access" to telecom companies' customers' subscriber information, online activities, telephone conversations, and encrypted communications. It comes deep into a sweeping discussion paper on how Canada should overhaul its national security laws. The so-called "green paper," released Thursday by Public Safety Minister Ralph Goodale, paints a picture of police and national security agencies stymied by technological advancements that terror suspects turn to their advantage, a Supreme Court of Canada decision that requires time-consuming unwieldy warrants for basic Internet subscriber information, and the failure of legislation to keep up with the bad guys. [Toronto Star](#), A8; [Canadian Press](#) (Guardian, B4, Cape Breton Post, Telegram, Telegraph-Journal, Times & Transcript)

Online Media / Médias en ligne

Cyberattack cripples Appalaches school board, cancer support group

The Sûreté du Québec's major crimes unit is investigating two cases of ransomware attacks. The Appalaches school board in Thetford-Mines and La Rose des Vents, a support group for cancer patients in Sherbrooke, reported the cyberattacks to authorities after they could no longer access their online documents. Both organizations reported that thousands of their files have been encrypted due to a virus called Zepto. Hackers are demanding \$20,000 in ransom from them in order to regain access to their data. [CBC News](#)

NATO officials, industry meet on cyber attack challenge

NATO officials, representatives from member states and private industry are meeting to discuss how to better defend against cyber attacks, which alliance leaders have called a security challenge that could cause as much harm as conventional military attacks. Ian West, chief of cybersecurity for NATO's Communications and Information Agency, told the conference in the Belgian city of Mons on Thursday that "all of us are facing the same ever-increasing number of incidents, types of incidents and sophistication of incidents." In July, U.S. President Barack Obama and other NATO leaders agreed to add cyberspace as a domain for alliance operations, along with land, sea and air. [Associated Press](#) (CTV News)

White House names retired Air Force general as first cyber security chief

The White House on Thursday named a retired U.S. Air Force brigadier general as the government's first federal cyber security chief, a position announced eight months ago that is intended to improve defenses against hackers. Gregory Touhill's job will be to protect government networks and critical infrastructure from cyber threats as federal chief information security officer, according to a statement. [Reuters](#); [Computing](#); [Hacked](#); [CSO](#); [Register](#)

Hot-cross-platform Mac vuln

Hackers have developed a cross-platform backdoor capable of infecting Windows, Linux or Mac OS X desktop computers. The Mokes malware family is able to steal various types of data from the victim's machine, including but not limited to screenshots, files and keystrokes. Researchers at Kaspersky Lab first came across malicious binaries on Linux and Windows systems back in January before the recent discovery of an OS X variant of Mokes. The malware was put together in C++ using Qt, a cross-platform application framework. [Register](#); [Tech Radar](#); [Telegraph](#)

Google Hacker Finds Way To Exploit Yet Another 'Stagefright' Bug

More than a year after the original discovery of the infamous Android bugs known as Stagefright, hackers keep finding similar flaws. On Wednesday, Google's own elite team of hackers released a proof-of-concept hacking technique that some believe could be used against practically all Android phones. Last summer, a security researcher found that a

series of bugs in a core part of the Android operating system could be abused to hack users with a simple multimedia message, potentially giving hackers full control of the phone before the target even saw the message notification. The bugs came to be known as Stagefright, and other security researchers and hackers soon found other ways to exploit them. [Motherboard](#)

New Linux Trojan Discovered Coded in Mozilla's Rust Language

A new trojan coded in Rust is targeting Linux-based platforms and adding them to a botnet controlled through an IRC channel, according to a recent discovery by Dr.Web, a Russian antivirus maker. Initial analysis of this trojan, detected as Linux.BackDoor.Irc.16, reveals this may be only a proof-of-concept or a testing version in advance to a fully weaponized version. Currently, the trojan only infects victims, gathers information about the local system and sends it to its C&C server. [Softpedia](#)

Cryptocurrency Mining Malware Discovered Targeting Seagate NAS Hard Drives

A malware variant named Mal/Miner-C (also known as PhotoMiner) is infecting Internet-exposed Seagate Central Network Attached Storage (NAS) devices and using them to infect connected computers to mine for the Monero cryptocurrency. Miner-C, or PhotoMiner, appeared at the start of June 2016, when a report revealed how this malware was targeting FTP servers and spreading on its own to new machines thanks to worm-like features that attempted to brute-force other FTP servers using a list of default credentials. [Softpedia](#)

CryLocker Ransomware Uses Imgur, Pastee, and Google Maps

MalwareHunterTeam has discovered a new ransomware family that calls itself CryLocker and abuses legitimate services such as Google Maps, Imgur, and Pastee. Researchers first spotted this ransomware towards the end of August, when they noticed something peculiar about its mode of operation, meaning the usage of UDP packets instead of TCP and several connections made to legitimate sites. [Softpedia](#)

Hypervisor security ero-Xen: How guest VMs can hijack host servers

The Xen project has today patched four security bugs in its open-source hypervisor – three potentially allowing guest virtual machines to take over their host servers. The other programming cockup allows a guest to crash the underlying machine. This is not great news for cloud providers or anyone else running untrusted VMs on their hardware and relying on Xen, because the three holes can be exploited by malicious guests to escape their confines and attack other virtual machines or the system beneath. Linode, for example, has had to patch and reboot its Xen-powered servers today to address the aforementioned flaws. Amazon's AWS is not affected. [Register](#)

WordPress update fixes XSS issues

Bloggers using the WordPress platform are "strongly encouraged" to update their sites immediately to address persistent XSS issues. The latest iteration, WordPress 4.6.1, rolled out on Wednesday to address two security issues: a cross-site scripting vulnerability via image filename, and a path traversal vulnerability in the upgrade package uploader, according to WordPress.org. The update also patches 15 other bugs in the underlying CMS codebase. [SC Magazine](#); [Threatpost](#)

Come in HTTP, your time is up: Google Chrome to shame leaky non-HTTPS sites from January

Starting New Year's Day, Google will begin labeling as "insecure" all websites that transmit passwords or ask for credit card details over plain text HTTP. If you use the ad giant's Chrome browser, and a lot of people do, in its 56th build and onwards any website that does not use a security certificate will feature a red exclamation mark and the text "Not secure," also in red, at the start of the web address. Those that do use certificates and so have an HTTPS connection will continue to get a nice little green padlock icon. [Register](#); [Threatpost](#)

Poorly secured smart home devices and wearables are a potential launch pad for cyber threats

You should be able to trust your garage door opener, but in the age of the Internet of Things (IoT), it and other smart-connected devices are entry points for hackers and other ne'er-do-wells. While security in the automotive sector is top of mind given recent vehicle hacks, and the FDA highly regulates medical devices, consumer connected home and wearable technology products are a segment where security is looser, and that's why it's the focus of the non-profit Online Trust Alliance (OTA), which found that 100 per cent of recently reported IoT vulnerabilities were easily avoidable (...) This conclusion was based on OTA researchers analyzed publicly reported device vulnerabilities from November 2015 through July 2016 to determine if an OTA IoT Trust Framework principle could have averted them. [IT World Canada](#)

Your Next Phone Could Have Quantum Security

Researchers have developed a "quantum entropy source" for random number generation that can fit into a phone or tablet, potentially offering new levels of safety and encryption for mobile transactions. Random number generators today are not entirely random because every "random" number starts somewhere. A computer takes a random "seed" number, like the time that the computer last rebooted, and then does some other math to it to shake it up. This is generally good enough for most purposes, but it means that a random number generated this way can actually be reproduced if you know

the starting point and the math that happened afterwards. If hackers can figure out even one of those two things, they've got a leg up on stealing data. [Popular Mechanics](#); [Scientific American](#)

How America's 911 emergency response system can be hacked

Critical to the success of the 911 emergency phone system, which has saved countless lives since it was first implemented in 1968, is its ability to quickly route calls to emergency responders closest to a caller. But a group of researchers say they've found a way to effectively disable the 911 emergency system across an entire state for an extended period of time by simply launching what's known as a TDoS attack, or telephony denial-of-service attack, against 911 call centers. The tactic involves infecting mobile phones to cause them to automatically make bogus 911 calls -- without their owners' knowledge -- thereby clogging call-center queues and preventing legitimate callers from reaching operators. [Washington Post](#)

Enterprise cloud apps carry 26 malware, on average

On average, enterprises have 26 piece of malware in their cloud apps, according to a new report. Cloud access security broker Netskope just released its Cloud Report – Autumn Edition, showing an overview of cloud app usage and trends in the EMEA (Europe, Middle East, Africa) region. Besides having an average of 26 malware in cloud apps, more than half (56 per cent) of infected files have been shared, both internally (within an organisation), and externally (shared either publically or with other organisations). Obviously, this represents the risk of malware spreading. Almost half of this malware (43.7 per cent) delivered ransomware, it was also said. [IT Pro Portal](#)

IoT Security Fears as Healthcare Software Tops 'Buggiest' Top 20

There were over 2,600 software bugs reported from May to July across the 'top 20' products, including flaws in highly sector-specific applications, which could be a worrying sign of things to come, according to Secunia. The vulnerability management division of Flexera Software claimed in its latest Vulnerability Update that there were 2,686 flaws in the top 20 most buggy products appraised, in line with the November 2015-January 2016 list after a brief dip to 1,768 in February-April this year. Microsoft topped the list of the most buggy vendors with a total of 518 vulnerabilities reported, with Windows 10, Windows Server 2012, Windows 8 and Windows RT the four products landing in the top 20. However, Secunia claimed that users are at least patching when a fix becomes available. [Infosecurity Magazine](#)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Sent to: !Cyber Security Media Summary Dist List #1; !Cyber Security Media Summary Dist List #2; !Cyber Security Media Summary Dist List #3; !Cyber Security Media Summary Dist List #4

**Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
September 9, 2016 / le 9 septembre 2016**

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse quotidienne peut également être accédée via [InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS |
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRE

INTERNATIONAL

MINISTER / MINISTRE

*** CSIS to brief other agencies on operations**

A controversial law that allows Canada's spies to engage in terrorism-disruption campaigns may pose problems for federal police and diplomats. For this reason, they are being given a peek at some CSIS operations - and even allowed to challenge them. Newly released records suggest that Bill C-51, the controversial 2015 omnibus bill that overhauled the Canadian Security Intelligence Service, has sent ripples throughout the federal-security bureaucracy. CSIS's so-called "threat-reduction activities" (or TRAs) have prompted fears of unintended fallout. To mollify concerns, the spy agency has committed to giving potentially affected agencies a heads up about what it is doing, according to records recently released to The Globe and Mail via access to information laws. For example, an "enhanced consultation memo" was recently signed between CSIS and Global Affairs Canada. While much is redacted in the

undated document, CSIS promises to loop in foreign-affairs functionaries about things it is doing. "The Service will provide intelligence assessments ... of TRA measures which have a foreign policy component." On Nov. 24, 2015, CSIS Director Michel Coulombe and RCMP Commissioner Bob Paulson cosigned a memo where they agreed to have their lieutenants brief each other on counterterrorism probes. CSIS's "new mandate to reduce threats" could potentially increase the likelihood of the agencies "adversely affecting each other." So, "when CSIS is considering the use of threat-reduction measures, CSIS will initiate strategic case-management discussions with the RCMP on the target of the measure," the memo says. It then adds that the RCMP can try to block any CSIS actions that could impair police investigations. "The RCMP may indicate that it needs time to review the information discussed to assess any potential conflict," it says. Should the two agencies end up at loggerheads, "the matter will be referred for a more senior level discussion." The memo came shortly after Liberal Prime Minister Justin Trudeau gave **Public Safety Minister Ralph Goodale** the job of undoing "the problematic elements" of C-51. Globe and Mail, A4

* **Liberals' slow movement on Bill C-51 raises suspicions**

Ralph Goodale is a minister who can spend 10 minutes answering a yes-or-no question, and that's a particularly useful skill when the topic is ragging the puck. The Liberal government has been putting off promised changes to Bill C-51, the controversial anti-terror legislation passed by Stephen Harper's Conservatives. On Thursday, **Mr. Goodale** and Justice Minister Jody Wilson-Raybould announced consultations on broader national security issues - the kind the Liberals promised to launch once they'd tabled legislation to replace C-51. But now changing Bill C-51 will come after the consultations, at some point in the future. That delay, **Mr. Goodale** said, was because the government is following an "**orderly**" process. He listed some things the government has done in the area of national security, which, he said, shows the Liberals aren't failing to live up to their promises to amend Bill C-51. (...) Government consultations can be self-confirming processes, but national-security policy has been a closed-circuit thing for too long. And **Mr. Goodale** noted the government has addressed two of the eight measures it promised to "**fix**" Bill C-51, notably by tabling legislation to create an intelligence-oversight committee of parliamentarians. (...) **Mr. Goodale** did say Thursday the government will still make five of those promised measures law, eventually. If you're counting, there's still one platform promise left out, and it's a big one: the pledge to limit the powers of the Communications Security Establishment, Canada's electronic eavesdropping agency, "by requiring a warrant to engage in the surveillance of Canadians." That promise grew out of a private member's bill sponsored by Liberal MP Joyce Murray, and security agencies don't want it. The CSE isn't supposed to target Canadians, but it can pick up their communications when they are targeting foreigners, and do warrantless bulk tracking of communications, intercepting so-called metadata - who called whom, when, for how long. They don't want to go to a judge each time. Is that change still Liberal policy? **Mr. Goodale** didn't recommit; an aide noted the CSE is under the jurisdiction of Defence Minister Harjit Sajjan. Mr. Sajjan's office didn't respond by press time. We'll see, eventually. **Mr. Goodale**, despite his verbal gymnastics, is a serious minister. But he might disappoint those anti-C-51 NDP-Liberal voters who now seem to have gone Liberal. The long version of the discussion paper released for public consultation gives the impression the Liberals aren't looking to roll back spy powers. Its tone suggests they favour the biggest feature of Bill C-51, which was giving Canadian Security Intelligence Service broad powers to "disrupt" threats - traditionally the purview of the RCMP - rather than to just collect intelligence. Globe and Mail, A7

Liberals seek public input on national security review

The Liberal government is taking another crack at making it easier for police and spies to gain "lawful access" to telecom companies' customers' subscriber information, online activities, telephone conversations and encrypted communications. It comes deep into a sweeping discussion paper on how Canada should overhaul its national security laws. The so-called "green paper," released Thursday by **Public Safety Minister Ralph Goodale**, paints a picture of police and national security agencies stymied by technological advancements that terror suspects turn to their advantage, a Supreme Court of Canada decision that requires time-consuming unwieldy warrants for basic Internet subscriber information, and the failure of legislation to keep up with the bad guys. The Liberals are broaching the hot-button topic more than four years after the Conservatives triggered an uproar when a senior cabinet minister - Vic Toews - accused opponents of siding with child pornographers if they didn't support a bill to update state powers of electronic surveillance. Amid a storm of criticism and a backlash from privacy advocates, that

bill was withdrawn. This time, the government is making a detailed legal argument in favour of updating its powers in public and inviting Canadians to weigh in. **Goodale** did not refer to the lawful access proposals in a news conference in Edmonton meant to highlight that the Liberals are keeping a promise to consult Canadians on changes to the Anti-Terrorism Act of 2015, also known as Bill C-51. He said the government wants Canadians' input on all kinds of changes to the country's national security framework to "**get it right.**" Toronto Star, A8

Liberals launch security consultation

The Liberal government's promised changes to a controversial anti-terrorism law likely won't come until next year, once officials have digested an array of public suggestions on revamping national security. The government opened an online consultation Thursday, soliciting feedback on everything from sharing information and preventing attacks to conducting surveillance and ensuring intelligence agencies are accountable. The consultation, which can be found at canada.ca/national-security-consultation, runs until Dec. 1. **Public Safety Minister Ralph Goodale** told a news conference in Edmonton the government also hopes House of Commons and Senate committees will hold public hearings on the national security framework. It means any legislation flowing from these reviews would not be tabled until December at the earliest and more likely in late winter or spring 2017. In the 2015 election campaign, the Liberals promised to repeal "problematic elements" of omnibus security legislation, known as Bill C-51, ushered in by the previous Conservative government. The bill gave the Canadian Security Intelligence Service explicit powers to disrupt terrorist threats, not just gather information about them. Canadian Press (Guardian, B4, Cape Breton Post, Telegram, Telegraph-Journal, Times & Transcript, Waterloo Region Record, Hamilton Spectator); * Postmedia Network (Edmonton Sun, A9, Edmonton Journal); *La redaction (45eNord)

Terrorists have rights

An opinion piece states, "The Liberal government of Justin Trudeau, which went apoplectic over the mere notion that the Stephen Harperites would yank the Canadian citizenship of a dual citizen convicted of terrorism, now wants to further restrict our security agencies in tracking down and neutralizing threats. It wants the RCMP, CSIS, and all agencies monitoring national security issues and terrorist activities, to play nicey-nice or face the consequences for colouring outside the guidelines. It wants them to use the Canadian Charter of Rights and Freedoms as a love-in template, even against those bound and determined on blowing us to kingdom come. It wants to geld them, and don't think otherwise. In announcing yesterday the start of an online consultation process for all Canadians to weigh in on how best to neuter the Tories' Bill C-51, the Anti-terrorism Act, **Public Safety Minister Ralph Goodale** kept stressing the rights and freedoms offered by the Charter should also be applied to the terrorism file. (...) While it is all well and good to ask Canadians to go online and assist **Goodale's** ministry in helping to define security measures, let's be real about what it really is. It's nothing more than a public-relations exercise to give the unjaded the impression of inclusive politics, not as a tool to drill down on policy. Remember, a camel is nothing more than a horse designed by a committee, so be prepared for an unwieldy monstrosity to emerge when the online input of Canadians ends on Dec. 1. Just don't expect to feel safer, or be safer, once the Liberals are done with the watered-down version of a piece of Conservative legislation that has thus far never failed us. But, hey, not that it matters, right? It wasn't long into **Goodale's** press conference on national security yesterday that it got derailed with an off-topic question from the media about a Canadian who was banned for life from entry into the United States for admitting to having smoked marijuana. From that point on, the terrorism talk went limp." Postmedia Network (Winnipeg Sun, A8, Toronto Sun, Ottawa Sun, Edmonton Sun, Calgary Sun)

*** Goodale rescinds Conservative directive that opened door to gun 'misclassification'**

Former public safety minister Steven Blaney issued a secret directive in the dying days of the Conservative government that opened the door for firearms to be classified according to a gun manufacturer's suggestion, CBC News has learned. Responding to complaints from firearms advocates and the industry, Blaney's directive gave the RCMP 180 days to evaluate a gun, decide its classification and issue the Firearms Reference Table (FRT) number needed to import that model into Canada. (...) The next day, Blaney issued a news release to announce he had overturned the RCMP's decision to classify the Ceska Zbrojovka CZ-858 rifle and certain Swiss Arms firearms as prohibited firearms — but there was no public announcement of his directive to Paulson. In fact, **Ralph Goodale**, the current Liberal

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Wednesday, October 05, 2016 8:47 AM
To: Cyber Security / Sécurité cybernétique (PS/SP)
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique October 5, 2016 / le 5 octobre 2016

Print Media / Médias imprimés

How Ottawa revived Canada's most controversial privacy issue

An opinion piece written by Michael Geist, Canada Research Chair in Internet and E-commerce Law at the University of Ottawa, states "The controversial issue of lawful access rules, which address questions of police access to Internet subscriber information and the interception capabilities at Canadian telecommunications companies, has long been played down by Canadian governments. When the policy proposals first emerged in the early 2000s, the Liberal government focused on the anti-terrorism and antispam benefits. Subsequent Conservative proposals promoted the ability to combat child pornography and, most recently, cyberbullying (...) Notwithstanding the legislative resolution and renewed legal certainty, Public Safety Minister Ralph Goodale has quietly revived the lawful access debate with a public consultation that raises the prospect of new rules that would effectively scrap the 2014 compromise. Ironically, the focus this time is the public's demand for amendments to Bill C-51, the Conservatives' anti-terrorism law that sparked widespread criticism and calls for reform during last year's election campaign. In other words, the balance of Canadian privacy is being put at risk by a policy initiative the purports to fix privacy. The Public Safety consultation skips over the years of lawful access debate by putting everything back on the table, acknowledging that the law was updated less than 24 months ago but suggesting that more change may be needed (...) In fact, Mr. Goodale places another controversial issue on the policy table, noting that encryption technologies are "vital to cybersecurity, e-commerce, data and intellectual property protection, and the commercial interests of the communications industry" but lamenting that those same technologies can also be used by criminals and terrorists." [Globe and Mail](#), B4

Yahoo scanned emails for NSA, FBI

Yahoo Inc. last year secretly built a custom software program to search all of its customers' incoming emails for specific information provided by U.S. intelligence officials, according to people familiar with the matter. The company complied with a classified U.S. government directive, scanning hundreds of millions of Yahoo Mail accounts at the behest of the National Security Agency or FBI, said two former employees and a third person apprised of the events. Some surveillance experts said this represents the first case to surface of a U.S. Internet company agreeing to a spy agency's demand by searching all arriving messages, as opposed to examining stored messages or scanning a small number of accounts in real time (...) Reuters was unable to determine what data Yahoo may have handed over, if any, and if intelligence officials had approached other email providers besides Yahoo with this kind of request. According to the two former employees, Yahoo chief executive Marissa Mayer's decision to obey the directive roiled some senior executives and led to the June 2015 departure of chief information security officer Alex Stamos, who now holds the top security job at Facebook Inc. [Postmedia Network](#) (Financial Post, FP1); [Ottawa Citizen](#); [Reuters](#) (CBC, Guardian (UK)), [Associated Press](#) (CTV News); [CNET](#); [ZDNet](#); [SC Magazine](#); [Infosecurity Magazine](#); [Softpedia](#)

Online Media / Médias en ligne

After Yahoo Revelations, Microsoft Swears It Didn't Spy on Users for the NSA

Microsoft was one of the first tech companies to deny involvement in spying programs secretly launched by the NSA and the US government and carried by Yahoo, according to recent revelations. The Redmond-based tech giant provided a very short statement to explain that the firm has never been involved in spying programs like the ones that Yahoo might have been part of, but the company refused to provide any other details on this. [Softpedia](#)

New FBI head in San Francisco was key figure in iPhone hack

The FBI's new leader in San Francisco is a former drug investigator who developed expertise in technology that put him at the centre of the government's effort to unlock an iPhone used by one of the San Bernardino shooters. Special Agent

Jack Bennett previously headed the bureau's digital forensics labs, which were tasked with accessing the San Bernardino gunman's phone. Bennett was at an FBI lab in Quantico, Virginia, in March when an outside company showed the bureau how it could hack the device. The tool ended the FBI's high-profile fight with Apple Inc. over access to the cellphone. That battle exposed a rift between the bureau and Silicon Valley over encryption. [Associated Press](#) (Montreal Gazette, Cape Breton Post, Guardian, Telegram)

Feds subpoena, gag encrypted chat firm Open Whisper Systems

Open Whisper Systems, the brainchild of cryptographer Moxie Marlinspike, has published the results of an unsealed subpoena set against the company -- and how little US law enforcement received for their trouble. The company is the developer of encrypted messaging application Signal, recommended by NSA whistleblower Edward Snowden, of which the technology is also used in other services including WhatsApp, Facebook Messenger and Google Allo. According to court documents unsealed last week, OWS was forced to hand over user data as part of a federal investigation, but the firm's ethos gave law enforcement very little to work with. [ZDNet](#); [Threat Post](#)

Facebook rolls out opt-in encryption for 'secret' Messenger chats

As of today, all of Facebook's 900 million Messenger users should be able to choose to have specific chat threads end-to-end encrypted, protecting a message from all eyes except the sender and recipient. Called Secret Conversations, the feature also allows users to set messages to self-destruct anywhere between five seconds to one day. Once a Secret Conversation is initiated, Facebook's app says that the conversation has been "encrypted from one device to the other". Encrypted conversations can be started from the home page by tapping a new message and then tapping the Secret button on the top right corner of the page, followed by the contact you want to start a secret chat with. The new privacy feature follows the completion of Facebook's end-to-end encryption rollout for the billion users of its other chat app, WhatsApp, earlier this year. [ZDNet](#)

Brand-New Delphi Trojan Exfiltrates Vast Amounts of Info

A never-before-seen credential-stealing Trojan has been uncovered, found to be backdooring machines and exfiltrating large amounts of information. Written in Delphi coding language (should we call it the Oracle at Delphi?), the Trojan.sysscan malware is being used by a single source as the payload for attacks that repeatedly use brute-force passwords for RDP credentials, according to GuardiCore. The malware has extensive capabilities to search and extract cookies and other credentials containing authentication details such as usernames and passwords. It appears to be targeted at banking, gambling and tax websites, and can scavenge information saved by Point of Sale (PoS) software. It also can run on every Windows version from XP through Server 2012 R2, the firm said. [Infosecurity Magazine](#)

OpenJPEG Flaw Allows Code Execution via Malicious Image Files

An update released last week for the OpenJPEG library addresses several bugs and important security issues, including a flaw that can be exploited to execute arbitrary code using specially crafted image files. OpenJPEG is an open-source library designed for encoding and decoding JPEG2000 images, a format that is often used to embed image files inside PDF documents. OpenJPEG is used by several popular PDF readers, including PDFium, the default PDF viewer in Google Chrome. Cisco Talos researchers discovered that OpenJPEG is plagued by an out-of-bounds heap write issue. The vulnerability allows an attacker to execute arbitrary code on the targeted user's system if they can trick the victim into opening a specially crafted JPEG2000 image or a PDF document containing such a file (...) The vulnerability was reported to OpenJPEG developers in late July and it was patched last week with the release of version 2.1.2. The issue is tracked as CVE-2016-8332 and it has been assigned a CVSS score of 7.5, which puts it in the high severity category. [Security Week](#)

Researchers spot remote code execution flaw in FreeImage

Cisco Talos researchers spotted a remote code execution vulnerability in the FreeImage Library XMP Image Handling affecting version 3.17.0. The bug is caused by an out-of-bounds write vulnerability which exists in the XMP image handling functionality of the FreeImage library and if exploited, would allow an attacker to use a specially crafted XMP file to cause an arbitrary memory overwrite resulting in code execution, according to an Oct. 3 blog post (...) A user can become infected if they open a malformed file sent to them via email, are tricked into downloading and opening the malicious file, or if the file is sent via instant message and is automatically opened due to user configuration, Talos Senior Technical Leader and Global Outreach Manager Craig Williams told SCMagazine.com. The file only needs to get to the victim's machine in order to execute the attack, he said. The vulnerability has already been reported and was patched in the CVS on Aug. 7, although the firm hasn't released a new version of the software. [SC Magazine](#)

Hacked WordPress Core File Leveraged for Hijacking a Site's Web Traffic

With WordPress dominating the CMS market by far, hackers will become more creative and aggressive in taking over websites and persisting infections for as much as possible. A new trick discovered by Sucuri experts during the past weeks sees attackers leveraging yet another WordPress core file to insert malicious code on hacked websites and redirect traffic to malicious sites. The file in question is wp-includes/template-loader.php, a core WordPress file that is

responsible for managing the site's page templates. In this most recent incident, hackers had altered this file to casually redirect some of the website's legitimate traffic to a malicious page that was offering users product keys for various Microsoft products at reduced prices. [Softpedia](#)

Insulin pump vulnerabilities could lead to overdose

Users of the Animas OneTouch Ping insulin pump system have been warned that security vulnerabilities in the device allow attackers to remotely deliver insulin doses. On Tuesday, researchers from Rapid7 revealed the existence of three vulnerabilities in the Animas OneTouch Ping insulin pump system (...) According to Rapid7 researcher Jay Radcliffe, the first vulnerability, CVE-2016-5084, reveals that data flowing between these two modules is transmitted in the clear. This opens the door for eavesdroppers to capture information such as dosage data and blood glucose results. The second critical security flaw, CVE-2016-5085, stems from the weak pairing between the pump and meter. The pairing process takes place during setup to prevent pumps from taking orders from other remotes in the vicinity and is done through a five-packet exchange in cleartext where the devices exchange serial numbers and some additional information (...) The third security vulnerability is equally as dangerous. The bug, CVE-2016-5086, highlights the fact the communication taking place between the pump and meter has no timestamps or sequence numbers and because of this, no defense against replay attacks, in which legitimate commands could be intercepted by an attacker and then played back at a later date. [ZDNet](#); [Threat Post](#)

Three-quarters of Firms Hit by DDoS

Nearly three-quarters of global firms have suffered a DDoS attack over the past 12 months with half losing \$100,000 or more each hour during peak periods, according to the latest study from Neustar. The global DDoS mitigation provider polled just over 1,000 C-suite execs to compile its October 2016 Worldwide DDoS Attacks & Protection Report. Of those who had experienced an attack, 85% said they were subject to multiple blasts, with the largest number (29%) suffering attacks between 2-5 times. Although 49% claimed they lost \$100,000 per hour during peak periods as a result of an attack, the figure went as high as \$250,000 or more for a third of respondents. Time is money, but unfortunately 71% of respondents said they took an hour or more to detect attacks and 72% an additional hour to respond. More worrying still for organizations is the fact that DDoS attacks appear to be increasingly used in conjunction with efforts to steal information, infect systems with ransomware or other cyberattacks – possibly as a smokescreen to distract IT teams. [Infosecurity Magazine](#)

Newsweek Site Suffered DDoS Attack After Trump Report

Newsweek's website suffered a distributed denial of service (DDoS) attack after it broke the story that US presidential candidate Donald Trump's company had violated a trade embargo on Cuba, reports TPM quoting Newsweek editor-in-chief Jim Impoco. A probe into the hack continues, but initial examination of the rogue IP addresses indicate that they originate from Russia, but they also could be spoofed, according to Newsweek. "As with any DDoS attack, there are lots of IP addresses, but the main ones are Russian, though that in itself does not prove anything," said Impoco. [Dark Reading](#)

Attack on South Korean "vaccine" router blamed on North Korea

North Korea is suspect number one in an attack against South Korea's cyber command last month, according to a member of the main opposition party, Minjoo. Representative Kim Jin-pyo, a member of the parliament's national defence committee, told South Korea's Yonhap News Agency the attack targeted a "vaccine routing server" on the cyber command network. The server provides security for around 20,000 military computers that access the internet. [SC Magazine](#)

Assange vows Google, US election leaks as WikiLeaks turns 10

In coming weeks, the site is set to publish documents related to Google, the US presidential election and more, according to controversial founder Julian Assange (...) Assange promised new information every week for the next 10 weeks, related to Google, military operations, arms trading and mass surveillance. He also promised that all documents related to the US presidential election would be published before the vote on November 8. Assange denied reports that he intended to harm the campaign of Democratic candidate Hillary Clinton, although he did describe the reaction to leaks of Democratic emails as "neo-McCarthy-esque hysteria." [Motherboard](#)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Sent to: !Cyber Security Media Summary Dist List #1; !Cyber Security Media Summary Dist List #2; !Cyber Security Media Summary Dist List #3; !Cyber Security Media Summary Dist List #4

**Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
October 5, 2016 / le 5 octobre 2016**

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse quotidienne peut également être accédée via [InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS |
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRE

INTERNATIONAL

MINISTER / MINISTRE

*** Windsor-Tecumseh politicians demand more disaster relief**

Politicians from Windsor-Tecumseh called on the federal and provincial governments to provide more financial assistance to homeowners suffering from flood damages. MPP Percy Hatfield wants the provincial government to change legislation to expand disaster relief coverage to people who suffered damages from sewer backup. Hatfield raised the issue during question period at Queen's Park on Tuesday afternoon, describing some of the widespread devastation left behind by last week's severe rainfall. Earlier in the day, provincial officials said people who suffered damages caused by sewer backup exclusively will not qualify for its Disaster Recovery Assistance program. "This is unfair," Hatfield said. "We should change the legislation, so everyone who is flooded during a proclaimed state of emergency

regions and Indigenous communities to collect and share data. In his mandate letter to **Public Safety Minister Ralph Goodale**, Prime Minister Justin Trudeau asked the minister to come up with a national plan on PTSD. [CBC News](#) (2016-10-04); [Canadian Press](#) (Kingston Whig-Standard, Waterloo Region Record, Vancouver Sun, Chronicle-Herald, Red Deer Advocate)

How Ottawa revived Canada's most controversial privacy issue

An opinion piece written by Michael Geist, Canada Research Chair in Internet and E-commerce Law at the University of Ottawa, states "The controversial issue of lawful access rules, which address questions of police access to Internet subscriber information and the interception capabilities at Canadian telecommunications companies, has long been played down by Canadian governments. When the policy proposals first emerged in the early 2000s, the Liberal government focused on the anti-terrorism and antispam benefits. Subsequent Conservative proposals promoted the ability to combat child pornography and, most recently, cyberbullying. Yet when the Conservatives passed lawful access legislation in late 2014, it seemed that more than a decade of debate had delivered a typical Canadian compromise... Notwithstanding the legislative resolution and renewed legal certainty, **Public Safety Minister Ralph Goodale** has quietly revived the lawful access debate with a public consultation that raises the prospect of new rules that would effectively scrap the 2014 compromise. Ironically, the focus this time is the public's demand for amendments to Bill C-51, the Conservatives' anti-terrorism law that sparked widespread criticism and calls for reform during last year's election campaign. In other words, the balance of Canadian privacy is being put at risk by a policy initiative the purports to fix privacy. **The Public Safety** consultation skips over the years of lawful access debate by putting everything back on the table, acknowledging that the law was updated less than 24 months ago but suggesting that more change may be needed." [Globe and Mail](#), B4

TOP STORIES / MANCHETTES

*** ISIL posts terrorist's account of attack**

Six weeks after a Canadian terrorist leader was killed by security forces in Bangladesh, ISIL has released what it said was his account of how his group attacked a Dhaka restaurant popular among foreigners. The Holey Artisan Bakery "was selected for this blessed operation because it was well-known for being frequented by the citizens of the Crusader countries," Tamim Chowdhury wrote in the Islamic State of Iraq and the Levant's magazine, Rumiya. Posted online Tuesday, it was the first acknowledgment from ISIL that Chowdhury, 30, was the head of "military and covert operations" in Bangladesh. The former Windsor resident died when police raided a Dhaka apartment Aug. 27. In his posthumous report on the attack at the restaurant, Chowdhury said it had been chosen from several potential targets because it was a "sinister place (where) Crusaders would gather to drink alcohol and commit vices through the night." Nine Italians, seven Japanese, an Indian, American and two locals died in the July 1 siege. [National Post](#), A1 (Leader-Post, Ottawa Citizen, Edmonton Journal, Calgary Herald, Montreal Gazette, Vancouver Sun, Windsor Star, London Free Press, StarPhoenix); [Globe and Mail](#)

*** Yahoo scanned emails for NSA, FBI**

Yahoo Inc. last year secretly built a custom software program to search all of its customers' incoming emails for specific information provided by U.S. intelligence officials, according to people familiar with the matter. The company complied with a classified U.S. government directive, scanning hundreds of millions of Yahoo Mail accounts at the behest of the National Security Agency or FBI, said two former employees and a third person apprised of the events. Some surveillance experts said this represents the first case to surface of a U.S. Internet company agreeing to a spy agency's demand by searching all arriving messages, as opposed to examining stored messages or scanning a small number of accounts in real time (...) Reuters was unable to determine what data Yahoo may have handed over, if any, and if intelligence officials had approached other email providers besides Yahoo with this kind of request. According to the two former employees, Yahoo chief executive Marissa Mayer's decision to obey the directive roiled some senior executives and led to the June 2015 departure of chief information security officer Alex Stamos, who now holds the top security job at Facebook Inc. [Postmedia Network](#) (Financial Post, FP1); [Ottawa Citizen](#); [Reuters](#) (CBC, Guardian (UK)), [Associated Press](#) (CTV News)

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Thursday, October 06, 2016 8:49 AM
To: Cyber Security / Sécurité cybernétique (PS/SP)
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique October 6, 2016 / le 6 octobre 2016

Online Media / Médias en ligne

NSA contractor arrested over 'stolen secret code used to hack Russia'

The FBI has secretly arrested a National Security Agency (NSA) contractor suspected of stealing highly classified computer codes used to hack the computer systems of foreign governments including Russia and China, raising fears of another embarrassing intelligence leak to rival the Edward Snowden affair, the New York Times reported on Wednesday (...). The contractor in this case, who was reportedly arrested "in recent weeks", is suspected of stealing the NSA's "source code", used to break into the computer networks of rival powers such as Russia, China, Iran and North Korea. Independent (UK); New York Times; Washington Post; CNET; SC Magazine; IT Wire; Intercept; Softpedia

Google Patches 78 Vulnerabilities in Android

Google this week released another set of monthly patches for the Android mobile operating system, in an attempt to address no less than 78 security vulnerabilities.

Just as it has over the past few months, Google split the October 2016 security patches in two, each focused on specific issues. The *2016-10-01 security patch level* addresses 20 vulnerabilities in various platform components, while the *2016-10-05 security patch level* plugs 58 flaws in kernel subsystems, drivers, and OEM components. Security Week

Researcher finds flaws in industrial control devices

In a report by Applied Risk, ICS security researcher, Alexandru Ariciu, said that flaws found in MOXA E1242 Ethernet remote I/O series used in factory automation, range from code injection in the web application to weak password policies and implementation. One of the problems lies in the devices web application that fails to sanitise user input, resulting in Javascript injection in the webpage. An exploit could allow an attacker to execute arbitrary code in the context of the browser of the users visiting the affected web pages... Another issue is that passwords are sent via the HTTP GET method. The md5 hash of the password that is used for authentication on the device is sent as a parameter in each GET request to the server. "This is considered to be bad practice, as an attacker with a MITM position can easily circumvent this implementation and bypass the authentication mechanism," said Ariciu. Also the password used to authenticate users to the system is truncated to eight characters. Any user trying to use a longer password will have its password cut down to the first eight characters. Also, the MD5 hash challenge that is created for authentication and is later used in all GET requests will be created using these first eight characters. SC Magazine

Akamai Post-Mortem Report Confirms Mirai as Source of Krebs DDoS Attacks

With all the infosec community impatiently waiting for more details on the huge DDoS attack that hit the KrebsOnSecurity blog, Akamai has now released its official post-mortem report on the aforementioned incident... As Krebs moved his website to Google's Project Shield, other investigators looking into the DDoS traffic determined that attackers had used a botnet created with the Mirai malware. Discovered by MalwareMustDie in September, the researcher said this malware is vaguely related to the Gafgyt malware family tree (also known as Lizkebab, BASHLITE, BashOday, Bashdoor, and Torlus). According to Akamai's own investigation, the malware is also related to the Kaiten malware, which, just like Gafgyt, targets smart IoT devices. Akamai says its researchers had been tracking this Kaiten variant (identified as Kaiten/STD) since January this year. Akamai's analysis of Kaiten/STD is identical with MalwareMustDie's Mirai findings, so there's nothing new to surprise us in relation to the malware's mode of operation, which consists of brute-forcing Telnet and SSH ports left open on IoT devices, mainly on IP cameras, CCTV and DVR systems... According to Akamai's official numbers, the Krebs DDoS attack reached 620 Gbps, as Krebs tweeted himself, and also involved an additional, smaller botnet, outside of Mirai. Akamai also confirmed that the Mirai botnet was mainly comprised of security cameras and DVRs, as initially rumored. Around half of the bots were located in the EMEA (Europe, Middle East, and Africa) region, while North America and the APJ (Asia-Pacific and Japan) region accounted for around a quarter each. Softpedia

DDoS attacks consistent, relentless and costly

Neustar, a provider of real-time information services, has published its "October 2016 Worldwide DDoS Attacks & Protection Report: A Steady Threat in the Connected World," (registration required for a free report) focused on DDoS attack and protection trends. The report says the DDoS attack volume has remained consistently high and these attacks cause real damage to organisations. The global response also affirms the prevalent use of DDoS attacks to distract as "smokescreens" in concert with other malicious activities that result in additional compromises, such as viruses and ransomware. [IT Wire](#)

Spotify Free is Serving Up Malware

Numerous users are flooding music streaming service Spotify's Twitter feed, reporting that the freemium tier service has been hit with a malvertising attack. Those running Spotify Free on the desktop are periodically seeing strange browser behavior, with malicious ads serve malware popping up unbidden... For its part, Spotify responded in the user forum, saying that it has placed the issue under investigation. [Infosecurity Magazine](#); [SC Magazine](#)

Oil 'slick': Sneaky OilRig malware campaign flows into new territory

A backdoor malware campaign dubbed OilRig that in May was discovered targeting organisations in Saudi Arabia is now trying to drill into government entities in Turkey, Israel and the US, as well as Qatari companies and organisations. Palo Alto Networks Unit 42 threat research team updated the campaign's latest spear-phishing efforts in a blog post on Tuesday, warning that the campaign has updated its "Helminth" backdoor software as well as the malicious Excel documents that distribute the malware via macros. According to the blog post, the phishing emails targeting Qatari organisations "were very specific to the organisation receiving them and in some cases were sent from partner organisations that already had a relationship with the recipient." Changes to malware over the last five months include the emergence of four distinct variants, each of which drops different filenames upon execution, Palo Alto continued in its report. [SC Magazine](#)

Beware of New Steam Spam Leading to Malware

Since last week, Steam gamers have been warning each other, via Twitter and Reddit, about a new spam campaign that tries to lure them to a site to download malware on their computers, which in the end, allows crooks to take over their PCs. This spam campaign begins with a hacker taking over a legitimate Steam account. This is possible today thanks to the large number of data breaches disclosed this year, many of which included cleartext passwords. If Steam gamers haven't turned on two-factor authentication for their Steam accounts and reused the same password on multiple sites, attackers can gain control over their accounts, and then use this newly-found access to spam their friends with malicious links. [Softpedia](#)

Official: Hackers who hit French TV station are still active

A French official says the hackers who knocked a French television station offline last year are still regularly trying break in to French government computers. Senior French cybersecurity official Guillaume Poupard says sensors deployed at government ministries routinely pick up electronic signatures linked to the group. The revelation adds another dose of intrigue to the attack, which briefly interrupted 11 channels belonging to TV5 Monde and packed its social media sites with propaganda for the Islamic State group. The idea that tech-savvy fanatics could hijack a major broadcaster sent a shiver across France. But L'Express magazine turned those fears on their head when it reported that investigators believed a Russian group carried out the attack. [Associated Press](#) (Yahoo News)

Two-thirds of IT Bosses Fear Ransomware Attack

Over two-thirds (69%) of IT decision makers believe their organization will be hit by a ransomware attack over the next 12 months, although many are still unsure what that will actually entail, according to Trend Micro. The security giant shared more findings from a poll of over 300 IT leaders, which has already revealed that 44% have experienced an attack over the past two years. The figure for those bracing themselves for an attack in the next year rose to 75% for organizations that have already been on the receiving end, Trend Micro claimed. [Infosecurity Magazine](#)

And the country with the most bot infections is... Turkey

Turkey has the largest number of total "bot" infections with one bot for every 1,139 internet users in the country and also contains 18.5 percent of all of the bots across the EMEA region, according to researchers at Symantec's Norton division. Most of the affected computers resign in the cities of Istanbul and Anakara which together account for more than half of the country's population, according to the press release. The report also found that following Turkey, the top ten countries by total bot population in descending order include, Italy, Hungary, Germany, France, Spain, the U.K., Poland, Russia, and Israel. [SC Magazine](#)

Watch a Quantum Computing Expert Describe How the World's About to Change

Quantum physics, with its descriptions of bizarre properties like entanglement and superposition, can sound like a science fiction fever dream. Yet this branch of physics, no matter how counterintuitive it seems sometimes, describes the universe

all around us: As physicists have often told me, we live in a quantum world. Soon, this will be better reflected in our technology, and everything it can do. "We're moving towards a new paradigm for computation," quantum information scientist Michele Mosca, who's based at the Institute for Quantum Computing at the University of Waterloo, recently told me. He compared this shift in thinking to when humanity abandoned the flat Earth hypothesis and accepted that our world is round... In a public lecture delivered on Wednesday from the Perimeter Institute for Theoretical Physics, Mosca will describe the "new quantum era" and the promises and challenges it brings. Take, for example, public key cryptography that is used to protect secret communications around the world. When the first true quantum computer powers up, maybe a decade from now, it's predicted that it will be able to crack this type of encryption, no problem. Mosca has been urging governments and corporations to start planning for this. Mosca's talk, which begins at 7 pm E.S.T., will be livestreamed here on Motherboard. [Motherboard](#)

Terror groups likely to be first to unleash cyber weapons, says Eugene Kaspersky

Terror groups, not nation states, are the most likely to unleash devastating cyber weapons, according to Eugene Kaspersky, chief executive and co-founder of security firm Kaspersky Lab... Unlike traditional weapons, cyber weapons can be reverse engineered, improved and used on those who developed them, so nation states are unlikely to use them on each other. "But I am really afraid some terrorist group will pay cyber criminals to develop and deploy such weapons on their behalf," he said, noting that some cyber criminals work like mercenaries, providing cyber crime services to anyone who is willing to pay. Kaspersky said cyber weapons are likely to fall in one of three categories: those aimed at causing physical damage, destroying critical data and telecommunications... Critical infrastructure is the most "problematic" and probably the "scariest" area, he said, because cyber criminals are well-resourced and can attack even well-protected networks... According to Kaspersky, the vast majority (384 million) of malicious files detected are aimed at Windows, compared with Android (18 million) and Mac OS (30,000). [Computer Weekly](#); [SC Magazine](#)

Canada's National Security Consultation I: Digital Anonymity & Subscriber Identification Revisited... Yet Again

An opinion piece states, "Last month, Public Safety Canada followed through on commitments to review and consult on Canada's national security framework. The process reviews powers that were passed into law following the passage of Bill C-51, Canada's recent controversial anti-terrorism overhaul, as well as invite a broader debate about Canada's security apparatus. While many consultation processes have explored expansions of Canada's national security framework, the current consultation constitutes the first modern day attempt to explore Canada's national security excesses and deficiencies. Unfortunately, the framing of the consultation demonstrates minimal direct regard for privacy and civil liberties because it is primarily preoccupied with defending the existing security framework while introducing a range of additional intrusive powers..." [CIPPIC](#)

The Canadian Government's Plan to Sell New Spying Powers to Citizens

Canada's government is taking a forum for citizens to sound off about its spying powers and flipping it into an opportunity to sell Canadians on new and overbroad police capabilities, according to a new watchdog report. In September, Trudeau's Liberals made good on a promise to open a public consultation on national security and released two documents, a green paper and a background document, explaining the issues at stake to Canadians at a time when the government is ramping up its efforts to thwart domestic terrorists. These included hot topics such as the difficulties police face when dealing with encrypted devices and issues surrounding data retention. However, according to the watchdog report, the government's framing of the issues is selling Canadians on a police power that has been shot down again and again by the courts and the public: warrantless access to subscriber information from telecom companies. "Successive federal governments have sought to legislatively enshrine a state power to access subscriber identification data from telecommunications companies," Citizen Lab researcher Christopher Parsons and Canadian Internet Policy and Public Interest Clinic staff lawyer Tamir Israel write in their report. "Such legislative initiatives would have facilitated access to such data on an indiscriminate basis and without any judicial authorization or control." "All of these attempts have proven controversial and each has fallen in the face of public resistance," they continue. In 2014, the Supreme Court of Canada ruled that accessing subscriber information without a warrant constitutes an illegal search. In its green paper, the government describes subscriber information as being akin to a phone book. However, subscriber information includes IP addresses, name, home address, phone number, email address, and mobile devices' IMSI number—much more information than is contained in your average phone book. "Our laws on how information can be properly collected and then used in court as evidence were mostly written before the rapid pace of new technology became a consideration," the government's green paper states. Now, police worry about "slow and inconsistent access to basic subscriber information to help identify who was using a particular communications service at a particular time," the report states. [Motherboard](#); [Boing Boing](#)

Canadian government re-opens privacy debate on access to telecom subscriber info

The Canadian government has revived a discussion on a particularly controversial privacy topic: how much access law enforcement should have to telecom subscriber information in the name of public safety. In September 2016 the government opened a public consultation on national security, releasing a 'green paper' and background document that details issues, challenges and general questions surrounding national security threats like domestic terrorism. Many

topics are covered in the documents, but there's one in particular that may sound familiar to Canadians: the issue of warrantless access to subscriber information from telecom companies. Michael Geist, Canada research chair in internet and e-commerce law at the University of Ottawa, states in an article for The Globe and Mail that the government has been pushing for easier access to carrier data since the early 2000s, with the initiative seeing setbacks such as the defeat of Bill C-30. Lawful access legislation eventually passed in 2014, resembling something near a compromise between consumer and government interests. Warrant-less disclosure of information and government surveillance capabilities for telecoms were nixed, but the legislation also eliminated liability concerns for Internet service providers (ISPs) that voluntarily disclose basic information and gave the police new powers to require access to digital data. The above-mentioned public consultation — started by Public Safety Minister Ralph Goodale — has put the issue back up for debate, however. “The Public Safety consultation skips over the years of lawful access debate by putting everything back on the table,” writes Geist, “acknowledging that the law was updated less than 24 months ago but suggesting that more change may be needed.” As for the Minister's thoughts on the matter, a spokesperson stated to Motherboard: “*While both basic subscriber information (BSI) and a phone book can both be used to identify someone, BSI requires safeguards because some of it can reveal intimate details of a person's activities when linked to other information. That principle has been affirmed by the courts. The government is committed to protecting both Canadians' safety and their rights, including their privacy rights.*” The spokesperson added that the green paper was meant to “*provoke discussion.*” The public consultation remains open until December 1st, 2016 and can be accessed here if you'd like to add your voice to the conversation. MobileSyrup.com

Russian special services to decrypt internet traffic

The Russian Federal Security Service (FSS, or FSB) together with the country's Ministry of Communications, are introducing a set of technical procedures that will provide it with unencrypted access to the Internet traffic of all Russian citizens. This move is the implementation of the recently approved Yarovaya Law, (a package of bills which amended a pre-existing counter-terrorism law as well as separate laws regulating counter-terror and public safety measures), which obliged local and global IT companies, operating in Russia, including Google, "Yandex", Mail.ru Group, Whatsapp, Telegram, Viber, Facebook, "VKontakte" to provide encryption keys for their web-servers at the request of the FSB. [SC Magazine](#)

Yahoo email scanning: Apple, Google, Microsoft say they'd fight similar requests in court

Yahoo is facing increased scrutiny after being accused of secretly building a custom software program to search all of its customers' incoming emails at the request of the U.S. government (...) Yahoo has neither confirmed nor denied the report. In a statement to Reuters a company spokesperson said, “Yahoo is a law abiding company, and complies with the laws of the United States.” It's still unclear whether the alleged software searched only U.S. citizens' emails, or if Canadian users were also impacted (...) While Microsoft declined to comment on whether it had ever received a similar request, the company said it has “never engaged in the secret scanning of email traffic.” Facebook and Twitter both said they had not received similar requests and noted that if they did they would oppose them in court. Apple, which fought a U.S. government order to hack an iPhone belonging to one of the San Bernardino shooters by creating custom software, maintained that it would fight these types of requests in court. [Global News](#)

Facebook Marketplace launches, selling guns, drugs and baby hedgehogs

Facebook's Marketplace has immediately been flooded with people selling guns, drugs and baby hedgehogs. The company has been forced to apologise after its brand new feature — intended to let people sell things in the same way as they would through Ebay or Craigslist — has already been flooded with illegal items, those that break rules, and others that are just odd. As well as offering illegal items like drugs, some users appeared to be selling things that are banned by Facebook's own terms, like snakes and hedgehogs. [Independent \(UK\)](#)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.

Sent to: !Cyber Security Media Summary Dist List #1; !Cyber Security Media Summary Dist List #2; !Cyber Security Media Summary Dist List #3; !Cyber Security Media Summary Dist List #4

**Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
October 6, 2016 / le 6 octobre 2016**

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse quotidienne
peut également être accédée via [InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS |
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRE

INTERNATIONAL

MINISTER / MINISTRE

RCMP to settle suits: Sources

The RCMP commissioner is expected to issue an apology on Thursday as part of a historic settlement reached with the plaintiffs in two proposed class-action lawsuits alleging systemic gender-based harassment and discrimination within the force, sources say. Any female member who experienced harassment or discrimination will be eligible to apply for damages. Amounts will depend on the injuries, a source said. The potential number of Mounties who could be eligible is in the thousands and compensation could potentially reach as much as \$100 million. As part of the settlement, the force will announce new details of how it plans to change its workplace culture. Reaching a settlement is a significant event, said Angela Workman-Stark, a former RCMP chief superintendent who played a key

role in helping the force address harassment and bullying. "For the women, it's a resolution for them. I think it's an acknowledgment of the issues they brought forward. I think it's great for the organization to move forward and take responsibility. Resolution and recognition is an important piece," said Workman-Stark, who left the force earlier this year. Thursday's announcement will take place at 11 a.m. ET in Ottawa. Bob Paulson, the commissioner, and **Public Safety Minister Ralph Goodale** will be joined by the lead plaintiffs in the proposed class-action lawsuits, Janet Merlo and Linda Gillis Davidson. National Post, A1 (Windsor Star, Leader-Post, London Free Press, The Province, Edmonton Journal, Montreal Gazette, Vancouver Sun, Calgary Herald, StarPhoenix, Ottawa Citizen); Globe and Mail; Canadian Press (680 News); * La Presse Canadienne (L'actualité); La Presse+; Le Journal de Montréal (Le Journal de Québec); Toronto Star; * Global News; The Hill Times; iPolitics; * Ottawa Citizen

Espionage bill will allow PM to muzzle watchdog, report says

Canada's new spy-accountability legislation will create a parliamentary watchdog that prime ministers can keep on a short leash, or even muzzle, a report on the bill by the Library of Parliament says. The Liberal government has said the national-security legislation will create an independent committee of MPs that will have regular briefings from government spy agencies on their activities. However, a report on Bill C-22 suggests the national security and intelligence committee of parliamentarians could end up "in effect, accountable to the Prime Minister alone." The report, done by the nonpartisan Library of Parliament and released this week, is a synopsis of the bill for parliamentarians. Such reports are among the information services the staff of the library provide to MPs and senators. The Library of Parliament's report points out that the bill would allow prime ministers and cabinet to shape, block or censor the committee's work. This hits a decidedly different tone from an essay published this week by **Public Safety Minister Ralph Goodale**, who said Bill C-22 creates a committee that "will set its own agenda and report when it sees fit. Every democracy has to determine how far legislators should be able to go to act as a check on government spies, who typically work under secret orders from presidents and prime ministers. Canada gives its elected politicians less information about and fewer review powers over the security agencies than most governments do. And, unlike its closest allies, Canada has not cleared any parliamentarians to hear state secrets. Under C-22, that would change. Globe and Mail, A1

*** Canadian government re-opens privacy debate on access to telecom subscriber info**

The Canadian government has revived a discussion on a particularly controversial privacy topic: how much access law enforcement should have to telecom subscriber information in the name of public safety. In September 2016 the government opened a public consultation on national security, releasing a 'green paper' and background document that details issues, challenges and general questions surrounding national security threats like domestic terrorism. Many topics are covered in the documents, but there's one in particular that may sound familiar to Canadians: the issue of warrantless access to subscriber information from telecom companies. Michael Geist, Canada research chair in internet and e-commerce law at the University of Ottawa, states in an article for The Globe and Mail that the government has been pushing for easier access to carrier data since the early 2000s, with the initiative seeing setbacks such as the defeat of Bill C-30. Lawful access legislation eventually passed in 2014, resembling something near a compromise between consumer and government interests. Warrant-less disclosure of information and government surveillance capabilities for telecoms were nixed, but the legislation also eliminated liability concerns for Internet service providers (ISPs) that voluntarily disclose basic information and gave the police new powers to require access to digital data. The above-mentioned public consultation — started by **Public Safety Minister Ralph Goodale** — has put the issue back up for debate, however. "The Public Safety consultation skips over the years of lawful access debate by putting everything back on the table," writes Geist, "acknowledging that the law was updated less than 24 months ago but suggesting that more change may be needed." As for **the Minister's** thoughts on the matter, a spokesperson stated to Motherboard: ***"While both basic subscriber information (BSI) and a phone book can both be used to identify someone, BSI requires safeguards because some of it can reveal intimate details of a person's activities when linked to other information. That principle has been affirmed by the courts. The government is committed to protecting both Canadians' safety and their rights, including their privacy rights."*** The spokesperson added that the green paper was meant to ***"provoke discussion."*** The public consultation remains open until December 1st, 2016 and can be accessed here if you'd like to add your voice to the conversation. MobileSyrup.com

Today's News / Actualités
November 16, 2016 / le 16 novembre 2016
08:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 08h00 et 14h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS /
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

Confidentialité des sources: des journalistes réclament une loi fédérale

Le premier ministre Justin Trudeau, qui s'est présenté comme un défenseur de la liberté de la presse, doit joindre la parole aux actes et légiférer afin de protéger les sources confidentielles des journalistes. C'est ce qu'ont réclamé mercredi en conférence de presse au parlement trois journalistes qui ont vu cette liberté entravée, Patrick Lagacé, Ben Makuch et Mohammed Fahmy, ainsi que le directeur exécutif de Journalistes canadiens pour la liberté d'expression (CJFE), Tom Henheffer. Ils ont exhorté le gouvernement à déposer un projet de loi pour protéger les sources, à revoir la façon dont les mandats de

BCSARA

Update on Announced Funding for SAR in BC [http://www.bcsara.com/2016/11/update-on-announced-funding-for-sar-in-bc/...](http://www.bcsara.com/2016/11/update-on-announced-funding-for-sar-in-bc/)

Nova Scotia EMO

Storm surge warnings in place for Digby & Yarmouth counties. Higher than normal water levels & large waves expected. [http://weather.gc.ca/warnings/index_e.html...](http://weather.gc.ca/warnings/index_e.html)

Naomi Yamamoto

Free Disaster Response Workshop. Nov 16, 7-9:30pm [@NorthShoreEMO](#) [@CityOfNorthVan](#) <http://bit.ly/2fQLK9k> [#beprepared](#)

IBC West

[#FortMcMurray](#) [#ymmfire](#) [#wildfire](#) recovery to spur \$5.3B in spending: report [http://herald.ca/ubC#.WCyMRGXBCiO.twitter...](http://herald.ca/ubC#.WCyMRGXBCiO.twitter) via [@chronicleherald](#) [@ibickis](#) [@WBEcDev](#)

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Christopher Parsons

AND Canada's is currently having a national security consult ON EACH OF THESE POINTS. How can CBC/RCMP claim 'conversation' not happening?!

The Muslim Lawyer

Less than a month left to provide your input. Canadians should worry more about Bill C51 than Trump. Please...

NATIONAL SECURITY / SÉCURITÉ NATIONALE

CBC News

RCMP Commissioner Bob Paulson 'consumed' with 'inability' to investigate in digital world <http://www.cbc.ca/1.3851955>

CBC Nova Scotia

RCMP Commissioner Bob Paulson 'consumed' with 'inability' to investigate in digital world

Christopher Parsons

Pleading the Case: How the RCMP Fails to Justify Calls for New Investigatory Powers christopher-parsons.com/pleading-the-c...

Christopher Parsons

I have a hard time believing that the CBC is just reproducing the RCMP's own documents, with no 3rd party analysis, as facts on the ground

Christopher Parsons

Absent in CBC/TorStar pieces is the RCMP GOT a raft of lawful access powers just a few years ago. Not everything. Now they're back for rest

PACC

The argument for/against law enforcement gaining greater investigatory powers: what's at stake christopher-parsons.com/pleading-the-c... [#privacy](#) [#security](#)

Open Media

Another privacy scandal strikes Canada: RCMP used data from police + social media to track down Aboriginal activists ow.ly/v888306eBaL

ishmael n. daro

RCMP lobbying federal government for more surveillance powers, including warrantless access to subscriber info on.thestar.com/2fg2cij

Nora Loreto



**Federal-Provincial-Territorial meeting of Ministers responsible
for Justice and Public Safety**

**Réunion des ministres responsables de la Justice et de la Sécurité publique
à l'échelon fédéral, provincial et territorial
October 1, 2015 – October 10, 2016**



Table of Contents / Table des matières



[Criminal justice system review / Révision du système de justice pénale](#)

[Cyber security consultations / Consultations sur la cybersécurité](#)

[Countering radicalization / Lutte contre la radicalisation](#)

[Violence against Indigenous women and girls / Violence faite aux femmes et filles autochtones](#)

[Canadian Police Information Centre / Centre d'information de la police canadienne](#)

Criminal justice system review / Révision du système de justice pénale

Overview / Vue d'ensemble

The coverage was varied based on the topics of interest from October 1, 2015 to October 10, 2016. Criminal justice review in general generated little coverage, with specific aspects of the review mandated to the Minister of Justice in November 2015 being covered on their own as well as a number of different key issues related to the criminal justice system coming to prominence through a variety of outlets.

The coverage on the issue of criminal record suspensions and the potential reintroduction of pardons spiked in late January 2016, in the wake of a CBC interview with Public Safety Minister Ralph Goodale. The Minister vowed to revisit and revise the Criminal Records Act. The media also reported that the Parole Board of Canada launched an online consultation asking the public their opinion on the current application charge of \$631 for a criminal pardon.

The question of warrantless access to basic online subscriber information gained prominence, in November and December 2015, when the Canadian Press and several other outlets reported that RCMP Commissioner Bob Paulson stated his desire to have police access to this information. Privacy Commissioner Daniel Therrien's response in mid-December also was widely reported, where he stated that he could see the possibility of allowing said access without overly compromising Canadians' privacy, later urged caution in a January editorial in the Toronto Star. In April 2016, media coverage on the issue was extensive, catalyzed by the revelation that the RCMP had used a key to decrypt and unlock PIN-to-PIN messages between personal BlackBerry users. This revelation generated extensive media coverage lamenting privacy concerns about lawful access. The broader issue of lawful access to private electronic information continued to receive coverage throughout the year and was an element of the national security consultations launched in September 2016.

Today's News / Actualités
November 23, 2016 / le 23 novembre 2016
08:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 08h00 et 14h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS |
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

Corrections brings in third party to investigate sexual recordings at Edmonton Institution

Canada's **minister of public safety** is calling on authorities to thoroughly investigate and put an end to alleged harassment at Edmonton's federal prison, and his office says part of the investigation will be handled by a third party. **Ralph Goodale's** response comes after a CBC report released Tuesday that outlined fears from corrections staff over sexually explicit phone conversations between male prison guards at work. Whistleblower employee sources say an intelligence worker wanted to figure out why inmates' multiple calls for help on a cell buzzer system were missed, and noticed some guards were on

Colin Freeze

The relationship between a journalist & source is sacrosanct, according to a [#cdnpoli](#) Senator who wants it in law. <https://t.co/o02Tdqlbl2>

Colin Freeze

Former [#CSIS](#) boss Dick Fadden telling [#cdnpoli](#) [#secu](#) that "time has come" for [#c22](#) committee. So long as it is "review" not "oversight."

OccupyToronto

"Other security agencies may take the same view that led CSIS to illegally keep data for almost a decade." <https://www.thestar.com/news/canada/2016/11/22/more-rules-around-spies-information-sharing-needed-privacy-commissioner.html> ... [#cdnpoli](#)

globeandmail

New scanner technology could reduce need for unpacking at airport security <http://trib.al/za0y1St>. From [@globetechnology](#)

StephanieCarvin

At a [@uOttawaCIPS](#) event with [@NewmanRobinson](#) & CSE ADMPOL Rochon, latter acknowledges CSE must do a better job of communication to public.

StephanieCarvin

Rochon says that he also wants to talk about threats to Canada. But our intel agencies are also pretty terrible at that too.

StephanieCarvin

Rochon says [@cse_cst](#) is opposed to "back doors" on cyber-encryption because cyber security is so important.

StephanieCarvin

Rochon differentiates between "lawful access" in the Spencer decision as having more of an impact on RCMP than CSE.

StephanieCarvin

[@cforcese](#) asked about under what circumstances CSIS and RCMP can get access to metadata. If I understand the question/answer correctly...

StephanieCarvin

Rochon replies some kind of legal "authority" is required, but not necessarily a warrant.

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

The Globe and Mail

Whether TPP or NAFTA, Canada needs to walk a careful line <http://trib.al/uzZ7L9A>. From [@GlobeBusiness](#)

CYBER SECURITY / CYBERSÉCURITÉ

alexboitillier

Journos (and everybody, really): Take security seriously.

LAW ENFORCEMENT / APPLICATION DE LA LOI

CACP ACCP

[#CACP](#) Board of Directors meeting to discuss the many issues facing policing. MJ legalization, fentanyl, [#MMIW](#), cybercrime just to name a few

chintapuxley

Man accused of shooting Colten Boushie on Saskatchewan farm facing more charges. Story via [@CdnPress](#)

Today's News / Actualités
November 29, 2016 / le 29 novembre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS |
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

Inside the RCMP's plan for a 'new public narrative' on cyber surveillance

A four-page memo obtained by VICE News sheds light on how the Royal Canadian Mounted Police intends to lobby the public for new surveillance powers. As the Trudeau government contemplates new powers for the federal police force, the documents call for the RCMP to push for "the creation of a new public narrative around why police need judicially authorized and timely access to online information." The memo was prepared by the RCMP in advance of a February meeting in Washington, D.C., where **Public Safety Minister Ralph Goodale** sat down with his American, British, Australian, and New Zealand

counterparts in the Five Eyes intelligence partnership. "Foremost, the problem must be articulated in terms of its impact on safety and the economic well-being of individuals and businesses," the memo, obtained through an access to information request, states. "This will require messaging that aims to re-establish the importance of balancing community safety needs with online privacy and anonymity expectations." The memo lists four perceived problems where the RCMP want to push this "new public narrative" — a lack of interception hardware on Canadian telecommunication networks, the use of encryption to protect communications, the deletion of user data by companies, and the inability to obtain users' data hosted in some foreign countries. **All four of these issues later showed up in national security consultations set up by the Liberal government, spearheaded by Minister Goodale. Those consultations will inform new anti-terrorism legislation expected in the new year...** "It will be important for the Public Safety Portfolio to reframe 'lawful access' as broader 'going dark' digital evidence challenges," the February memo reads. The Public Safety Portfolio includes everyone from **Minister Ralph Goodale** to the Canadian Security Intelligence Service and the Canadian Border Services Agency. **Minister Goodale** has, himself, been using the rhetorical device of "going dark" more and more lately. It has also been a catchphrase that FBI Director James Comey has employed liberally in recent years... **A request sent to Minister Goodale's office about the nature of the memo, and on whether his office signed off on this new public relations plan, went unanswered.** The last time these powers were on the table, under the guise of Bill C-30 and "lawful access," it was met with widespread backlash. That legislation would have given police warrantless access to internet users' personal data, required telecommunications companies to install interception powers on their networks, and would have forced companies to decrypt information on their networks. The RCMP has put those powers back on the table, and **Goodale's national security consultations have raised the spectre of re-writing those proposals into law.** Vice News

No way to tell if border plan helps: auditor

The federal spending watchdog says the government has no way of telling whether its billion-dollar border plan is improving security or helping to speed the flow of goods and people between Canada and the United States. While departments and agencies completed many commitments of the high-profile Beyond the Border plan, they faced numerous challenges and lacked the means to measure results, auditor general Michael Ferguson said in a report released Tuesday. In addition, Ferguson found the government's own evaluation, made public in September, painted an "incomplete and inaccurate" picture... He urged a number of federal agencies to develop indicators so they can fully assess efforts involving everything from checked baggage screening to so-called trusted-trader programs... **Public Safety Minister Ralph Goodale said the government is "very determined" to get effective measurement systems in place.** Canadian Press (The Record)

New indigenous elders council to advise Ontario on justice issues

A new elders council that will offer advice to Ontario's attorney general should help make the justice system more responsive to the aboriginal population, the provincial government said Tuesday. The announcement came on a day the federal auditor general in his annual report criticized correctional authorities for failing aboriginal inmates. In announcing the council, Ontario's Indigenous Relations Minister David Zimmer acknowledged the long-standing concern about the over-representation of indigenous peoples in the criminal justice system... In Ottawa Tuesday, Auditor General Michael Ferguson found Correctional Service Canada was failing to provide timely rehabilitation programs for indigenous offenders and that relatively few of them were released on parole — a situation he called "beyond unacceptable"... Ferguson faulted the prison system for failing to take into account aboriginal social history factors, including the lingering trauma inflicted by the Indian residential school system, poverty and substance abuse. **Public Safety Minister Ralph Goodale** responded that the federal Liberal government wanted to improve the situation. **"Our government is seized with the issue of over-representation of indigenous persons in the correctional system," Goodale said.** Canadian Press (Times-Colonist; Prince George Citizen)

Biden to meet with Trudeau in Ottawa to discuss Canada-U.S. ties

U.S. Vice-President Joe Biden will visit Ottawa next week to meet with Prime Minister Justin Trudeau and the country's premiers will discuss the Canada-U.S. relationship before the Trump administration takes over early next year. Mr. Biden is scheduled to visit Ottawa on Dec. 8 and 9 to meet with Mr. Trudeau and

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Tuesday, November 29, 2016 4:13 PM
To: Today's News / Actualités (PS/SP)
Subject: Vice News: Inside the RCMP's plan for a 'new public narrative' on cyber surveillance (Minister mentioned)

Inside the RCMP's plan for a 'new public narrative' on cyber surveillance

Vice News

Justin Ling
2016-11-29

A four-page memo obtained by VICE News sheds light on how the Royal Canadian Mounted Police intends to lobby the public for new surveillance powers.

As the Trudeau government contemplates new powers for the federal police force, the documents call for the RCMP to push for "the creation of a new public narrative around why police need judicially authorized and timely access to online information."

The memo was prepared by the RCMP in advance of a February meeting in Washington, D.C., where **Public Safety Minister Ralph Goodale** sat down with his American, British, Australian, and New Zealand counterparts in the Five Eyes intelligence partnership.

"Foremost, the problem must be articulated in terms of its impact on safety and the economic well-being of individuals and businesses," the memo, obtained through an access to information request, states. "This will require messaging that aims to re-establish the importance of balancing community safety needs with online privacy and anonymity expectations."

The memo lists four perceived problems where the RCMP want to push this "new public narrative" — a lack of interception hardware on Canadian telecommunication networks, the use of encryption to protect communications, the deletion of user data by companies, and the inability to obtain users' data hosted in some foreign countries.

All four of these issues later showed up in national security consultations set up by the Liberal government, spearheaded by Minister Goodale. Those consultations will inform new anti-terrorism legislation expected in the new year.

These documents clearly lay out how the RCMP intends to frame the public debate, and exactly which issues they intend on pursuing, but — even internally — the RCMP has remained vague over what legal powers they are actually seeking.

Legal powers to compel decryption and mandate interception have been proposed before, but they were shelved by the previous government because they could undercut Canadians' privacy, civil liberties, and the right to be free of self-incrimination, or because they could weaken cyber-security at Canada's major telecommunications industries.

The previous Canadian government tried to sell to the public mandatory decryption powers and more expansive communication interception technology in Bill C-30, in 2012. Then-Public Safety Minister Vic Toews employed the euphemistic tagline of "lawful access," only to have that phrase pick up negative connotation as public opinion turned against many of those legislative proposals. The bill was later shelved and, ultimately, killed.

The RCMP is not looking to make the same mistake.

"It will be important for the Public Safety Portfolio to reframe 'lawful access' as broader 'going dark' digital evidence challenges," the February memo reads. The Public Safety Portfolio includes everyone from **Minister Ralph Goodale** to the Canadian Security Intelligence Service and the Canadian Border Services Agency.

Minister Goodale has, himself, been using the rhetorical device of "going dark" more and more lately. It has also been a catchphrase that FBI Director James Comey has employed liberally in recent years.

The RCMP underscores: "This will need to be supported by evidence of the impacts on police operations of the various digital evidence challenges."

The RCMP had a chance to lay out its public relations case around "going dark" when it partnered with the CBC and Toronto Star for a five-part series that sought to showcase ten cases where the federal police's investigations were thwarted by technological shortfalls.

One graphic provided to the CBC, which purports to show that Canada lags behind the rest of its Five Eyes partners when it comes to "investigative capability," is also included in the documents obtained by VICE News.

But the memo obtained by VICE News was not just an overview. It proposed a new communications and partnership plan for the police agency.

"It is recommended that you actively support action towards further senior-level engagement of [technology service providers], other IT industry partners, and privacy-related academics by the Five Eyes partner countries as such," the memo, addressed to an unnamed official, reads.

When asked by VICE News what that outreach entailed, an RCMP spokesperson said in an email: "The RCMP has been attending conferences and working with partners on developing solutions for going dark. The main point of highlighting some of the challenges to law enforcement on Going Dark has been to educate the public and open public debate in order to arrive at solutions to combat the issue of cybercrime."

A request sent to Minister Goodale's office about the nature of the memo, and on whether his office signed off on this new public relations plan, went unanswered.

The last time these powers were on the table, under the guise of Bill C-30 and "lawful access," it was met with widespread backlash.

That legislation would have given police warrantless access to internet users' personal data, required telecommunications companies to install interception powers on their networks, and would have forced companies to decrypt information on their networks. The RCMP has put those powers back on the table, and **Goodale's national security consultations have raised the spectre of re-writing those proposals into law.**

Christopher Parsons, managing director of the Telecom Transparency Project and a research associate with the Citizen Lab in the Munk School, says the documents expose some of the vagueness in this public relations campaign from the RCMP.

"I think you have to sort of squint and peer at it through foggy glasses for it to appear accurate," Parsons told VICE News.

Parsons does say that the police force has effectively launched a broad discussion about these perceived legal and policing problems, but are not offering clear arguments for the powers they are seeking.

"What they're saying is: There's this new technology and it's creating some real problems, but it doesn't seem clear to me that they're saying: here's how we're going to roll back the clock."

Sent to: !!INTERNAL; !!INTERNAL 2; RCMP Breaking News

Lauzon, Adam (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Tuesday, November 29, 2016 4:13 PM
To: Today's News / Actualités (PS/SP)
Subject: Vice News: Inside the RCMP's plan for a 'new public narrative' on cyber surveillance (Minister mentioned)

Inside the RCMP's plan for a 'new public narrative' on cyber surveillance

Vice News
Justin Ling
2016-11-29

A four-page memo obtained by VICE News sheds light on how the Royal Canadian Mounted Police intends to lobby the public for new surveillance powers.

As the Trudeau government contemplates new powers for the federal police force, the documents call for the RCMP to push for “the creation of a new public narrative around why police need judicially authorized and timely access to online information.”

The memo was prepared by the RCMP in advance of a February meeting in Washington, D.C., where **Public Safety Minister Ralph Goodale** sat down with his American, British, Australian, and New Zealand counterparts in the Five Eyes intelligence partnership.

“Foremost, the problem must be articulated in terms of its impact on safety and the economic well-being of individuals and businesses,” the memo, obtained through an access to information request, states. “This will require messaging that aims to re-establish the importance of balancing community safety needs with online privacy and anonymity expectations.”

The memo lists four perceived problems where the RCMP want to push this “new public narrative” — a lack of interception hardware on Canadian telecommunication networks, the use of encryption to protect communications, the deletion of user data by companies, and the inability to obtain users’ data hosted in some foreign countries.

All four of these issues later showed up in national security consultations set up by the Liberal government, spearheaded by Minister Goodale. Those consultations will inform new anti-terrorism legislation expected in the new year.

These documents clearly lay out how the RCMP intends to frame the public debate, and exactly which issues they intend on pursuing, but — even internally — the RCMP has remained vague over what legal powers they are actually seeking.

Legal powers to compel decryption and mandate interception have been proposed before, but they were shelved by the previous government because they could undercut Canadians’ privacy, civil liberties, and the right to be free of self-incrimination, or because they could weaken cyber-security at Canada’s major telecommunications industries.

The previous Canadian government tried to sell to the public mandatory decryption powers and more expansive communication interception technology in Bill C-30, in 2012. Then-Public Safety Minister Vic Toews employed the euphemistic tagline of “lawful access,” only to have that phrase pick up negative connotation as public opinion turned against many of those legislative proposals. The bill was later shelved and, ultimately, killed.

The RCMP is not looking to make the same mistake.

“It will be important for the Public Safety Portfolio to reframe ‘lawful access’ as broader ‘going dark’ digital evidence challenges,” the February memo reads. The Public Safety Portfolio includes everyone from **Minister Ralph Goodale** to the Canadian Security Intelligence Service and the Canadian Border Services Agency.

Minister Goodale has, himself, been using the rhetorical device of “going dark” more and more lately. It has also been a catchphrase that FBI Director James Comey has employed liberally in recent years.

The RCMP underscores: “This will need to be supported by evidence of the impacts on police operations of the various digital evidence challenges.”

The RCMP had a chance to lay out its public relations case around “going dark” when it partnered with the CBC and Toronto Star for a five-part series that sought to showcase ten cases where the federal police’s investigations were thwarted by technological shortfalls.

One graphic provided to the CBC, which purports to show that Canada lags behind the rest of its Five Eyes partners when it comes to “investigative capability,” is also included in the documents obtained by VICE News.

But the memo obtained by VICE News was not just an overview. It proposed a new communications and partnership plan for the police agency.

“It is recommended that you actively support action towards further senior-level engagement of [technology service providers], other IT industry partners, and privacy-related academics by the Five Eyes partner countries as such,” the memo, addressed to an unnamed official, reads.

When asked by VICE News what that outreach entailed, an RCMP spokesperson said in an email: “The RCMP has been attending conferences and working with partners on developing solutions for going dark. The main point of highlighting some of the challenges to law enforcement on Going Dark has been to educate the public and open public debate in order to arrive at solutions to combat the issue of cybercrime.”

A request sent to Minister Goodale’s office about the nature of the memo, and on whether his office signed off on this new public relations plan, went unanswered.

The last time these powers were on the table, under the guise of Bill C-30 and “lawful access,” it was met with widespread backlash.

That legislation would have given police warrantless access to internet users’ personal data, required telecommunications companies to install interception powers on their networks, and would have forced companies to decrypt information on their networks. The RCMP has put those powers back on the table, and **Goodale’s national security consultations have raised the spectre of re-writing those proposals into law.**

Christopher Parsons, managing director of the Telecom Transparency Project and a research associate with the Citizen Lab in the Munk School, says the documents expose some of the vagueness in this public relations campaign from the RCMP.

“I think you have to sort of squint and peer at it through foggy glasses for it to appear accurate,” Parsons told VICE News.

Parsons does say that the police force has effectively launched a broad discussion about these perceived legal and policing problems, but are not offering clear arguments for the powers they are seeking.

“What they’re saying is: There’s this new technology and it’s creating some real problems, but it doesn’t seem clear to me that they’re saying: here’s how we’re going to roll back the clock.”

Sent to: !INTERNAL; !INTERNAL 2; RCMP Breaking News

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Wednesday, November 30, 2016 12:22 PM
To: Today's News / Actualités (PS/SP)
Subject: Transcript - CIWW-NEWSTALK 1310 - Ottawa Today - RCMP Plan to Reframe Debate Over Surveillance - 2016-11-30 - 10h20 ET

SOURCE:
CIWW-NEWSTALK 1310

PROGRAM:
OTTAWA TODAY

DATE:
NOVEMBER 30, 2016

TIME:
10H20 ET

LENGTH:
8:00 MINS

SUBJECT:
RCMP PLAN TO REFRAME DEBATE OVER SURVEILLANCE

MARK SUTCLIFFE (Host): We are joined now by Justin Ling, the Canadian features editor at VICE News, who has a story about how the RCMP wants to create a new public narrative around why police need judicially authorized and timely access to online information. This is all about the balance between privacy and following up on terrorist threats and monitoring what people are doing online.

Justin Ling joins us on Ottawa Today. Good morning.

JUSTIN LING (VICE News): Hey, good morning.

SUTCLIFFE: A new public narrative. I guess that means the RCMP wants to convince Canadians that they need these new powers.

LING: Yeah, that's basically it. I mean, these documents that we obtained pretty clearly lay out exactly how the RCMP wants to both lobby the public, lobby government, lobby academia, lobby the telecommunications industry to basically get on side with them on this request for more cyber surveillance powers. It's... it's an interesting document. I mean, in black and white, they're basically saying we need to reframe the debate around lawful access. And if you'll remember lawful access was a favourite buzzword of Vic Toews back when he introduced Bill C-30 which, you know, later got re-branded the 'cyber snooping act' but was originally called the Protecting Canadians from Child Pornographers Act, or something of that ilk. Lawful access was his favourite catchphrase.

Lawful access is now essentially a dirty word in Ottawa. Whenever you say it, it rekindles images of Vic Toews proclaiming: you're either with us or you're with the child pornographers. So the RCMP here is saying, okay, you know, that old rhetoric is not going to work here so what can we say instead? And the new public narrative essentially involves them talking about the problems around going dark, and encryption, and, you know, their inability to obtain certain communications on the Internet. And, you know, their whole philosophy on selling this is to basically go to the public and give them examples of where encryption or, you know, new technology has thwarted their efforts on terrorism or cybercrime or you name it.

And, you know, part of this is well and good, and I imagine there's people out there saying, yeah, that's fine. I mean, you know, the RCMP should have the right to make this case. And that's certainly true to an extent except part of the problem here is that they're being deliberately vague and they're kind of running this shadow campaign. They're not coming out

and actually saying what they want, they're sort of alluding to it and suggesting it and using the media as sort of a conduit to ask for some of these powers. And, you know, I'm not sure that that's the right way they should be going about this.

SUTCLIFFE: I do have some sympathy for the RCMP being put in the position of having to follow up on some threats to the country, national security threats, but at the same time being limited in what it can do. And I'm sure that can be frustrating at times. But obviously there are limits to how far it should be able to go before crossing into the invasion of privacy of many people. So is this... are they... do they want more powers? Do they want the public to have more sympathy for them? What's at the heart of this, ultimately?

LING: Okay, so let's look at one of the specific problems they've identified. And that's the problem of, you know, the perceived problem of encryption. You know, the RCMP have suggested, and not really in black and white said, but they've suggested, that they would like some sort of a lawful authority to force either an individual or a company to decrypt communications that they've obtained that are encrypted. And on paper that sounds fine. On paper a lot of people will say, you know, if you're a drug dealer or a terrorist and you've encrypted all of your text messages or your emails, the RCMP should have the authority to break that encryption.

On paper that makes a lot of sense. But when you actually drill down on it – and this is kind of the disingenuous thing the RCMP is doing -- when you drill down on this, that doesn't make any sense. On the one hand, everybody has the right to be free from self-incrimination. You know, the RCMP can't necessarily, you know, compel you to give over information on yourself. The RCMP can't compel you to talk. They can't force you to take the stand at your own trial. So this is a long-standing legal precedent. The RCMP can't necessarily compel you to give over the password to your entire life. That's nothing they have the authority to do. Our constitution protects you from that.

So, you know, that's one problem. The other problem is that in a lot of cases, companies can't break their own encryption. We saw this a couple of months ago in the San Bernardino case. The FBI wanted Apple to decrypt the iPhone of one of the San Bernardino attackers. Apple came back and said, listen, we don't have the decryption key. We don't make a decryption key for every one of our phones. If we did, that would be a huge cyber security problem. If somebody ever got a hold of that decryption key they could break into every single iPhone in the world. Now that's a problem. There's a reason why these decryption keys don't exist. So if you're going to force companies to build that decryption key, you are completely undercutting your cyber security nationwide, and cyber security experts are basically saying that that's a catastrophic scenario.

Now a couple of months ago VICE News reported that Blackberry had actually given over its global decryption key to the RCMP. That raised a lot of alarm bells amongst a lot of people and, you know, there was a big conversation there about whether or not Blackberry was a company you ought to stay with because they have such apparently such poor cyber security that they would do such a thing.

So, you know, there is a big debate to be had here but I think if the RCMP wants to have it it's incumbent on them to just come out and have that debate. We've seen recently that the RCMP, you know, participated in a long back and forth with the *Toronto Star* and the CBC where they kind of laid out summaries of certain investigations where they were thwarted by encryption or whatever.

SUTCLIFFE: Right.

LING: But they wouldn't get specific there. They didn't actually say, you know, if we had this power we would have solved the case. At no point did that happen. And there is... and every one of those summaries I read, you can sit there and read it and go, there's no solution to this, you know, this is just a reality. If a criminal gets on a plane and flies to North Korea, there's nothing we can do. You know, the solution there is not to invade North Korea or whatever. There's certain barriers to investigations that are just going to exist no matter what. And if we can talk about reasonable ways in which we can kind of work around that, but this sort of... this RCMP campaign of just sort of highlighting the problems and pushing them into the public conversation without having a real conversation about what the solutions are, I think is a problem.

SUTCLIFFE: We're almost out of time but just quickly, before we let you go Justin, they're suggesting that we're far behind some of the other countries in the so-called Five Eyes partnership. Is that true?

LING: Yes and no. So there's this kind of summary that the RCMP provided about what powers exist in New Zealand, and Australia, and the UK, and the USA. So, a lot of the powers – and these are powers of forcing decryption, of retaining communications on certain network servers. Those powers have just got passed in the United Kingdom and they are highly controversial. They are very, very problematic according to a lot of privacy experts. Similarly in Australia and in New Zealand these powers are very new. We don't really know what the ramifications are yet. In the USA... the USA only has a couple of these powers that the RCMP are requesting and they date back to the Patriot Act. We all know that

that is not exactly something that we want to go forward with here in Canada. So they're being a little disingenuous when they highlight these powers. These powers are very new, very controversial, and I don't know that, you know, that they made the case that they deserve them yet.

SUTCLIFFE: All right Justin. Great stuff. Thank you very much for joining us today. Appreciate it.

LING: Thanks for having me.

SUTCLIFFE: Justin Ling is the Canadian features editor at VICE News. You can read his article online.

NOTE: TRANSCRIPTS CANNOT BE SHARED OR TRANSFERRED OUTSIDE OF YOUR DEPARTMENT.

*Questions? Please contact us at PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.
Questions? Veuillez communiquer avec nous au PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca*

Sent to : !!INTERNAL; !!INTERNAL 2; RCMP Breaking News

GRC-RCMP



GENDARMERIE ROYALE DU CANADA / ROYAL CANADIAN MOUNTED POLICE

**Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
November 30, 2016 / le 30 novembre 2016**

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse quotidienne peut également être accédée via [InfoMédia](#)

TOP STORIES / ACTUALITÉS

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

OTHER / AUTRES

TOP STORIES / ACTUALITÉS

Inside the RCMP's plan for a 'new public narrative' on cyber surveillance

A four-page memo obtained by VICE News sheds light on how the Royal Canadian Mounted Police intends to lobby the public for new surveillance powers. As the Trudeau government contemplates new powers for the federal police force, the documents call for the RCMP to push for "the creation of a new public narrative around why police need judicially authorized and timely access to online information." The memo was prepared by the RCMP in advance of a February meeting in Washington, D.C., where Public Safety Minister Ralph Goodale sat down with his American, British, Australian, and New Zealand counterparts in the Five Eyes intelligence partnership. "Foremost, the problem must be articulated in terms of its impact on safety and the economic well-being of individuals and businesses," the memo, obtained through an access to information request, states. "This will require messaging that aims to re-establish the importance of balancing community safety needs with online privacy and anonymity expectations." The memo lists four perceived problems where the RCMP want to push this "new public narrative" — a lack of interception hardware on Canadian telecommunication networks, the use of encryption to protect communications, the deletion of user data by companies, and the inability to obtain users' data hosted in some foreign countries. All four of these issues later showed up in national security consultations set up by the Liberal government, spearheaded by Minister Goodale. Those consultations will inform new anti-terrorism legislation expected in the new year... "It will be important for the Public Safety Portfolio to reframe 'lawful access' as broader 'going dark' digital evidence challenges," the February memo reads. The Public Safety Portfolio includes everyone from Minister Ralph Goodale to the Canadian Security Intelligence Service and the Canadian Border Services Agency. Minister Goodale has,

himself, been using the rhetorical device of “going dark” more and more lately. It has also been a catchphrase that FBI Director James Comey has employed liberally in recent years... A request sent to Minister Goodale’s office about the nature of the memo, and on whether his office signed off on this new public relations plan, went unanswered. The last time these powers were on the table, under the guise of Bill C-30 and “lawful access,” it was met with widespread backlash. That legislation would have given police warrantless access to internet users’ personal data, required telecommunications companies to install interception powers on their networks, and would have forced companies to decrypt information on their networks. The RCMP has put those powers back on the table, and Goodale’s national security consultations have raised the spectre of re-writing those proposals into law. [Vice News](#) (2016-11-29)

Canada’s Police Allowed Journalists to ‘Embed’ to Argue For More Surveillance

Police in Canada have been making their case in the media for greater powers to crack encryption and other digital privacy measures, which they say are increasingly stymying investigations into criminal activities online. To demonstrate the need for expanded powers, federal police recently gave “unprecedented access” to two of the country’s biggest media outlets. The RCMP allowed journalists from the *Toronto Star* and the CBC to access 10 “top secret” case files, which were essentially vetted summaries prepared by police, intended to illustrate the roadblocks that investigators say they are coming up against. The CBC/*Star* five-part investigative series, which was published in November, sparked widespread debate about police powers and privacy online. In *Motherboard*, critics accused the police of using the media to spark “moral panic” about encryption. Talk from RCMP officials about “going dark” mirrors language used by the FBI in the US, which has had its own debate about these issues going back for years. Canada is in the midst of a public consultation on a green paper on national security that highlights four proposals, including one that would give police “warrantless access” to Canadians’ basic internet subscriber information. Police argue that they need expanded digital powers to keep us all safe from crime. Privacy advocates, on the other hand, say that the police already have wide-ranging capabilities to surveil Canadians, maybe more now than than ever. And encryption, of course, isn’t just used by criminal. [Motherboard](#) (2016-11-29)

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

Update: Bust nets drugs, weapons and cash

You could smell the room before you walked into it. RNC and RCMP police officers with the Combined Forces Special Enforcement Unit spoke to reporters Tuesday afternoon about what they say is a significant drug bust, and displayed the drugs — four kilograms of cocaine, up to 30 pounds of marijuana, a kilogram of hash and 100 oxycodone pills, with a total street value of about \$750,000 — on a table. Other items seized by police were also on display, including \$340,000 in Canadian cash, two guns, bear spray, and an aluminum baseball bat with five blades from a utility knife taped to the end. “We believe this is going to make a significant impact,” said Supt. Marlene Jesso, officer in charge of the unit. “We believe they’ve been operating for quite a long time now, so we think it will definitely put a dent in it for a while, for sure.” [The Telegram](#) (*Western Star*) (2016-11-30); [CBC News](#); [VOCM](#) (2016-11-29)

Gang 'ego' behind recent violence

The bullets are flying, and a string of recent shootings in the **Winnipeg** area - including three in as many days- are believed to be the result of rising tensions within the criminal underworld over lucrative drug turf and profits. Six people have been shot in less than two weeks, one of them fatally. No arrests have been made in any of the attacks. “Various microcosms are becoming more brazen. The proliferation of handguns in our gang members’ hands has been there a long time. They seem more apt to use them now as opposed to just showing or flashing for threats and intimidation,” a veteran police officer told the *Free Press* Tuesday. His name isn’t being published because he is not authorized to speak on the issue. (...) RCMP are investigating the case, which occurred on Raleigh Street in East St. Paul. The victims were listed in stable condition. RCMP said Tuesday the incident was not random and they are looking for information on a light-coloured, four-door sedan seen leaving the area around 6:15 a.m. Monday with the headlights off. Three men were believed to be inside. [Winnipeg Free Press](#), B1

Lauzon, Adam (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Wednesday, November 30, 2016 12:22 PM
To: Today's News / Actualités (PS/SP)
Subject: Transcript - CIWW-NEWSTALK 1310 - Ottawa Today - RCMP Plan to Reframe Debate Over Surveillance - 2016-11-30 - 10h20 ET

SOURCE:
CIWW-NEWSTALK 1310

PROGRAM:
OTTAWA TODAY

DATE:
NOVEMBER 30, 2016

TIME:
10H20 ET

LENGTH:
8:00 MINS

SUBJECT:
RCMP PLAN TO REFRAME DEBATE OVER SURVEILLANCE

MARK SUTCLIFFE (Host): We are joined now by Justin Ling, the Canadian features editor at VICE News, who has a story about how the RCMP wants to create a new public narrative around why police need judicially authorized and timely access to online information. This is all about the balance between privacy and following up on terrorist threats and monitoring what people are doing online.
Justin Ling joins us on Ottawa Today. Good morning.

JUSTIN LING (VICE News): Hey, good morning.

SUTCLIFFE: A new public narrative. I guess that means the RCMP wants to convince Canadians that they need these new powers.

LING: Yeah, that's basically it. I mean, these documents that we obtained pretty clearly lay out exactly how the RCMP wants to both lobby the public, lobby government, lobby academia, lobby the telecommunications industry to basically get on side with them on this request for more cyber surveillance powers. It's... it's an interesting document. I mean, in black and white, they're basically saying we need to reframe the debate around lawful access. And if you'll remember lawful access was a favourite buzzword of Vic Toews back when he introduced Bill C-30 which, you know, later got re-branded the 'cyber snooping act' but was originally called the Protecting Canadians from Child Pornographers Act, or something of that ilk. Lawful access was his favourite catchphrase.

Lawful access is now essentially a dirty word in Ottawa. Whenever you say it, it rekindles images of Vic Toews proclaiming: you're either with us or you're with the child pornographers. So the RCMP here is saying, okay, you know, that old rhetoric is not going to work here so what can we say instead? And the new public narrative essentially involves them talking about the problems around going dark, and encryption, and, you know, their inability to obtain certain communications on the Internet. And, you know, their whole philosophy on selling this is to basically go to the public and give them examples of where encryption or, you know, new technology has thwarted their efforts on terrorism or cybercrime or you name it.

And, you know, part of this is well and good, and I imagine there's people out there saying, yeah, that's fine. I mean, you know, the RCMP should have the right to make this case. And that's certainly true to an extent except part of the problem here is that they're being deliberately vague and they're kind of running this shadow campaign. They're not coming out and actually saying what they want, they're sort of alluding to it and suggesting it and using the media as sort of a conduit to ask for some of these powers. And, you know, I'm not sure that that's the right way they should be going about this.

SUTCLIFFE: I do have some sympathy for the RCMP being put in the position of having to follow up on some threats to the country, national security threats, but at the same time being limited in what it can do. And I'm sure that can be frustrating at times. But obviously there are limits to how far it should be able to go before crossing into the invasion of privacy of many people. So is this... are they... do they want more powers? Do they want the public to have more sympathy for them? What's at the heart of this, ultimately?

LING: Okay, so let's look at one of the specific problems they've identified. And that's the problem of, you know, the perceived problem of encryption. You know, the RCMP have suggested, and not really in black and white said, but they've suggested, that they would like some sort of a lawful authority to force either an individual or a company to decrypt communications that they've obtained that are encrypted. And on paper that sounds fine. On paper a lot of people will say, you know, if you're a drug dealer or a terrorist and you've encrypted all of your text messages or your emails, the RCMP should have the authority to break that encryption.

On paper that makes a lot of sense. But when you actually drill down on it – and this is kind of the disingenuous thing the RCMP is doing -- when you drill down on this, that doesn't make any sense. On the one hand, everybody has the right to be free from self-incrimination. You know, the RCMP can't necessarily, you know, compel you to give over information on yourself. The RCMP can't compel you to talk. They can't force you to take the stand at your own trial. So this is a long-standing legal precedent. The RCMP can't necessarily compel you to give over the password to your entire life. That's nothing they have the authority to do. Our constitution protects you from that.

So, you know, that's one problem. The other problem is that in a lot of cases, companies can't break their own encryption. We saw this a couple of months ago in the San Bernardino case. The FBI wanted Apple to decrypt the iPhone of one of the San Bernardino attackers. Apple came back and said, listen, we don't have the decryption key. We don't make a decryption key for every one of our phones. If we did, that would be a huge cyber security problem. If somebody ever got a hold of that decryption key they could break into every single iPhone in the world. Now that's a problem. There's a reason why these decryption keys don't exist. So if you're going to force companies to build that decryption key, you are completely undercutting your cyber security nationwide, and cyber security experts are basically saying that that's a catastrophic scenario.

Now a couple of months ago VICE News reported that Blackberry had actually given over its global decryption key to the RCMP. That raised a lot of alarm bells amongst a lot of people and, you know, there was a big conversation there about whether or not Blackberry was a company you ought to stay with because they have such apparently such poor cyber security that they would do such a thing.

So, you know, there is a big debate to be had here but I think if the RCMP wants to have it it's incumbent on them to just come out and have that debate. We've seen recently that the RCMP, you know, participated in a long back and forth with the *Toronto Star* and the CBC where they kind of laid out summaries of certain investigations where they were thwarted by encryption or whatever.

SUTCLIFFE: Right.

LING: But they wouldn't get specific there. They didn't actually say, you know, if we had this power we would have solved the case. At no point did that happen. And there is... and every one of those summaries I read, you can sit there and read it and go, there's no solution to this, you know, this is just a reality. If a criminal gets on a plane and flies to North Korea, there's nothing we can do. You know, the solution there is not to invade North Korea or whatever. There's certain barriers to investigations that are just going to exist no matter what. And if we can talk about reasonable ways in which we can kind of work around that, but this sort of... this RCMP campaign of just sort of highlighting the problems and pushing them into the public conversation without having a real conversation about what the solutions are, I think is a problem.

SUTCLIFFE: We're almost out of time but just quickly, before we let you go Justin, they're suggesting that we're far behind some of the other countries in the so-called Five Eyes partnership. Is that true?

LING: Yes and no. So there's this kind of summary that the RCMP provided about what powers exist in New Zealand, and Australia, and the UK, and the USA. So, a lot of the powers – and these are powers of forcing decryption, of retaining communications on certain network servers. Those powers have just got passed in the United Kingdom and they are highly controversial. They are very, very problematic according to a lot of privacy experts. Similarly in Australia and in New Zealand these powers are very new. We don't really know what the ramifications are yet. In the USA... the USA only has a couple of these powers that the RCMP are requesting and they date back to the Patriot Act. We all know that that is not exactly something that we want to go forward with here in Canada. So they're being a little disingenuous when they highlight these powers. These powers are very new, very controversial, and I don't know that, you know, that they made the case that they deserve them yet.

SUTCLIFFE: All right Justin. Great stuff. Thank you very much for joining us today. Appreciate it.

LING: Thanks for having me.

NOTE: TRANSCRIPTS CANNOT BE SHARED OR TRANSFERRED OUTSIDE OF YOUR DEPARTMENT.

*Questions? Please contact us at PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.
Questions? Veuillez communiquer avec nous au PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca*

Sent to : !INTERNAL; !INTERNAL 2; RCMP Breaking News

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Tuesday, December 06, 2016 6:46 PM
To: Today's News / Actualités (PS/SP)
Subject: CBC News: Privacy watchdogs urge caution with encryption laws (Department quoted)

Privacy watchdogs urge caution with encryption laws

CBC News

Matthew Braga

December 6, 2016 15h00 ET

Privacy watchdogs from across Canada warned the government on Tuesday to "proceed cautiously" before passing encryption legislation — a move that would have the potential to undermine the security of everything from financial transactions to online communication.

The warning comes at a time when government and law enforcement agencies have been seeking the ability to access encrypted information, the lack of which they see as a growing investigative problem.

However, both privacy and cryptography experts have long warned that efforts to weaken or defeat encryption for police puts the security of all users at risk.

The government is currently soliciting feedback and holding public consultations on this and other national security issues, as part of its pledge to to repeal the "problematic elements" of Bill C-51.

In a submission to **Public Safety Canada**, Canada's Privacy Commissioner Daniel Therrien and his colleagues warned against introducing any legislation aimed squarely at encryption, as well as other proposed powers that police do not currently have.

"The government should only propose and Parliament should only approve new state powers if they are demonstrated to be necessary and proportionate — not merely convenient," Therrien said in a prepared statement to reporters Tuesday morning in Ottawa. The statement was also posted to the commissioner's website.

Existing tools should be examined

A recurring theme of the group's submission is that police have not provided adequate evidence for why they should require additional powers — such as expanded data retention requirements, or lower thresholds for acquiring basic subscriber information — nor explained why existing tools are insufficient.

Therrien, along with the country's other provincial and territorial commissioners, are advocating for a closer examination of existing tools, and recommending that some rules should even be tightened.

"This is not the time to further expand state powers and reduce individual rights," Therrien said in his statement.

"This is the time to enhance both legal standards and oversight to ensure we do not repeat past mistakes and achieve real balance between security and respect for basic individual rights."

Legal measures sought

One particularly divisive issue is the matter of encryption — cryptographic protections that prevent attackers and police alike from eavesdropping on messages as they travel across the internet, or from accessing files on a password-protected device.

"There is currently no legal procedure designed to require a person or an organization to decrypt their material," according to Public Safety Canada's "National Security Green Paper," which was released in September to "prompt discussion and debate about Canada's national security framework."

Both law enforcement and government agencies have increasingly characterized encryption as an impediment to investigations, a problem they refer to as "going dark." Canada's police chiefs, for example, recently called on the government to introduce legal measures that deal with encryption, and the US Senate introduced a draft bill addressing encryption earlier this year.

Yet Therrien argues that powers that came into force with Bill C-31 last year already allow police to seek "assistance" in decrypting information, without compromising the underlying technology behind encryption.

"The crux of the problem springs from the fact there is no known way to give systemic access to government without simultaneously creating an important risk to the security of this data for the population at large," the submission reads. "Laws should not ignore this technological fact."

The country's privacy watchdogs suggest "technical solutions which might support discrete, lawfully authorized access to specific encrypted devices, as opposed to imposing general legislative requirements."
Push for transparency

Encryption isn't the only issue dealt with in the Privacy watchdogs' submission.

Metadata is a perennial concern, and the submissions suggests more stringent legislation under which metadata can be collected and shared with police, as well as international partner agencies.

The commissioners also call on the government to strengthen requirements that private companies and government agencies "be open about the number, frequency and type of lawful access requests they respond to," in regularly issued transparency reports.

They also propose an expanded oversight committee that includes independent expert reviewers, and would oversee all agencies that have a role in national security, calling the government's current proposal "insufficient."

Sent to: !!INTERNAL; !!INTERNAL 2; RCMP Breaking News

**Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
December 7, 2016 / le 7 décembre 2016**

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse quotidienne peut également être accédée via [InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS |
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRE

INTERNATIONAL

MINISTER / MINISTRE

*** Amended national security committee bill sails through committee: Conservatives argue changes don't go far enough, NDP say they're a good start**

The Liberal government's legislation to create a new national security committee of parliamentarians sailed through committee late Tuesday afternoon and is set to head back to the House of Commons with several significant amendments. (...) At its heart, the bill aims to fulfill a Liberal campaign promise to create an all-party committee tasked with overseeing the activities of Canada's national security agencies. **Public Safety Minister Ralph Goodale** announced Ottawa South MP David McGuinty as chair of the committee in January, five months before the bill itself was tabled in Parliament. The government's power to appoint the chair has been among the core points of contention for critics of the bill. (...) However, it's not yet clear what the government's approach will be to honouring those changes: C-7 is under review by **Minister Goodale** and he has not yet said whether he will accept those changes. "One

would be a place for people to go, if that happens again. The club raised \$80,000 to buy a generator and emergency supplies. It also built an additional storage room with a government grant. [CBC News](#)

*** Flood victims give back to Salvation Army in annual Christmas drive**

The Salvation Army in Sydney, N.S., has had a heartwarming surprise this holiday season. With hundreds of people hit by flooding and even more losing jobs out West, the church expected fewer donations to its Christmas campaign. Early indications, however, are they will reach their \$140,000 goal by Christmas, according to Capt. Corey Vincent. On top of that, those donations are flowing from unexpected sources. "We've noticed that many of our donations are coming from the [flood] disaster area," said Vincent (...) For weeks following the flood, the Salvation Army mobile unit took two hot meals a day to people working in their flooded homes. "You don't realize that even in the midst of tragedy just a small act of kindness of giving a hot meal can be appreciated so much," Vincent said. [CBC News](#)

*** La Ville achemine des solutions à Marc Garneau**

Pendant que la Coalition des citoyens et organismes engagés pour la sécurité ferroviaire au centre-ville de Lac-Mégantic est en croisade à Ottawa cette semaine, la Ville de Lac-Mégantic révèle qu'elle a fait parvenir au ministre des Transports Marc Garneau la semaine dernière «des pistes de solutions afin d'accélérer l'étude de faisabilité de la voie de contournement ferroviaire». «Nous avons entendu la demande des Méganticois de voir se construire le plus rapidement possible une voie ferrée qui contournerait le centre-ville. Nous avons fait nos devoirs et nous avons proposé au ministre des Transports un scénario pour accélérer l'étude», annonce le maire Jean-Guy Cloutier. Dans un communiqué émis en fin de journée mardi, sans plus d'explications sur la nature des pistes de solutions proposées, le maire Cloutier répète que la construction d'une voie de contournement ferroviaire est un projet essentiel au rétablissement de la population de Lac-Mégantic. [La Tribune](#), 4 (L'Voix de l'Est)

*** Airbus seen winning \$3B deal for search and rescue planes**

The Liberal government will announce the winner of a multi-billion dollar program for new search and rescue aircraft on Thursday, even as industry sources say aerospace giant Airbus has won the deal. The announcement was planned for Winnipeg on Thursday but, at the last minute, was changed to the Canadian Forces base at Trenton, Ont., sources say. The Airbus C-295 was selected over the C-27J built by the Italian firm, Leonardo. The \$3-billion project is divided into a contract for the acquisition of the aircraft and another contract for 20 years of in-service support. [Postmedia](#) (National Post, A12; Ottawa Citizen)

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

*** Protect privacy of subscribers, but don't stick us with the bill, CWTA tells Ottawa**

Canadian wireless carriers shouldn't be stuck with the bill if new legislation or regulations requires them to buy new equipment to intercept or collect subscriber communications or metadata, says an industry group. As part of a public consultation on updating the country's national security framework the Canadian Wireless Telecommunications Association (CWTA), which lobbies for most of the country's wireless carriers, wrote Ottawa last week to say that giving police and intelligence agencies more timely access to basic subscriber information "must consider the impact on service providers and the privacy rights of Canadians." (...) **Public Safety Canada** is looking at updating the country's security framework, everything from lawful access to carrier data to getting better access to encrypted data of criminals. The wind-up to the consultation comes as the U.K. just enacted a new law forcing Internet providers to record every subscriber's top-level Web history in real-time for up to a year, and to force companies to decrypt data on demand. Providers here worry that any new Canadian national security framework will demand they, too, store customer metadata – from browsing histories to wireless location data – for lengthy periods of time, and that they be ordered to buy expensive equipment allowing police to more easily tap into data feeds. [Cartt](#) (2016-12-06)



**Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
December 7, 2016 / le 7 decembre 2016**

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse quotidienne peut également être accédée via [InfoMédia](#)

TOP STORIES / ACTUALITÉS

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS /
ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINEES

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

OTHER / AUTRES

TOP STORIES / ACTUALITÉS

Security shouldn't trump privacy, watchdogs say

Privacy watchdogs from across the country have come together to challenge proposals to expand police and intelligence agencies' powers. Federal privacy commissioner Daniel Therrien told a press conference Tuesday that state spying and investigative powers have "already been significantly increased" in recent years. The RCMP have recently undertaken a public push for more powers to investigate online crime, arguing privacy-protecting software and laws are preventing them from catching criminals. But Therrien suggested the balance is actually tipped in police agencies' favour, and argued for greater legal safeguards to protect Canadians' privacy. In my view, this is not the time to further expand state powers and reduce individual rights," Therrien said in a statement. "Rather, it is time to enhance both legal standards and oversight to ensure we do not repeat past mistakes and that we ultimately achieve real balance between security and respect for basic individual rights." The commissioner's comments come as the Liberals wrap up a months-long consultation on Canada's national security apparatus. The Liberals have pledged to repeal "problematic" elements of the previous Conservative government's controversial terrorism law, Bill C-51, and have promised to put in place meaningful oversight for the country's 17 national security agencies. [Toronto Star](#), A8; [Globe and Mail](#); [Le Devoir](#); [La Presse+](#) (2016-12-07); [Canadian Press](#) (Metro News); [CBC News](#); [IT World Canada](#); [iPolitics](#) (2016-12-06)

implement them. The Liberal government has struck an inquiry on missing and murdered indigenous women and it pledged billions of dollars in its most recent budget to improve drinking water on reserves and support education, among other plans." Hill Times

Pearl Harbor still haunts us

An editorial piece states, "Seventy-five years ago today, planes from the Japanese navy attacked the U.S. Pacific Fleet anchored in Hawaii's Pearl Harbor, "a date which will live in infamy," in the words of U.S. president Franklin D. Roosevelt. It was indeed a day of infamy, and was followed within hours by Japan's attack on Hong Kong, where about 2,000 Canadian troops were stationed, 290 of whom were killed in the two-week battle that followed, with another 264 dying over the next four years because of the inhumane conditions in Japanese prison camps. But the infamy, sadly, was not confined to the Japanese military. Within months, Japanese immigrants and citizens of Japanese descent were interned in Canada and the U.S., deprived of their property and rights and treated as enemies. The supposed justification was that they posed a threat to security as potential enemy agents, despite the complete lack of evidence. "From the army point of view, I cannot see that Japanese Canadians constitute the slightest menace to national security," wrote Maj.-Gen. Kenneth Stuart, the head of the Canadian army. The RCMP, too, saw no reason to question the loyalty of Japanese-Canadians. Yet the pressure to intern people of Japanese descent grew, and most of that pressure came from B.C., where it was clear the motivation was long-standing racism, not national security. The roundup of Japanese fishing boats began the day after the Pearl Harbor attack. Following the impoundment of the fishing fleet, other Japanese-Canadians began to feel the effects of the war. The Canadian Pacific Railway began firing porters and section hands. Other businesses followed suit in discharging Japanese-Canadian employees, and Japanese businesses were vandalized." Times Colonist

OTHER / AUTRES

Protect privacy of subscribers, but don't stick us with the bill, CWTA tells Ottawa

Canadian wireless carriers shouldn't be stuck with the bill if new legislation or regulations requires them to buy new equipment to intercept or collect subscriber communications or metadata, says an industry group. As part of a public consultation on updating the country's national security framework the Canadian Wireless Telecommunications Association (CWTA), which lobbies for most of the country's wireless carriers, wrote Ottawa last week to say that giving police and intelligence agencies more timely access to basic subscriber information "must consider the impact on service providers and the privacy rights of Canadians." (...) Public Safety Canada is looking at updating the country's security framework, everything from lawful access to carrier data to getting better access to encrypted data of criminals. The wind-up to the consultation comes as the U.K. just enacted a new law forcing Internet providers to record every subscriber's top-level Web history in real-time for up to a year, and to force companies to decrypt data on demand. Providers here worry that any new Canadian national security framework will demand they, too, store customer metadata – from browsing histories to wireless location data – for lengthy periods of time, and that they be ordered to buy expensive equipment allowing police to more easily tap into data feeds. Cartt (2016-12-06)

Here Are the Next '20 Standing Rocks' According to Frontline Activists

Anyone with even a passing knowledge of energy politics surely knows what a massive, unexpected victory it was for thousands of Standing Rock campers when the US Army announced its decision to block the Dakota Access pipeline from its planned route. (...) Even before that surprise, Indigenous groups north of the border were already encouraged by what was happening in Standing Rock. Just last month, Kaneshatake Grand Chief Serge Simon made it clear that mass civil disobedience is on the table for Indigenous people opposing megaprojects. The Mohawk leader told APTN Canada could see "20 Standing Rocks" if projects go ahead without free, prior and informed consent. (...) Kinder Morgan's recently-approved Trans Mountain expansion, which will transport raw bitumen from Alberta through BC's lower mainland, is the most obviously heated pipeline fight in Canada, and one the major political players are already gesturing toward. "The Standing Rock Sioux won today, and we will win on Kinder Morgan," Green Party Leader Elizabeth May said in an email blast yesterday. Opponents say the project will

Rowe, Melissa (PS/SP)

From: Miller, Kevin (PS/SP)
Sent: Thursday, December 08, 2016 10:21 AM
To: Baker3, Ryan (PS/SP)
Subject: FW: Urgent - NS Consult Line Needed
Attachments: PS-SP-#1860341-v1J-Qs&As_-_NS_Consultation.doc

From our Qs and As:

We have published a discussion paper to provoke further debate and to prompt input. It raises ten areas of possible interest for Canadians to consider. And there may well others. It's up to Canadians to decide what they want to discuss. Remember this discussion paper does not purport to be some statement of new government policy. It's intended to raise issues, to simulate input and to get people engaged; that's good cause this is a very vital topic. (This is a direct quote from the launch of the consultation)

From the consultation website – disclaimer - <https://www.publicsafety.gc.ca/cnt/cnslttns/ntnl-scr/index-en.aspx>

Please note that participation in this consultation – in whole or in part – is voluntary. Acceptance or refusal to participate will in no way affect any relationship with the Government of Canada or with any of its organizations. The information provided during this engagement initiative can be subject to Access to Information and Privacy requests and will be administered in accordance with the Access to Information Act and Privacy Act.

From: Grenier, Julie (PS/SP)
Sent: Thursday, December 08, 2016 10:16 AM
To: Baker3, Ryan (PS/SP); Miller, Kevin (PS/SP)
Cc: Magee, Heather (PS/SP); Gowing, Andrew (PS/SP)
Subject: RE: Urgent - NS Consult Line Needed

Hi Ryan,

We do not have an existing line re: Privacy Act. There is a disclaimer on the online consultation re: ATIP & Privacy – this aspect was led by Policy & Web (possibly with input from Citizen Engagement) so they might be able to help you craft something. The Policy lead is Yacine Touizrar.

I've attached our supporting Qs&As on the consultation in case that's helpful.

For the latter question about bias in the Green Paper – here's a quote from the Minister to consider:

We have published a discussion paper to provoke further debate and to prompt input. It raises ten areas of possible interest for Canadians to consider. And there may well others. It's up to Canadians to decide what they want to discuss. Remember this discussion paper does not purport to be some statement of new government policy. It's intended to raise issues, to simulate input and to get people engaged; that's good cause this is a very vital topic. (This is a direct quote from the launch of the consultation)

Julie G
Tel : 613-993-4415 | BB : 613-410-6059

From: Baker3, Ryan (PS/SP)
Sent: Thursday, December 08, 2016 10:07 AM
To: Grenier, Julie (PS/SP); Miller, Kevin (PS/SP)

Cc: Magee, Heather (PS/SP); Gowing, Andrew (PS/SP)
Subject: Urgent - NS Consult Line Needed
Importance: High

Hi Kevin and Julie,

Do we have a line that explains how the NS consultation approach is in line with the Privacy Act? MO wants one quickly and wants to ensure the wording is appropriate, given an official privacy impact assessment wasn't done.

The request is in response to this story on the Huffington Post (see near the end about the consultation).

http://www.huffingtonpost.ca/daniel-tencer/liberals-canada-surveillance-data-retention-lawful-access_b_13493112.html

Any other lines we have about how the consultation questions were developed and are objective in nature would help too, as the story suggests some of the questions are deliberately leading.

Lastly, are these the latest lines on the NS consultation? I'd like to share a package with Scott.

- The Government of Canada is conducting a public consultation to obtain Canadians' views to ensure Canada's national security framework is effective in keeping Canadians safe, while also safeguarding our values in a free and democratic society
- These consultations are one part of the government's approach to national security issues. In June, the government also introduced new legislation to create a "National Security and Intelligence Committee of Parliamentarians" to strengthen scrutiny and accountability of all our security agencies. It is also working on the establishment of a new national office and centre of excellence to bolster and coordinate community efforts to prevent vulnerable individuals from being radicalized to violence. In addition, it has undertaken a complete re-examination of Canada's cyber-security capabilities.
- The Government believes it is important for Canadians to be informed and engaged in a discussion on these important elements of Canada's national security framework.
- The input that the Government receives from Canadians, including experts, stakeholders, and Parliamentarians, will help inform the development of national security law and policies.
- The Government is committed to repealing the problematic elements of the former Bill C-51 and ensuring that Canada's counter-terrorism laws and policies comply with the *Charter* and respect Canadian values.
- The consultation supports the Government of Canada's commitment to openness and transparency.

Ryan Baker
Director, Public Affairs / Directeur, Affaires publiques
Public Safety Canada / Sécurité publique Canada
Tel: (613) 991-3549
Mobile: (613) 796-9750
Ryan.Baker3@canada.ca

Questions and Answers

Consultation on National Security

Context: On September 8, the Government launched a public consultation on national security.

Q1. How were the topics selected for the consultation? (OR Why wasn't x issue included?)

A1. The Government is consulting Canadians on 10 key topics, as it believes it is important for Canadians to be informed and engaged on various elements of Canada's national security framework. This includes, but is not limited to, measures contained in the *Anti-terrorism Act, 2015* (the former Bill C-51).

Canadians are also welcome to provide comments on the current national security framework in general, if they wish.

Q2. Why is the Government consulting on such a broad range of topics when the predominant topic of interest for discussion is the former Bill C-51? Doesn't this dilute the consultation?

A2: The measures enacted by the *Anti-terrorism Act, 2015* operate within a greater national security framework, with many other important components. The Government is committed to ensuring that our national security framework and procedures are effective in keeping Canadians safe, while also safeguarding our values in a free and democratic society. A broad discussion on Canada's framework is important to fulfilling this commitment.

Q3. Why didn't the Government repeal the *Anti-terrorism Act, 2015* (or the problematic elements of the Act) and then consult on new legislation?

A3: The Government has been clear and consistent on the matter of former Bill C-51: it will repeal the problematic elements of the legislation. This consultation is a first step in that process, and will be instrumental in helping the Government ensure its national security framework reflects Canadian values and priorities.

Q4. How can Canadians trust that the information will be used, and that this isn't just window-dressing?

A4: The consultation process has been designed to ensure that the input we receive from the public, stakeholders and experts is not only heard, but analyzed and evaluated, and used to help inform the policy development process.

The Government will be transparent in informing Canadians about what it has heard, and how the information will be used. The Government will be reporting back to Canadians following the conclusion of the consultations.

Q5. Will the Government be providing updates throughout the consultation process to keep Canadians informed of its progress and any emerging trends?

A5: The Government of Canada is committed to openness and will keep Canadians updated throughout this process.

The Government will be transparent in informing Canadians about what it has heard, and how the information will be used. The Government will be reporting back to Canadians following the conclusion of consultations.

Q6. How will the input be evaluated and balanced to ensure that neither safety nor rights are compromised in relation to the new national security measures that could be put in place?

A6: The Government is unwavering in its commitment to keep Canadians safe, and will not compromise on the safety and security of Canadians.

The Government will integrate input received into the policy analysis and development process to ensure that Canada's national security framework is effective in keeping Canadians safe, while also safeguarding our values in a free and democratic society.

Q7. If a majority of the participants indicate that they would like to see Bill C-51 repealed entirely, will the Government follow the wishes of Canadians and do so?

A7: The Government has been clear and consistent on former Bill C-51: it will seek to repeal the problematic elements of the legislation. This commitment was reiterated in the federal budget, and the Government will continue to move forward with it. This consultation is a first step in that process, and will be instrumental in the development of national security laws and policies.

Q8. When do you anticipate that the Government will introduce legislation to amend the Anti-terrorism Act, 2015 (the former Bill C-51)?

A8: The consultation on national security will be ongoing until December 1, 2016. The Government will be reporting back to Canadians following the conclusion of consultations on what it has heard and next steps. It is anticipated that legislation would be introduced in 2017.

Q9. Will the consultation lead to an updated Counter-Terrorism Strategy?

A9: At this time, the Government of Canada is focusing on getting Canadians' views on the various consultation topics included in the consultation documents. Until the consultations have concluded and a fulsome analysis of the input has been done, it is too early to comment on what the possible outcomes from this process could entail.

Q10. When will the in-person consultations be held and who will be able to participate in these sessions?

- 3 -

A10: A series of open town hall events will take place in the fall. The dates and locations will be provided on the consultation webpage as the events are confirmed. These discussions will be open to the public.

In addition, the Government will hold targeted meetings with stakeholders and academic experts in the national security field. The Government will keep Canadians informed on the progress of the consultations, including the in-person component.

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Tuesday, December 13, 2016 1:56 PM
To: Today's News / Actualités (PS/SP)
Subject: Transcript: Task Force on Cannabis Legalization and Regulation Chair Anne McLellan, and Vice Chair Dr. Mark Ware, discuss their report to the Ministers of Justice, Health and Public Safety - 2016-12-13 - 10:45 ET

DATE/DATE:

December 13, 2016, 10:45 a.m. (EST)

LOCATION/ENDROIT:

NPT, OTTAWA, ON

PRINCIPAL(S)/PRINCIPAUX:

Hon. Anne McLellan, Chair, Task Force on Cannabis Legalization and Regulation
Dr. Mark Ware, Vice-Chair, Task Force on Cannabis Legalization and Regulation

SUBJECT/SUJET:

Task Force on Cannabis Legalization and Regulation Chair Anne McLellan, and Vice Chair Dr. Mark Ware, discuss their report to the Ministers of Justice, Health and Public Safety.

Moderator: Bon matin. Bienvenue au Théâtre national de presse.

Welcome everyone to the National Press Theatre in Ottawa for the report of the Chair and Vice-Chair of the Task Force on Cannabis Legalization and Regulation. We have the Honourable Anne McLellan. She will lead off with the English portion, and after that, Dr. Mark Ware, he's the Vice-Chair, and he'll be doing the French section. And then we have to be done by about 11:30. So I'll open the question list and hand over to Anne McLellan.

Hon. Anne McLellan: Thank you, Chris. Good morning everyone. Bonjour tous et toutes.

I am Anne McLellan and I am Chair of the Task Force on Cannabis Legalization and Regulation. With me is Dr. Mark Ware, who has served as Vice-Chair to this task force. On behalf of the nine-person task force, we are pleased today to present our report, a framework for the legalization and regulation of cannabis in Canada to the Ministers of Justice, Public Safety and Health.

This report fulfils our mandate to consult and provide independent advice on the design of a new legislative and regulatory framework. I would like to thank all task force members for their dedication and thoughtful counsel throughout this process. Members volunteered time and energy throughout the summer and fall to develop this report. Their expertise in the fields of public health, law enforcement and justice were essential in ensuring that this report reflects an understanding of the perspectives we heard. I would also like acknowledge and thank Mr. Bill Blair, the Parliamentary Secretary to the Minister of Justice who served as government liaison to the task force, and provided valuable support throughout this process.

The advice contained in our report is the culmination of more than five months of work. We traveled across the country and heard from Canadians, including representatives of indigenous communities, parents, youth and patients who use cannabis for medical purposes. We spent time with experts and organizations who shared their diverse perspectives and helped us to appreciate the complexities of legalization and regulation.

We met with officials from provincial, territorial, municipal and indigenous governments who emphasized the need for close collaboration amongst all levels of government. We traveled to Colorado and Washington and spoke to officials in the Government of Uruguay, the only other country to have legalized access to cannabis, to hear directly from those who have had firsthand experience enacting systems for legal access to cannabis.

Mark and I would like to thank all of those with whom we met as well as those experts, organizations and Canadians who took the time to provide us with close to 30,000 responses. Our report contains more than 80 recommendations. Our advice details safeguards we believe are important to achieve the objectives set out by the government to better protect the health and safety of Canadians by regulating access to cannabis.

Our report presents measures to create a viable legal market which will be essential to meet the government's objective of displacing the entrenched illicit market that exists in Canada today. And in setting out these measures, we recommend taking a public health approach to minimize harms associated with cannabis use. We recommend a series of actions to educate Canadians in advance of the coming changes in order to increase overall awareness and knowledge of cannabis, including risks related to impaired driving.

We recommend the establishment of a well regulated production, manufacturing and distribution environment, including production safety controls which would specify important things like appropriate pesticide use, safe packaging and labeling requirements. We recommend rules to protect youth, including a minimum age of 18 to purchase cannabis and restrictions on marketing and promotional activities.

Generally, we believe that it is appropriate to proceed with caution. We are only the second nation to move forward in this way and we were told by those who have gone before to expect surprises. While there are important lessons to be learned from places like Colorado and Washington State, designing and implementing a Canadian system is a unique undertaking. Continued research will help us to better understand and mitigate risks associated with problematic use.

We also encourage additional research to enhance our understanding of the health benefits of cannabis. This is particularly important when considering questions of cannabis for medical use. We did hear compelling accounts from patients who told us of the benefits they experience from cannabis use and from researchers and the medical community who call for more evidence to better understand its therapeutic potential.

It is for this reason, as well as existing jurisprudence, that we recommend maintaining the current regulations for medical access to cannabis. In our judgement, the government will be in a better position to determine changes to the medical access system once the new system for legal access is established. As we make clear in our report, certain activities should remain subject to criminal penalties. For example, those who were found to be producing outside the legal system, or who are found to be selling to minors or into international markets or who operate a motor vehicle while impaired by cannabis.

On the other hand, we believe that administrative sanctions such as tickets or fines are appropriate for minor offenses. The overall integrity and success of this new system depends in large part on the effective enforcement of the new rules. Therefore, we encourage all levels of government to make the necessary investments to increase capacity in enforcement activities, especially in the initial years of implementation.

Our report makes clear that this initiative is complex, and that collaboration among governments is critical to its overall success. The recommendations in our report, taken together, outline the foundations for a new system of regulatory safeguards for legal access to cannabis that aims to better protect health and to enhance public safety. We provide our report to the Ministers today with the conviction that Canada is well positioned to undertake this work carefully and safely.

Thank you for your attention. And I will now ask my Vice-Chair, Dr. Mark Ware, to make some remarks. Mark.

Dr. Mark Ware: Merci Anne. Et bonjour tout le monde.

Comme Mme McLellan l'a indiqué, je suis le Dr Ware, et j'assume la fonction de vice-président dans ce groupe de travail indépendant. À titre de médecin clinicien qui s'intéresse particulièrement à la gestion de la douleur, j'étudie depuis longtemps le cannabis à des fins médicales. J'ai pu constater un changement dans la culture canadienne qui nous a mené au point où nous sommes. Pour moi, la présentation de ce rapport constitue une étape importante et positive dans cette évolution, et c'est un honneur pour moi d'y avoir joué un rôle.

J'aimerais faire écho aux paroles de Mme McLellan et remercier tous ceux qui ont participé aux processus de consultation. J'aimerais aussi remercier les membres du groupe de travail pour leur dévouement et leur enthousiasme. En particulier, j'aimerais remercier notre présidente pour son leadership. En lui demandant de présider ce groupe de travail, le gouvernement a fait le bon choix. Je pense que je peux parler au nom de l'ensemble du groupe de travail lorsque je dis que ce rapport n'aurait pas été produit en aussi peu de temps et avec une telle qualité sans son leadership et son dévouement.

Je ne répéterai pas tout ce que Mme McLellan a dit en ce qui concerne la formulation de plus de 80 recommandations dans le rapport. Toutefois, j'aimerais mettre en évidence certains aspects. Nos recommandations décrivent en détails les mesures de protection qui, selon nous, sont importantes pour atteindre les objectifs établis pour, par le gouvernement qui sont de mieux protéger la santé et la sécurité des Canadiens en réglementant l'accès au cannabis.

Notre rapport présente des mesures visant à créer un marché légal. Cela rencontre les objectifs du gouvernement et sera essentiel pour enrayer le marché clandestin de la drogue qui existe au Canada aujourd'hui. Dans la mise en œuvre de ces mesures, nous recommandons avant tout que le gouvernement adopte une approche de santé publique afin de réduire au minimum les effets néfastes associés à la consommation de cannabis.

Cela veut dire qu'il faut être conscient des risques associés aux habitudes de consommation, des risques pour les populations vulnérables, ainsi que ceux liés aux marchés clandestins de la drogue. Nous recommandons de permettre la culture personnelle à petite échelle en tant que moyen de rechange pour les consommateurs pour se procurer du cannabis. Afin de limiter les risques, nous recommandons des mesures de protection appropriées telles que des limites quant à la quantité et à la taille des plantes, des interdictions relatives au processus de fabrication, des mesures de sécurité raisonnables et une surveillance par les autorités locales.

En général, nous estimons qu'il est approprié d'agir prudemment. Davantage de recherche nous aidera à mieux comprendre et à atténuer les risques associés à la consommation du cannabis et d'en comprendre aussi les avantages. La question est particulièrement importante lorsqu'on étudie l'usage du cannabis à des fins médicales. Nous avons entendu les récits convaincants des patients qui nous raconté les bienfaits qu'ils retirent de la consommation du cannabis, ainsi que des chercheurs et du milieu médical qui demandent davantage de données afin d'obtenir une compréhension plus approfondie du potentiel thérapeutique.

Les intérêts des médecins et des patients seront bien servis par l'avancement des recherches scientifiques et cliniques sur l'utilisation thérapeutique du cannabis. Nous reconnaissons aussi l'importance d'élaborer et de mettre en œuvre des efforts de sensibilisation fondés sur les données probantes pour ceux qui travailleront à établir un nouveau système de réglementation du cannabis.

Les Canadiens ont besoin de renseignements appropriés, équilibrés et crédibles sur le cannabis afin de s'assurer que les efforts stratégiques tiennent compte de leurs besoins. De nouveaux renseignements et meilleur (inaudible) sans doute au fur et à mesure que nous mettons en place et surveilleront la nouvelle réglementation sur le cannabis.

Nous soulignons la nécessité de faire preuve de souplesse dans l'intégration des nouvelles connaissances dans la politique. Comme l'indique notre rapport, cette initiative est complexe et la collaboration entre les gouvernements est cruciale pour sa réussite globale. Les recommandations émises dans le rapport exposent les fondements de nouveaux systèmes réglementaires visant l'accès légal au cannabis afin de mieux protéger la santé et d'améliorer la santé publique.

Comme l'a dit la présidente, nous présentons aujourd'hui notre rapport aux ministres avec la conviction que le Canada est en bonne posture pour entreprendre ce travail avec prudence et de façon sécuritaire. Je vous remercie. Nous prendrons maintenant vos questions.

Moderator: So we have 12 colleagues on this list and we have about, we were allotted about, till about 11:30 for questions, and we've still got to get to the phones for a couple of west coast after that. So consider the question list now closed, and we'll begin with Daniel Leblanc of The Globe and Mail.

Question: Hello Ms. McLellan.

Hon. Anne McLellan: Good morning. How are you Daniel?

Question: Very good. So the government will present legislation in the spring of next year. Do you think the regime can be put in place in 2017, 2018, 2019? When do you think this can be in place?

Hon. Anne McLellan: That is actually a decision for the Government of Canada. Our mandate was to provide advice to the government as to how they would, could go about legalization and creating a regulatory regime. Timelines from this point on in relationship to implementation are up to the Government of Canada.

Question: The rules on production and distribution that you propose, how do you, will this be corporate cannabis or do you want this to be more of a corporate cannabis culture that people who are already in the business can also join in or will it only be corporate Canada that can do this, be part of this?

Hon. Anne McLellan: I think it's very clear that we heard from a great many parties that they wanted a diversity of producers. And we agree with that. I'm not sure that, how I would define your phrase, corporate Canada, but what I would say is that our goal is a diversity of producers and even now with the licensed producers, many people don't understand that there are large license producers, but the vast majority of them aren't large. Some of them are actually quite small, and have been able to meet the regulatory standards presently in place.

So we would like to see – we know there are lots of growers out there, Daniel, who are producing illegally obviously outside the system. We would hope that some, at least some of those will wish to come within the new legal regime and will be able to meet the standards to do that.

Moderator: (inaudible) —

Hon. Anne McLellan: Sorry. Go ahead.

Moderator: Excuse-moi. Louis Blouin, Société Radio-Canada.

Question: Monsieur, Dr Ware, j'aimerais savoir au niveau de l'échéancier, d'après vous c'est réaliste de faire ça quand? Le gouvernement aura besoin de combien de temps, d'après vous, avant de pouvoir légaliser formellement?

Dr Mark Ware: C'est une question comme madame la présidente a dit, que c'est une question premièrement pour le gouvernement. Nous avons déposé notre rapport au ministre et c'est pour eux de décider le timing pour le, la mise en place de législation et en fait, finalement d'avoir le cannabis légal.

Question: Est-ce que ça vous inquiète de voir qu'il semble manquer beaucoup de preuves scientifiques, notamment ce qui a trait avec les conduites avec les facultés affaiblies, la quantité de travail de recherche scientifique qui reste à faire? Faudra du temps pour faire ça, non?

Dr Mark Ware: Mais c'est important de savoir qu'il y a un bon cadre de travail de recherche qui déjà existe, et nous avons écouté dans notre, notre processus plusieurs interprétations des données existantes et le besoin de nouveaux données. La meilleure chose que nous pouvons faire dans ce rapport, c'est d'établir un mécanisme pour faire plus de recherche pour comprendre mieux les effets de cannabis sur la rue et d'essayer de prévenir les, les problèmes et les problèmes de santé que le cannabis peut être associé. [sic]

Moderator: Catherine Cullen, CBC.

Question: You've opted to suggest a storefront model. I think when you look at what's happening in a lot of communities with dispensaries right now, that's causing serious concern. So I wonder how you see this new model shaping up and whether or not most concerns about dispensaries will continue to exist under this new model?

Hon. Anne McLellan: As you are probably aware, in the report, in chapter 3, we talk about not only production and manufacturing, but wholesale and retail distribution, and we make the point very clearly that actually wholesale and retail distribution is within the jurisdiction of the provinces and territories. And that was a position, as you can imagine, the provinces and territories made very clear to us.

So final decisions around the form of retail will be up to provinces, probably working with municipalities and the communities they represent. But certainly, there, there are a number of models which we discuss in the report, but at the end of the day, we are very respectful of the fact that any final decision around that model will be up to the provinces, probably in consultation with municipalities and local communities.

Question: I also note that you talk about maintaining criminal penalties in some areas. I believe the present government's platform commitment was actually to increase the criminal penalties when it comes to things like selling to youth. I wonder if you have any thoughts on, in fact, whether we ought to see harsher punishments in some cases.

Hon. Anne McLellan: Well, we clearly talk about the fact that it is important for us as a task force to retain or maintain criminal sanctions. What the exact penalty might be in, or sentence, in relation to those criminal prohibitions would be something that I am sure the Department of Justice would take a look at. But we did not make recommendations in terms of the exact, you know, should it be a, a minimum sentence or should it be X number of years, summary conviction versus indictment. No. Those were not things that we saw within our mandate but we were pretty clear about the kinds of things that we thought should continue to be subject to criminal prohibitions.

Moderator: David Ljunggren, Reuters.

Question: Good morning. You talk about the desire to set up a diverse market but isn't it the case that once cannabis is legalized, the major, well large producers are going to ramp up production. How do you protect the little one from being squished (laughter) and not having a chance to get off the ground?

Hon. Anne McLellan: I think your — let me say that first of all, I, we make the point that diversity is an important value in term, in relation to the producers. There will be means by which the government, going forward through implementation, could ensure a certain degree of diversity. There are different kinds of market interventions that a government could choose to adopt or apply to ensure a degree of diversity. And going forward, I think as the market develops, we recommend that that is something that the government watch pretty carefully.

Question: (off microphone) watching carefully and actually recommending they do it. Do you think the government should bring in some of these measures (inaudible)?

Hon. Anne McLellan: I think the government needs to understand the value of a diverse market with growers of different sizes and arguably different expertise and so on. but at the end of the day, how that market ultimately develops is up to the Government of Canada and quite honestly, the marketplace.

Moderator: Bruce Cheadle, The Canadian Press.

Question: Hi. You mentioned the diversity of views you received. I'm just wondering what the task force, if there was an issue you found most vexing and what, where were the areas where you found the most commonality where there was broad consensus?

Hon. Anne McLellan: Mark, why don't you —

Dr. Mark Ware: Yeah, I think over the course of the months that we spent on this report, there were several issues that came up that were predominantly that took the longest parts of discussion. Cannabis and driving was one, the youth age at which cannabis use should be considered legal. These were probably two of the major ones.

The less stringent issues were probably the federal-provincial jurisdictions regarding cultivation on the federal side, provincial responsibility for managing the retail side of things. So those were probably the two ends of the extremes in terms of what was most challenge and where there was most alignment.

Question: You mentioned the, this is a federal initiative, and yet you're recommending that the provinces and municipalities kind of do the regulation. Did you get any pushback from provinces or municipalities saying we don't want to have to be the ones to, to bring this in?

Dr. Mark Ware: I think in the same way that we heard a diversity of opinions from Canadians, we heard a diversity of opinions from the provinces and territories. Some of them were much more prepared and ready to engage, some of them were still in the process of working through their own thinking on the issues. So I think what we hope to do is to see really strong collaboration between the federal government and the provinces to ensure that there's adequate support, that there's adequate collaboration and that these models emerge and roll out in as effective and as safe a way as possible.

Moderator: Julie Van Dusen.

Question: Hi Ms. McLellan. I, I notice you used words like prudence and caution and surprises await you and so on. Are you convinced that legalization is the way to go? And if so, why?

Hon. Anne McLellan: Yes. Yes, I think obviously the, all nine members of the task force would not have taken up this task over the past five months if we did not believe that as a matter of public policy, legalization now is the time to move away from a system that for decades, has been based on prohibition of cannabis into a regulated legal market. And I think we're all aware of the challenges and societal problems that the existing system has created. Certainly, the existing system of prohibition has allowed illicit criminal organizations to flourish in this area.

We have also seen because of Criminal Code prohibitions against simple possession, the criminalization of many Canadians, many young Canadians and we know the effects of, the long-term, if you like, stigma and consequences of a criminal conviction. So there's, there's no question that you look, not only in this country and where people and Canadians' thinking is at, but in many other jurisdictions, that people are coming to the conclusion that the prohibition, the,

the prohibitory regime that has existed is not working and it is not meeting the basic principles of public health and safety that have to be at the core of this kind of public policy.

Question: So my follow-up, you talked about all those people that have criminal records. What happens to them? Are you, are you suggesting an amnesty? I didn't see it in there.

Hon. Anne McLellan: That was not part of our mandate. We are forward-looking in terms of after, with legalization, what would a new regulatory regime look like in this country. It will be up to the Minister of Justice to determine if she and the Government of Canada wish to make any recommendation in relation to those who have been convicted of simple possession in the past.

Moderator: Paul Vieira, the Wall Street Journal.

Question: It's kind of tied in to what Julie just asked, but you mentioned Uruguay, that Canada is going to be the largest advanced economy that's going down this road. How much pressure is there on policy makers to get this right and did the lack of global experience, were there places that did provide some insight? Did any of the US states, where, where did you go that was most helpful to learn about how to do this?

Hon. Anne McLellan: To your first point, it's very important, I should think, to the Government of Canada to get this right. It was important to us as a task force to become as well informed as possible and provide the most concrete balanced recommendations, keeping in mind the government's overall public policy objectives around public safety and public health.

In terms of jurisdictions, Mark took half the task force to Colorado, and you might like to comment a bit on some of the useful lessons we learned there. I took half of the task force to Washington, and you know, the basic lessons, I think, are expect surprises. It doesn't matter, we can look at what Colorado has done and the surprises they dealt with, we can look at Washington, we can look at Uruguay, but there will still be surprises.

And to your point, we are the largest developed country to ever move on legalization. And therefore, Uruguay, Uruguay is an important example, but a country of some 3.6 million people. Therefore, some of their challenges were different, some of them easier to meet than will be the case here at home in Canada. But we, we went where we thought it would be the most useful for us in terms of learning lessons and hopefully helping the government avoid unintended consequences, going forward.

But Mark, you might like to comment on some of the lessons that we have learned from others.

Dr. Mark Ware: We were very impressed at the time that people gave us from jurisdictions like Colorado, Washington state, Uruguay, the time they gave us to share with us the experiences that they had had in designing and implementing their policies. The key takeaways for us predominantly were these are the mistakes we made. Don't make the same mistakes we did. Know that you're going into territory that it is relatively unfounded, and learn as you go. Make sure that you set up the baseline measures so that you understand where you're starting from and then as the policy rolls out, as the country learns to manage with this new regulatory framework, you are constantly learning as you go along. And that can then, and you build flexibility into the framework that allows it to adapt as you go.

Question: (off microphone) very quickly on the, you said mistakes. I think one of the mistakes you pointed out in the report was taxation about somehow some jurisdictions put the taxation too high and that had effects on the illicit contribution. I just, on the whole section of taxation, are you suggesting that all the revenue that is raised go back into law enforcement and public health? Is that my understanding as opposed to general revenue?

Hon. Anne McLellan: I don't think we quantify. I know we don't quantify where 100% of the revenue should go. But, and in fact, the whole question around revenue going forward is one on which there is a wide variety at this point of nothing more than guesses and estimates. But we do make the case clearly in this report and maybe Mark and I would both, and the task force underscore this for all governments that revenue that is gained from creating this new legal market, some substantial part of it, especially at the outset should be going into public education, should be going into enforcement, inspection, should be going into ensuring that the Government of Canada on the production side, has the capacity and expertise to license producers who apply in a timely fashion.

All this, there is going to have to be additional capacity built to deliver this system, to implement this system and get it off the ground in a successful way. This is going to take upfront resources long before government sees any revenue. And then, in terms of your question, the revenue stream, that we do make some pretty clear recommendations in terms of where we think at least some part of that revenue should go.

Moderator: Michael Le Couteur, Global News.

Question: Ms. McLellan, you talked, actually Dr. Ware talked about how vexing and difficult it was on setting, on the implementation and testing for impairment. How troubling of an aspect was this for you, given that you're essentially going to throw the doors open to legalization but not be able to sort of get the horses back in afterwards if somebody takes the wheel and they're impaired? Because you acknowledge in the report that there's no real good test yet.

Hon. Anne McLellan: People need to keep in mind that drug impaired driving is already a problem, or a challenge in this country, right? This is not going to be a new challenge that is created by legalization. Drug impaired driving is a problem, or a challenging Canada today. That is why the science is very quickly catching up to the challenge. But are we quite there yet? No. But right now, for example, the OPP, the RCMP and other police forces across the country are testing at least to the best of my knowledge -- Mark, correct me if I'm wrong -- three roadside oral fluid testing devices to determine which, if any of those three might be, let me call it the breakthrough, that science and law enforcement and government and Canadians are all hoping for.

It is clear that THC metabolizes differently in the body than alcohol metabolizes in the blood. That's why you can't simply adopt a BAC approach to determining impairment. And that's what you've got to focus on here. It's not actually the, the amount of THC in the blood, but it's around the question of impairment. And what I would say is that there is a lot of research being done, not only in Canada, but around the world because this is an ongoing challenge. The Australians have done some interesting work. Obviously, in the United States, some good scientific work is being done.

And in the report, as you probably are aware, the Drug and Driving Committee, which is a subcommittee of the Canadian Forensic Scientists, have been charged by the Department of Justice and the Department of Public Safety, to look at this very question. Does it ma-, is it possible, based on the science to create a per se limit such as we have with alcohol. And they have been asked that question, among others, as it relates to drug impaired driving.

I think the government anticipates a report from the DDC in the coming months. And we hope that the DDC takes a look in terms of what we say about drug impaired, cannabis impaired driving. At the bottom, you know, at the end of all this, we have been brought up in a society where you don't drink and drive. You should not take cannabis in whatever form and drive. And that should be a key part of any public education campaign which we are also recommending.

Question: As a follow-up to Dr. Ware, being a doctor who's researched this for years, how difficult was it for you, did you wrestle with, the minimum age of 18, given that there is some medical evidence out there showing that the brain is still developing up to 25, balancing it with the illicit drug trade and how we know that the use would be higher in that sort of age bracket? For you as a medical professional, how difficult is it to set 18 as the limit?

Dr. Mark Ware: I think that the challenge with setting an age limit is always the balance between the potential risks to the brain and to the developing adolescent health versus the risk of the black market. And so there was always this balance between trying to ensure the safety on one side and safety on the other, quite frankly. The science in many areas of cannabis is sometimes non-existent, sometimes it's contradictory. There are studies which show one thing, there are other studies that show others.

There are differences in interpretation of the same data. During our report, we had several reviews coming out of Colorado about whether the experiment there was successful or not. And the same data, people draw very different conclusions. So in, in this particular area, we're constantly challenged by data interpretation and sometimes lack of data.

I think that the, where we've arrived is a fairly sensible point at which to draw a line that Canadian adults can make decisions. The critical point is that they're educated and informed about the decision that they're making. And I think that's the critical piece. The age, to some extent, is a line in the sand. What matters is how we teach parents, children, the public about what the potential risks and harms of cannabis use are, especially when used very young, 12, 13, especially high concentrations of THC at very early age, especially high frequency.

But also, it's not just the drug. It's the social determinants of health that go around people who are using cannabis that early, that much. There are other issues going on. We cannot separate the drug use itself from the society that people live in who are using drugs in that way. So we have to address all of these factors. And I think where we've arrived is a fairly decent balance and something that we should work with and, and build the education programs around.

Moderator: Leslie Young, Global.

Question: So to follow-up a bit on what Mike was asking, do you think that when this legislation actually goes through, that there should be a legal limit for impaired driving of some kind? And what would that be based on at this point in time?

Hon. Anne McLellan: You're asking about whether we think there should be a per se limit?

Question: Yeah.

Hon. Anne McLellan: Is that your question? In fact, the answer would be yes, if we had the science to back up the per se limit. That's the challenge right now. The science is not quite there, but the science is very quickly catching up. And that's what the DDC has been asked to consider right now. And it will be obviously instructive to all of us to see what they conclude. There are jurisdictions that have imposed per se limits.

And we felt that we looked at the challenges, we looked at what other countries have done, other states have done, but ultimately concluded because of the work the DDC is doing, it would be pre-emptory of us to suggest a per se limit when they are the forensic scientists, when they are doing a much deeper dive in terms of all the science. And it is developing, you know, almost on a daily basis, you get another report from some part of the world where science, our knowledge is becoming more refined in terms of what a THC level, an appropriate THC level that would speak to impairment, which then permits you with confidence to establish a per se limit and one that you hope and prosecutors, because we talked to prosecutors, prosecutors would hope would in fact stand up in court.

Question: And you suggest creating a maximum strength, I guess, for edible products, but not necessarily for other products. Can you explain why?

Hon. Anne McLellan: Sorry, maximum strength? You mean potency?

Question: Potency, per serving.

Dr. Mark Ware: Perhaps I can address that. You're talking about the recommendation to have edible portions with a limited amount of THC per dose. That again, comes out of experience shared with Colorado where they did not label and, and adequately warn the public when they were using edibles what the quantity of THC in the servings that they were taking, and as a result of that, they saw some public health issues emerge.

So we recommended that edible products that would be prepared not be appealing to children, be wrapped in very plain packaging and be adequately labeled in terms of the amount of THC and other cannabinoids that are in there so that the consumer knows what they're taking and that that is a standardized dose of 5 milligram or a per dose of THC in an edible quantity is, is sufficient to provide enough of the drug to have a desired effect but not such a high dose that's associated with increase in adverse events.

Moderator: Manon Cornellier, Le Droit. Manon?

Question: Merci. Enfin. Je trouve que vous prenez ça un peu passif dire que c'est au gouvernement de décider du, de l'échéancier. Vous écrivez ici qu'il doit veiller à ce que la capacité – et là on parle ici de recherche, l'application de la loi, etc., etc. – donc soit développé parmi tous les ordres de gouvernement avant le lancement du régime réglementaire. Donc, est-ce que c'est vraiment possible d'avoir une loi pour le printemps, ce serait, comme vous le dites, plus prudent d'attendre?

Dr Mark Ware: Encore, le timing de la loi, c'est une question pour le gouvernement. Qu'est-ce que nous pouvons mettre en place avant la, la disposition de la législation et éventuellement l'approbation de la législation, c'est d'avoir en place la recherche, l'éducation pour préparer le terrain pour l'implémentation de la loi.

Question: Donc, c'est pas réaliste d'avoir ça au printemps. Mais, Mrs. McLellan, you, you've been a Minister of Justice —

Hon. Anne McLellan: Yeah.

Question: — so what do you think about the fact that young people are still criminalized for something they will do without problem in maybe six months, one year? As an ex-Minister of Justice, would you recommend that the criminalization be changed, we stop criminalizing young people for just smoking a joint?

Hon. Anne McLellan: Well, in fact, that's going forward once the new regime is in place and implemented. That's what will happen. Oh, you mean now, maintenant?

Question: As an ex-Minister of Justice, what do you think of it?

Hon. Anne McLellan: You know, as an ex-Minister of Justice, I can probably do no better than the Prime Minister himself at the Toronto Star editorial board, where he made the point very clearly and one that Mr. Blair has made and one that I would make here this morning, that until such time as the law changes, the law as it exists should be enforced. That people understand what the law is today. And we are a country that operates under the rule of law.

And until the law is changed, and in whatever form it ultimately is changed, we're a task force making recommendations to the government. People should be aware of what the law is. I think people generally are in this area, and that the law should be enforced. I, I as a lawyer, let alone the former Minister of Justice, could not advocate that one disobey the existing law.

Moderator: Mélanie Marquis, Presse Canadienne.

Question: Merci. Bonjour. Peut-être le Dr Ware, ma question, je veux revenir sur la conduite avec facultés affaiblies. Mme McLellan a dit que c'était pas un nouveau défi, que c'était déjà un problème mais l'expérience de Colorado montre que ces cas-là va augmenter. Le gouvernement est au courant aussi. Dans votre rapport, vous dites que vous avez entendu beaucoup de préoccupations là-dessus, mais on dirait que les recommandations, il y en —

Dr Mark Ware: Excuse-moi. Je dois demander de reposer la question. La clique de caméras m'empêche un peu d'écouter. S'il vous répétez rapidement.

Question: La, la conduite, oui, arrêtez de prendre des photos. (rire) Mais il faut pas bouger les mains, quand vous bougez les mains, ils prennent des photos donc restez — (rire)

Sur la conduite avec facultés affaiblies, Mme McLellan disait ce n'est pas un nouveau défi. Par contre, l'expérience du Colorado montre que ces cas-là vont augmenter. Le gouvernement est au courant aussi. Et dans votre rapport, il y a aucune recommandation claire. Pardonnez-moi de le dire comme ça là. Est-ce que donc, pourquoi est-ce que vous avez pas de recommandations claires? Puis est-ce que c'est vraiment prudent pour le gouvernement de repousser à plus tard cette préoccupation-là juste pour avoir un projet de loi sur la légalisation?

Dr Mark Ware: Vous parlez du, de la conduite de voiture. Oui d'accord. Oui, c'est clair, la recommandation que nous avons c'était assez, je pense que c'est assez claire, de ne pas conduire une voiture sous l'influence du cannabis. Ça c'est clair. Le problème, c'est qu'est-ce qu'on peut démontrer pour déterminer est-ce qu'il y a un niveau dans le sang de THC pour déterminer un niveau d'intoxication, un niveau de impairment. Ça c'est très difficile, et depuis plusieurs années, l'évidence, la science n'est pas capable de démontrer.

Alors c'est pas responsable pour nous de recommander une limite qui n'est pas supportée par la science, de démontrer ou de indiquer que il y a des autres scientifiques qui sont bien préoccupés de cette question. Et à la fin de mettre en place ou de donner aux, aux polices, aux autres agents de la loi, d'avoir une meilleure éducation sur la détermination de impairment sur la roadside detection, avoir plus des officiers entraînés, donc un programme qui s'appelle Drug DRE, the Drug Roadside Evaluation.

Donc, il y a certains aspects qu'on peut mettre en place, et nous avons recommandé très fort de support la capacité de, de, d'évaluer le niveau d'impairment sur nos rues.

Question: Est-ce qu'on vous a recommandé d'ajouter au Code criminel une disposition particulière sur la conduite avec facultés affaiblies par la marijuana?

Dr Mark Ware: C'est une de nos suggestions que c'est une des questions pour le, le Criminal Code, Drug Impaired Driving, c'est encore un problème. C'est, ça commence de, de, peut-être continuer d'être un problème. Donc, c'est une de nos recommandations de laisser ça dans un, pour un acte criminel. Si ça existe avec une avec une, un outcome sévère.

Question: Bien il faut pas écrire dans le Code criminel marijuana?

Moderator: No. You're, we —

Unidentified Female: I don't think he understood her question, though.

Moderator: Okay. No. Probably no.

Question: Il faut pas, you don't have to add specifically that marijuana, drug impaired driving under the influence of marijuana is a criminal offense?

Dr. Mark Ware: That may be going in more detail than we went into in specifying exactly what was written into the Criminal Code or not.

Hon. Anne McLellan: Keep in mind, drug impaired charges are being laid now every day in this country, whether you're impaired by opioids, cannabis, prescription drugs. Those charges are being laid and convictions are being gained in courts all over this country. So that's why I don't want, and Mark and I don't want to leave the impression that 1) drug impaired driving is a new challenge in Canada, and 2) that there are not laws and tests, and Mark has referenced our DRE officers. Yes, we talk about the fact we don't have enough of them and we need better training and we need training, bilingual training and so on, but we don't want to leave here this morning suggesting to you that drug impaired driving is not being prosecuted in Canadian courts today. It is.

Moderator: Dernière collègue dans ma liste c'est Michelle Lamarche de TVA. Michelle?

Question: J'ai une question pour vous, Dr Ware. Vous parliez un peu plus tôt des préoccupations qui ont été soulevées pendant vos audiences notamment. Quelles sont les plus grandes préoccupations qu'on vous a rapportées par rapport à la légalisation et à la réglementation?

Dr Mark Ware: Okay, la préoccupation, je pense que juste dans cette discussion de 30 minutes, nous avons parlé de cannabis and driving depuis un bon 10 minutes. Ça c'est une préoccupation très, très importante. Et les messages de public education, les messages de support sont très, très clairs.

Question: Vous savez que le gouvernement veut agir très rapidement, donc déposer son projet de loi ce printemps. Vous dites que l'échéancier lui appartient mais sur quels aspects précisément et il y en a beaucoup, devrait-il être le plus vigilant, à votre avis?

Dr Mark Ware: Pour commencer, je pense que c'est plus l'éducation et ça commence aujourd'hui, avec le rapport qu'on demande, pour moi, je veux si tous les Canadiens au, au période des fêtes, lire le document, comprendre pourquoi le Canada considère cette approche pour l'éducation de la grande publique. Qu'est-ce que c'est le cannabis? C'est pas une drogue, c'est plusieurs molécules. Les besoins d'éducation pour les parents, pour les jeunes, pour les enfants, pour les médecins, pour les patients.

C'est quelque chose qu'on doit commencer d'éduquer nous-même tantôt. Pour moi, c'est la préoccupation (inaudible). Supporter la recherche en fait, c'est aussi quelque chose qu'on doit commencer tout de suite pour avoir le baseline, pour avoir une image où nous commençons avant de déposer la loi, avant de commencer. Il faut qu'on prépare le terrain.

Moderator: So at this point, we've come to the end of the list. We're five minutes over, but I recall your staff were really wanting to make sure that the west coast got in. So perhaps we could just squeeze one off the phones and then we'll, we'll wrap.

So Operator, are you there? Do you have a questioner please?

Operator: Certainly. Our first question is from David Brown from (inaudible) Canada's News. Please go ahead.

Question: Yes, thank you. The report mentions that you visited several compassion clubs and dispensaries in Canada as well, and I was wondering if you could speak to what you learned there in that experience?

Hon. Anne McLellan: Do you want me to go first? I'll, I, a number of the task force visited the BC Compassion Club. I believe it is the oldest or very close, to being the oldest compassion club in the country, David. And what I, what we saw there was a holistic approach where cannabis, the use of cannabis in whatever form is part and parcel of a wellness approach. And we had the opportunity to meet not only with the people who run the compassion club for many years, but also patients, members of their Board of Directors, those who provide advice and information to those who come through the Compassion Club's doors.

It, I think, look, we do have to be honest that presently that which is being done there is illegal, at least part, let me be clear, some part of that which they are doing, but they in fact, I now believe are licensed under the city of Vancouver application process as some other dispensaries have been licensed in that city. That obviously raises a host of other

issues. But I think what we learned there, putting to one side certain issues of illegality, is that there can be a holistic wellness based approach, street level approach that serves generally highly marginalized populations and that this is a model, if you want to call it that, that the report references and suggests that governments should take a look at, going forward.

Moderator: David, do you have a supplementary? If not, I'm going to wrap this.

Hon. Anne McLellan: Do you want to add anything to that?

Moderator: Let's see if he has a --? Operator, are you going to put him on for a supplementary?

Operator: We have no further questions.

Moderator: Great . Thank you very much.

Hon. Anne McLellan: Thank you.

Moderator: Happy Holidays, Merry Christmas.

Hon. Anne McLellan: Yes, Happy Holidays everyone.

- 30 -

NOTE: TRANSCRIPTS CANNOT BE SHARED OR TRANSFERRED OUTSIDE OF YOUR DEPARTMENT WITHOUT THE CONSENT OF MEDIA Q INC.

*Questions? Please contact us at ps.pspmediacentre-centredesmediaspsp.sp@canada.ca
Questions? Veuillez communiquer avec nous au ps.pspmediacentre-centredesmediaspsp.sp@canada.ca*

Sent to : !INTERNAL; !INTERNAL 2; RCMP Breaking News

Today's News / Actualités
December 13, 2016 / le 13 décembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES
AUTOCHTONES DISPARUES ET ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

Tech Execs To Liberals: Don't Make Online Surveillance Even Worse

Many tech entrepreneurs were already concerned that Bill C-51 — the controversial piece of national security legislation passed by the Harper government — is turning Canada into "a horrible place" for tech companies to do business, as one put it. Now, they are growing worried that the federal Liberals' are apparently considering expanding online surveillance as part of their review of Bill C-51. **Public Safety Canada** is considering warrantless access to Canadian Internet users' identifying information, as well as a rule that would require Internet providers to keep track of all web surfers' activities. More than 60 entrepreneurs from Canadian tech and new media companies have signed an open letter to Prime

Minister Justin Trudeau and **Public Safety Minister Ralph Goodale**, expressing “serious economic and data security concerns with the direction of the federal government’s national security consultation.” Among the signatories is Tim Bray, the founder of OpenText, Canada’s largest software company and one of the country’s overall largest businesses. Although the Liberals voted in favour of Bill C-51 while in opposition, Trudeau has expressed some regrets on the matter, and **Goodale** vowed to remove the “**problematic elements**” of Bill C-51. But the consultation launched this fall focuses its attention on ways to expand government powers online, and doesn’t ask the public if they would like to see any scaling back of the new powers given security agencies and police under Bill C-51. (...) The **Public Safety** consultation appears to be looking at ways of reinstating “lawful access” — the principle that police should be able to access data about Internet subscribers without a warrant. [1000 Islands Gananogue Chamber of Commerce](#) (Huffington Post)

Fentanyl overdoses killed hundreds of Canadians this year, experts say 2017 could be deadlier

Last year in Vancouver, a firefighter’s primary job was putting out fires. Now, it’s saving residents who’ve overdosed on opioids like bootleg-fentanyl. Firefighters located at Fire Hall No. 2, in Vancouver’s Downtown Eastside, responded to 1,255 calls in November to deal with the skyrocketing number of overdoses, said Dustin Bourdeaudhuy, the vice-president of Vancouver Fire Fighters’ union local 18. “This month they are projected — if things stay on pace — they’ll be up to 1,600 calls,” he told Global News. “It’s unimaginable, nobody could have predicted this.” (...) In response to the growing health crisis, the federal government announced it is taking steps to make it easier to set up supervised drug injection sites in Canada while cracking down on illicit shipments of fentanyl and the import of equipment used to make pills. Health Minister Jane Philpott and **Public Safety Minister Ralph Goodale** announced the proposed changes to the Controlled Drug and Substances Act on Dec. 12. [Digital Cameras Planet](#)

Think 2016 was bad? 3 Canadian decision-makers are working to make 2017 better

During the 2015 federal election campaign, Liberal leader Justin Trudeau vowed to boost the number of Syrian refugees Canada would take in to 25,000 by year’s end. And there would be an airlift if necessary to meet that goal. A month after Trudeau swept to victory, his Liberal government forged ahead with the plan in the face of public fears that security might be compromised. RCMP Commissioner Bob Paulson and CSIS director Michel Coulombe appeared at alongside **Public Safety Minister Ralph Goodale** to assuage such fears. While the goal of 25,000 by Jan. 1, 2016, wasn’t quite met, Canada — which normally takes in about 10,000 refugees a year — has thus far taken in about 33,000 Syrians — almost three times the number taken in by the United States over the same period. Overseas screening was expedited, with additional processing of newcomers by Immigration Canada and CSIS upon arrival. Trudeau met and welcomed the very first refugees in person when they arrived on a Canadian military flight from Beirut, Lebanon, on Dec. 11, 2015, at Toronto’s Pearson Airport. [Ottawa Citizen](#)

Canadian media sucks at representing Muslims in Canada

An opinion piece states, “When it comes to Muslims, even the good news stories can turn ugly. Take this example from September 2016: Prime Minister Justin Trudeau visited a mosque during Eid, one of the holiest celebrations in the Islamic calendar, to pay his respects. The story morphed into something sinister and malevolent. Several newspapers owned by Postmedia reported that the mosque our prime minister was stepping into—and the imam who leads it—have ties to terrorism; that the mosque is sexist for separating men and women; and that the PM can’t really be a feminist if he is prepared to speak before such a gathering. (...) The *Toronto Star*, despite its recent fault with the mosque story, actually leads the way when it comes to coverage of Islam and Muslims. Last spring, the country’s largest newspaper concluded that using the Islamic State to describe the violent extremist group was wrong. The newspaper decided to use Daesh, the Arabic acronym of the group, instead. It’s the term used by foreign leaders around the world, even recently adopted by our own government as the most accurate term to describe this “multinational gang of killers and rapists” as described by the *Star*’s editor-in-chief, Michael Cooke. And yet, even after **Public Safety Minister Ralph Goodale** made the announcement in August 2016 that Daesh is the right label to use, most Canadian media outlets continue to use the other term, feeding into a violent extremist myth: that this group is Islamic and that it is a state.” [THIS](#)

A Prison Abolitionist’s Meeting and Open Letter to Hon. Ralph Goodale, Minister of Public Safety

Today's News / Actualités
January 4, 2017 / le 4 janvier 2017
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES
AUTOCHTONES DISPARUES ET ASSASSINEES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

**Former CSIS director says expanded surveillance powers needed to prevent terror attacks - Ward
Elcock says current lawful access provisions insufficient for spy agency**

Former Canadian Security Intelligence Services director Ward Elcock says the spy agency needs expanded surveillance powers to address the risk of terror attacks on the scale of recent violence in Europe and Turkey. Elcock said modern technology has surpassed the legal framework for surveilling and foiling the threat of an attack. "Communications has moved on substantially from the days of alligator clips and copper wires," he said in an interview with Terry Milewski on CBC News Network's Power & Politics. The Liberals are currently reviewing the previous Conservative government's Bill C-51, now known as the Anti-terrorism Act. Elcock said current lawful access provisions are "absolutely" insufficient and should be expanded so CSIS would have additional powers and tools to investigate threats involving

smartphones and the internet. "I think the minister of public safety has suggested that he does see some room for movement on issues like lawful access," he said. [CBC News](#)

Broadcast Media / Médias télédiffusés

CBC News' Power and Politics interviewed former CSIS Director Ward Elcock on Canada's terror response capacity and other security issues. [Rough Transcript](#)

TOP STORIES / MANCHETTES

Updated: Hydro One says police investigating possible cyber threat

Ontario's Hydro One says it is assisting Canadian law enforcement agencies in an ongoing investigation into a possible cyber threat against the electricity distributor. The company's chief security officer, Rick Haier, says they were contacted by the RCMP on Dec. 29. Haier suggests that a company IP address, which may have been the target of the cyber threat, is old, inactive and not connected to the power system. Hydro One says in a statement that as the owner and operator of critical infrastructure, it takes its responsibility to combat cyber security very seriously. The company says it has no reason to believe that its power system has been compromised. The RCMP says it works diligently to disrupt cybercrime, but wouldn't comment on this matter in order to "protect a potential criminal investigation." [Canadian Press](#) (Global News)

Troubled Nova Scotia veteran, family found dead: 'There is a huge sense of loss'

Aaliyah Desmond celebrated her 10th birthday three days after Christmas. She had just begun horseback riding, and announced to her family on New Year's Eve she wanted to be a veterinarian. "She always had a nice little smile," her great aunt, Catherine Hartling, said Wednesday. On Tuesday, the first day back at school after the holidays, RCMP were called to Aaliyah's home in Upper Big Tracadie at about 6 p.m. They found the bodies of four people who had been shot: Aaliyah; her parents Lionel and Shanna Desmond, both in their early 30s; and her 52-year-old grandmother, Brenda Desmond. Police said her father killed himself, but would not confirm outright the deaths were a murder-suicide, saying only there was no forced entry and no lingering danger to the public. [Canadian Press](#) (680 News); [Radio-Canada](#)

Volunteering for death - Why Westerners keep joining the fight against IS

A Briton and a Canadian have become the latest Western volunteers to die fighting the Islamic State group alongside Kurdish militants, their families and military authorities confirmed Tuesday. Ryan Lock, a 20-year-old chef from Chichester, England, and Nazzareno Tassone, a 24-year-old parking officer from Edmonton, Canada, were killed during an ISIS attack on Dec. 21 north of Raqqa, the capital of the terror group's self-declared caliphate. News of the deaths only recently became public following an announcement by the Kurdish military force they were fighting with the People's Defense Units (YPG)... The volunteers have a variety of motivations and backgrounds, but tend to fall into two broad categories, according to a Briton who has fought alongside Kurdish forces and, who, for security reasons goes by the pseudonym Macer Gifford (not to be confused with a British banker of the same name). Some, Gifford told VICE News, are idealists who have been horrified by reports of IS's persecution of the Kurds, Yazidis, Christians and other minorities, and are inspired by the Kurds' fight against the terror group. Gifford, a man with no military background, considers himself among this category. Others, he said, are former servicemen who have previously battled Islamic extremists in the Middle East and Afghanistan. Angered by the rise of IS since allied forces withdrew from Iraq, they're motivated to personally take up arms in the absence of major Western ground forces fighting the extremists. [Vice News](#)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Thousands still hit by power outages across the region

Thousands of residents all over Eastern Ontario and West Quebec are still without power after a day of freezing rain was followed by a night of damp snow, causing branches to break on power lines. As of

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Wednesday, January 04, 2017 7:43 PM
To: Today's News / Actualités (PS/SP)
Subject: RT - CBC News - Power and Politics: Interview with former CSIS Director Ward Elcock on Canada's terror response capacity and other security issues - 2017-01-04 - 18:15 ET

Rough Transcript

Station: CBC News - Power and Politics
Time/heure: 18:15 ET
Date: 2017-01-04

Summary: *CBC News' Power and Politics interviewed former CSIS Director Ward Elcock on Canada's terror response capacity and other security issues.*

>> Terry: Turkey says it knows who carried out the New Year's Eve attack in Istanbul but stopped short of naming the suspect. 39 people were killed in the nightclub shooting and one was a Canadian woman from Milton, Ontario. Turkey isn't of course the only country to experience ISIS-inspired attack in recent months. How prepared is Canada for large scale terror event especially as the country prepares for its 150th anniversary celebrations? What else needs to be done to keep Canadians safe? Joining me now is the former director of the Canadian Security Intelligence Service Ward Elcock and we're very glad you're able to join us.

>> Interview: Pleasure.

>> Terry: Canada has been spared for the most part in attacks in Berlin and Istanbul and Nice and so on. We have seen terrorist attacks in Canada. I would like to know first how likely it seems to you that we will face eventually one day the kind of minister killings that we've seen -- mass killings we've seen elsewhere.

>> Interview: I think in the past when I was director of the Service, we could expect an attack, I think that's true. There are still -- Canada has been listed by Al Qaeda one time or other or ISIS or Daesh as a target and it's probably inevitable there will be an attack in Canada of some sort.

>> Terry: My next question is how ready we are. By that I mean ready to prevent such an attack and handle one when it happens?

>> Interview: I think from that point of view I think Canada is actually pretty well off. I think we have and I have had a lot to do with them over the last few years since I was director, I think the service is an excellent service compared to others around the world. I think the RCMP is also a very good national police force well prepared for an event like that. I think the relationship between the two agencies is better than it ever was for a bunch of reasons.

>> Terry: At the same time as you know, a good deal of criticism that we're not doing enough about deradicalization and not watching the lone wolves and not watching the returning foreign fighters, people have gone off to fight with ISIS in Syria and Iraq and coming back, that there's just not enough being done to be sure enough that we can prevent an attack?

>> Interview: You can never be absolutely sure you're going to be able to prevent an attack. Because no intelligence service or police force knows everything and they can't know everything. The reality is there is some risk that there will be an attack that will get missed. I think given the services that we have and the police forces that we have, the likelihood we will miss one is as low as it can be and inevitably there is some risk.

>> Terry: We should be worried about the lone wolves principally or the returning foreign fighters or I guess some people fall in both categories.

>> Interview: I'm not sure there is a distinction between the two categories and there is not a large one. The reality is major attack is less likely than lone wolf attack but the reality is you cough a major attack tomorrow and prove me wrong or could be a major attack tomorrow and prove me wrong.

>> Terry: What needs to be improved? And easy to believe we're not subject to the mass killings that are happening most recently in Europe that the impetus is not there to look for the gaps that may not be apparent right now? Where are the gaps and --

>> Interview: I think the agencies are looking for the gaps. I think there are gaps but there are gaps that probably have to be filled by more substantial things than the things that a service or the police forces can do from day-to-day. And those are things like better intercept capabilities and those are things like broadening some of the abilities of cis to do intercepts.

>> Terry: What do you mean by that?

>> Interview: Well, the -- the problem with communications is communications has moved on substantially from the days of alligator clips and copper wire. We're well beyond that at this point. Unfortunately some things like the legislation to give effect to broader powers intercept for the service that would effectively mean the service could do the things it could do and could do more than alligator clips and copper wire and the service could no longer do those things because the telecommunications technology moved so far beyond that.

>> Terry: When you talk about legislation, are you talking about C-51?

>> Interview: Lawful access.

>> Terry: Lawful access. You think there is insufficient lawful access as it stands?

>> Interview: Absolutely. Absolutely.

>> Terry: How would you fix that?

>> Interview: There was a piece of legislation that went to the house, some of it ultimately that was of some benefit to the police was passed into law, but the parts of that law that were -- would have applied to cis and given CSIS some capability or kept its capability up to the technology is probably a better way to put it. That was not enacted.

>> Terry: You're talking about a very touchy subject for privacy advocates who feel only too happy that this happened?

>> Interview: You asked me the question how do you prepare for an attack that is likely at some point to come? We're a major western country, a G8 country, we're a developed country, we are a logical target for is or whatever you want and the reality is at some point attack -- some sort of attack is probable.

>> Terry: The government is trying to roll back or in the process of deciding how to roll back the Harper government's legislation on these matters, C-51. What is your advice to the government, do you think they're on the right back of what you saw so far?

>> Interview: C-51 doesn't deal with intercept. It deals with other things. I'm not sure I like the legislation as it stands. Having said that, I don't know what it is that they intend to do. **I think the Minister of Public Safety suggests he does see room for movement on issues like lawful access. I think that would be very important.**

>> Terry: That's important thing for the intelligence community that that be expanded not reduced.

>> Interview: Yes.

>> Terry: I want to switch if I may to the more recent politics society of the border. As you know president-elect trump is still casting doubt in daily tweets on the intelligence communities assessment that the Russians were meddling in the U.S. Election. He seems to be defending Putin and Wikileaks and you smile and it's amazing isn't it? Isn't that alarming severe blow to the credibility of those intelligence organizations.

>> Interview: I'm not sure it says anything about the credibility of the organizations. It may say more about the understanding of others. But the reality is the Russians and the Chinese have been busy in that area for a long, long time. I haven't obviously seen the information that they have available to suggest that it was the Russians that hacked into the

DNC computers and so on. Having said that, if they're saying and saying it publicly as they're saying it, my guess would be it's probably true.

>> Terry: You would be inclined to believe them rather than Wikileaks.

>> Interview: Julian Assange wouldn't be high on my list of critical characters.

>> Terry: Final question about something else that Donald Trump has gone off lies at the heart of the security structure that we had in Canada since the war and that is nato. He's questioned its credibility and funding and sort of seems to see it more as a protection racket. If you pay enough, I'll look after you. Nice country you have here. Shame if anything happened to it. Doesn't this have an effect on us as a core member of NATO and also on the willingness to share intelligence under the Five Eyes system of the U.S. and UK and Australia and New Zealand. Doesn't that have an impact?

>> Interview: I'm not sure that would have an impact on anything like that, on sharing between intelligence agencies. There are some -- there is a nexus in NATO for intelligence agencies that is not the primary sharing arrangement the reality is that NATO is a crucial organization for us. We have been a long-time participant in it. It would be unfortunate if NATO did not continue in more or less the form, although there are always things you can do to modernize it if it didn't continue in the way to function the way it has so far and the other point it would be very unfortunate if the effect of a new president in the united States is in effect to damage the effectiveness of American intelligence agencies. I think we may have to interview again when things go bad.

>> Terry: You said it would be okay. Thanks very much to Ward Elcock, former Director of the Canadian Intelligence Service. Thank you.

>> Interview: Thanks very much.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Questions? Please contact us at ps.pspmediacentre-centredesmediaspsp.sp@canada.ca.

Questions? Veuillez communiquer avec nous au ps.pspmediacentre-centredesmediaspsp.sp@canada.ca.

Sent to: !!INTERNAL; !!INTERNAL 2; CBSA Breaking News; RCMP Breaking News

Today's News / Actualités
January 5, 2017 / le 5 janvier 2017
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES
AUTOCHTONES DISPARUES ET ASSASSINEES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

NIL

TOP STORIES / MANCHETTES

IIO called out to officer-involved shooting in Surrey

Officers with the Independent Investigations Office (IIO) have been called out to Surrey after a police incident early Thursday morning. Surrey RCMP would only confirm with Global News that a police incident took place near 120 St. and 100th Ave., but they are not commenting as to the nature of it. But the IIO confirmed on Twitter it's an officer involved shooting. [Global News](#)

At Least Nine Ontario Police Agencies Helped Deploy Secret Surveillance Gear

At least nine police agencies in Ontario participated in a provincial program to deploy secret surveillance equipment in the province's largest cities, according to documents released by Ontario's Ministry of the Attorney General under a freedom of information request. Moreover, the documents reveal that local police were trained in "lawful access" techniques—a police euphemism for intercepting digital communications—in order to keep up with "rapidly changing technology." (...) Although these documents don't name the specific police agencies involved, Motherboard previously reported that police in Toronto, York Region, Peel Region and Ottawa had each received hundreds of thousands of dollars in provincial grants since 2010 to reimburse costs of running the PESEDP. This program is briefly described in public documents as paying for activities to investigate organized crime. Police in those cities all refused to talk about the program, but it's well-known that police across Canada are investing in surveillance equipment, from facial recognition systems to IMSI catchers. (...) Last fall, the federal government opened a public consultation into the Anti-Terrorism Act, also known as Bill C-51, to address privacy concerns raised by civil liberties groups after the Act was passed in 2015. As part of the consultation, the feds released a green paper to "prompt discussion [...] about Canada's national security framework", but critics say that the document subtly advocates for expanded police powers, particularly for lawful access. [Motherboard](#)

Russian cyber attacks are 'major threat,' Congress hears

Russian cyber attacks pose a "major threat" to the United States, top U.S. intelligence officials told a congressional hearing on Thursday despite skepticism from President-elect Donald Trump about findings that Moscow orchestrated hacking of the 2016 election... Trump, who becomes the U.S. president on Jan. 20, will be briefed by intelligence agency chiefs on Friday on hacks that targeted the Democratic Party during the presidential election campaign that he won. Director of National Intelligence James Clapper, National Security Agency Director Mike Rogers and Undersecretary of Defense for Intelligence Marcel Lettre testified on Thursday before the Senate Armed Services Committee, which is chaired by Republican John McCain, a vocal critic of Putin. The intelligence officials described Moscow as a major threat to a wide range of U.S. interests because of its "highly-advanced offensive cyber program" and sophisticated capabilities. "Russia is a full-scope cyber actor that poses a major threat to U.S. government, military, diplomatic, commercial and critical infrastructure," they said in a joint statement. [Reuters](#) (CBC News; Reuters); [Associated Press](#) (Global News; Globe and Mail; Maclean's); [Agence France-Presse](#) (La Presse; TVA Nouvelles; Le Soleil); [New York Times](#); [Washington Post](#); [BBC News](#)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Encore 30 000 clients d'Hydro-Québec sans électricité

Plus de 30 000 abonnés d'Hydro-Québec sont toujours privés d'électricité. La pluie verglaçante et les rafales des derniers jours ont endommagé le réseau. Hier, c'est quelque 70 000 abonnés qui manquaient d'électricité. C'est le réseau électrique dans les régions des Laurentides, de Lanaudière, de l'Outaouais et de la Montérégie qui a le plus souffert. À midi, ce jeudi, un total de 30 546 clients attendaient toujours le retour de l'électricité. On en comptait 17 283 dans les Laurentides, 9438 à Lanaudière, 2303 en Outaouais, 862 en Montérégie et 165 à Montréal. [La Presse](#)

Saint-Lazare opens emergency shelter after power outages

While the day dawned clear and bright Thursday, many Quebecers living in Saint-Lazare remained in the dark... Many people in Saint-Lazare have been without power for the past 24 hours, forcing an emergency shelter to be opened at the community centre so residents aren't left in the cold. [Global News](#)

Wildfire mitigation work ongoing

The Town of Canmore is continuing work on lowering the wildfire risk to the community through FireSmart programs and projects. FireSmart is a provincially recognized and supported program out of Alberta Environment and Parks for communities and homeowners to protect themselves from the risk of wildfire. For communities like Canmore, which is surrounded by provincial parks and a national park – heavily forested lands – having a strategy for addressing wildfire risk is important, according to Fire Chief Todd Sikorsky. Sikorsky presented the current FireSmart situation for the municipality to council in December.

He said 2016's wildfire in Fort McMurray was a sobering reminder for this municipality that emergency preparedness for a wildfire situation here is key. [Rocky Mountain Outlook](#)

RCMP, Valley Search and Rescue looking for missing Morristown man

Kings RCMP spokeswoman Const. Kelli Gaudet confirmed that search efforts began for James Bell of Morristown the morning of Jan. 5. She said the Kings RCMP, a police dog, a RCMP helicopter and volunteers from Valley Search and Rescue are involved. [Kings County News](#); [Chronicle Herald](#); [CTV News](#); [Local XPress](#)

Avalanche safety courses recommended for backcountry enthusiasts

Avalanche conditions are currently low to moderate over most of B-C's mountains but Avalanche Canada says that does not mean skiers and snowmobilers should head into the wilderness without taking precautions. Spokeswoman Mary Clayton says avalanche courses are a fundamental skill for any backcountry travellers, and a rescue expert in Prince George says everyone should remember it's their friends who will save them after an avalanche, not search and rescue. [CFJC News](#)

Underwater beacon used in search for plane that went missing over Lake Erie

An underwater locator beacon is being used Thursday to search for a plane carrying six people that vanished last week over Lake Erie shortly after takeoff, officials confirmed. The search was hindered Wednesday by high winds and waves that did not allow boats and dive teams onto the lake. Officials said a technician from the National Transportation Safety Board will be on the lake Thursday to see if the locator beacon can detect a ping from the plane's emergency locator transponder. [Associated Press](#) (CBC News)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

At Least Nine Ontario Police Agencies Helped Deploy Secret Surveillance Gear

At least nine police agencies in Ontario participated in a provincial program to deploy secret surveillance equipment in the province's largest cities, according to documents released by Ontario's Ministry of the Attorney General under a freedom of information request. Moreover, the documents reveal that local police were trained in "lawful access" techniques—a police euphemism for intercepting digital communications—in order to keep up with "rapidly changing technology." (...) Although these documents don't name the specific police agencies involved, Motherboard previously reported that police in Toronto, York Region, Peel Region and Ottawa had each received hundreds of thousands of dollars in provincial grants since 2010 to reimburse costs of running the PESEDP. This program is briefly described in public documents as paying for activities to investigate organized crime. Police in those cities all refused to talk about the program, but it's well-known that police across Canada are investing in surveillance equipment, from facial recognition systems to IMSI catchers. (...) Last fall, the federal government opened a public consultation into the Anti-Terrorism Act, also known as Bill C-51, to address privacy concerns raised by civil liberties groups after the Act was passed in 2015. As part of the consultation, the feds released a green paper to "prompt discussion [...] about Canada's national security framework", but critics say that the document subtly advocates for expanded police powers, particularly for lawful access. [Motherboard](#)

No, the authorities can't actually track your iPhone's GPS without your permission and here's why

For the past several months, reports have been circulating that police have been tracking the GPS location of a Montreal journalist's iPhone after a judge signed off on a warrant to allow it. Since then, many headlines have been suggesting that the authorities not only have the ability to track an iPhone's GPS, but that they had actually already done it. The problem? The judge signed off on the warrant without realizing it's not technically possible for the GPS to be tracked on an iPhone by design. There are plenty of other things the police can do when it comes to surveillance, but iPhone GPS tracking isn't one of them without the user's permission. For an iPhone's GPS to be tracked, the person holding the phone has to tell the device to go into its emergency mode by making a 911 phone call. According to Apple, it has specifically designed the software in the phone's baseband – which is the processor that manages all



**Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
January 6, 2017 / le 6 janvier 2017**

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse quotidienne peut également être accédée via [InfoMédia](#)

TOP STORIES / ACTUALITÉS

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

**NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS /
ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINEES**

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

OTHER / AUTRES

TOP STORIES / ACTUALITÉS

Authorities take another look at how well indigenous women knew their killers

New categories that more precisely define the relationships between murdered indigenous women and their killers will provide a better picture of the circumstances in which the killings took place. Previously, the RCMP had been unable to elaborate on "casual relationships" in much detail. This frustrated indigenous leaders and families, who said the lack of clarity led to overly simplistic conclusions about a decades-long tragedy that has attracted global attention. (...) Nishnawbe Aski Nation Grand Chief Alvin Fiddler said trying to better classify how women knew their alleged killers is important, but it is secondary to the fact that many murdered and missing indigenous women and girls cases have not been investigated properly. "Going back 15 years with Rena Fox being found dead here (outside) Thunder Bay and there are a number of cases here in Thunder Bay where women are murdered and there have been no arrests," Fiddler said. Fox was a 38-year-old mother of four whose body was found on Feb. 28, 2003, near Kakabeka Falls. "Whenever a person goes missing or is found murdered, there is very little trust between the families and the police that there will be a proper investigation done," he said. [Waterloo Chronicle](#)

**CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET
AUTOCHTONES**

Woman, 82, pushed to the ground during carjacking

has enough terrorists. We do not need the police to create more out of marginalized people who have neither the capacity nor sufficient motivation to do it themselves." [Globe and Mail](#); [Canadian Press](#) (Toronto Star) (2017-01-05)

Crown drops charges against terror suspect

Federal prosecutors have dropped their case against suspected Ottawa terrorist Tevis Gonyou-Mc-Lean, who stood accused of threatening to avenge the police shooting of ISIL supporter Aaron Driver. Gonyou-Mc-Lean's arrest made national headlines but the alleged threat, which he denies, has not been revealed until now. On Aug. 12, 2016, two days after Driver's death in the back of a cab, Gonyou-Mc-Lean's mother reported to the RCMP that her son said he was going to exact revenge, and "that he would not hurt civilians, but he knew who he would hurt." While the mother provided the RCMP with secretly recorded conversations with her son, the alleged threat was not documented on tape. The Crown decided to abandon the case and formally stayed the uttering threats charges Thursday. Gonyou-Mc-Lean, 24, was arrested two days after Driver's death and charged with uttering threats. Instead of laying terrorism charges, the RCMP secured a terrorism bond that required him to wear a GPS ankle bracelet and live at a shelter for drug treatment. [Postmedia Network](#) (National Post, A7, Ottawa Sun, Ottawa Citizen, Toronto Sun, Winnipeg Sun, Calgary Sun, Edmonton Sun)

Tech experts divided on social media surveillance

A recent controversy involving an Ontario-based software company losing access to Twitter because of its marketing practices is just one salvo in an ongoing battle around online privacy, analysts say. Experts are divided on whether actions taken against Media Sonar of London, Ont., were justified, but are united in the view that the case highlights the elusive balance between public safety and basic privacy rights. Media Sonar touts its social media monitoring software and algorithms as ideal tools for police and corporations to aggregate and filter data to improve safety and protect corporate assets. But a U.S.-based investigation turned up marketing language that ran afoul of Twitter's policies, which state that posts on the popular social network should not be mined for surveillance purposes. Media Sonar's emails to past clients explicitly stated that the software, which allows officers to comb through publicly available posts on the likes of Twitter and Instagram, could help police search for "criminal activity" and "avoid the warrant process" when flagging people who have come under scrutiny. (...) Tamir Israel, staff lawyer with the Canadian Internet Policy and Public Interest Clinic, said there's a disconnect between what law enforcement feels it's entitled to do with data and what citizens believe may be happening. [Red Deer Advocate](#), A18 (Hamilton Spectator)

At Least Nine Ontario Police Agencies Helped Deploy Secret Surveillance Gear

At least nine police agencies in Ontario participated in a provincial program to deploy secret surveillance equipment in the province's largest cities, according to documents released by Ontario's Ministry of the Attorney General under a freedom of information request. Moreover, the documents reveal that local police were trained in "lawful access" techniques—a police euphemism for intercepting digital communications—in order to keep up with "rapidly changing technology." (...) Although these documents don't name the specific police agencies involved, Motherboard previously reported that police in Toronto, York Region, Peel Region and Ottawa had each received hundreds of thousands of dollars in provincial grants since 2010 to reimburse costs of running the PESEDP. This program is briefly described in public documents as paying for activities to investigate organized crime. Police in those cities all refused to talk about the program, but it's well-known that police across Canada are investing in surveillance equipment, from facial recognition systems to IMSI catchers. (...) Last fall, the federal government opened a public consultation into the Anti-Terrorism Act, also known as Bill C-51, to address privacy concerns raised by civil liberties groups after the Act was passed in 2015. As part of the consultation, the feds released a green paper to "prompt discussion [...] about Canada's national security framework", but critics say that the document subtly advocates for expanded police powers, particularly for lawful access. [Motherboard](#) (2017-01-05)

No, the authorities can't actually track your iPhone's GPS without your permission and here's why

For the past several months, reports have been circulating that police have been tracking the GPS location of a Montreal journalist's iPhone after a judge signed off on a warrant to allow it. Since then, many headlines have been suggesting that the authorities not only have the ability to track and iPhone's

**Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
January 12, 2017 / le 12 janvier 2017**

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse quotidienne peut également être accédée via [InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRE

INTERNATIONAL

MINISTER / MINISTRE

RCMP listened to journalist phone calls in 1992

Senator Vernon White is defending the Royal Canadian Mounted Police's decision to listen to a journalist's phone conversations in 1992 in the aftermath of a deadly bomb attack in Yellowknife. According to White, former assistant commissioner for information and identification with the RCMP, the phone-tapping was justified. "It was a murder. Nine people were killed," he told Radio-Canada, highlighting the exceptional nature of the situation. White was referring to the September 18, 1992 bombing at Giant Mine, in which over 40 kilograms of explosives 230 metres below ground killed nine men. (...) **Minister of Public Safety Ralph Goodale** defended the RCMP earlier this year when asked if the force used phone tapping the way Montreal police had done with La Presse journalist Patrick Lagacé. He said that this kind of activity is not happening now at the RCMP, but added that he is not aware of what may have happened during previous governments. [CBC News](#)

Unsung hero facing deportation

Victoria on Canada Day in 2013. Times Colonist, A7; * Globe and Mail; * Vancouver Sun; * Canadian Press (The Guardian, Cape Breton Post)

Personal privacy under threat by surveillance state

An opinion piece states, "The good news when it comes to the protection of privacy from Canada's surveillance state is that history has shown public opinion to be a powerful force against state overreach. Several times, Stephen Harper's Conservative government introduced "lawful access" legislation intended to make all digital communications subject to secret interception and decryption. Ministers pushed hot buttons ranging from terrorism to child pornography in an attempt to normalize total and unaccountable surveillance as the natural order of things. But each time, the legislation was beaten back by the weight of public outrage. An even more vocal public protest movement wasn't enough to stop the Conservatives from passing Bill C-51 (largely due to the Liberals' cowardly choice to support it). But discontent over its terms also represented a significant political force. (...) "Lawful access" may have been discarded as a label due to the public backlash when it was previously introduced. But rather than accepting the verdict of the public, the RCMP has rebranded substantially the same powers as a legislative response to "going dark." And a concerted campaign by both the federal minister responsible and law enforcement authorities has been met with relatively little public notice. Meanwhile, the Liberals' promises to revisit the worst abuses under C-51 seem to have been abandoned: All we have to show for over a year in office is a sad excuse for an oversight mechanism which is both limited in what information it can review, and bound to secrecy in reporting on what it discovers. So there's a distinct possibility that the state of the law may deteriorate even after the Conservatives' disregard for civil rights played a part in their being turfed from power." Postmedia Network (Leader-Post, A5, StarPhoenix)

*** Tech People Need to Shut Up About Canada**

An opinion piece states, "Every four years, a substantial number of Americans float the idea of moving to Canada if this or that loathed political candidate wins the Presidential election. Unsurprisingly, this political cycle drummed up an abnormal amount of interest; if the sheer volume of articles on the subject is to be believed, Trump might want to think about building a wall on the Canadian border as well, this one to keep Americans in. But this year, the quaint Canadian tradition took a darker turn, as it became a means to trick technology companies into undermining their and their users data security. When it comes to freedom of both speech and data, there's probably no worse Western country than Canada. (...) But that's getting a bit ahead of ourselves. Canada can't provide information to the NSA or any other US agency that it doesn't have. So, how likely is it that the Canadian authorities would have access to it in the first place? Thanks to a Patriot Act-like piece of Canadian legislation called Bill C-51, Canada's security and law enforcement agencies have wide powers to collect and share just about any sort of information — but it hardly matters, since those same agencies have been repeatedly proven to have exceeded those powers and spied on their own citizens, regardless. Just months ago, a Canadian court handed down a harsh rebuke of the government's bulk data collection program — which, remember, was only discovered thanks to an American whistleblower. The iconic, red-suited Royal Canadian Mounted Police in particular have a long history of this sort of abuse." Inverse

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Big opium seizure at Pearson

Canada Border Services Agency says a significant opium seizure was made at Toronto's Pearson International Airport. Officers examining a shipment from Germany last month noticed it weighed more than the 500 grams listed on the packaging. Inside the shipment, officers found 35 brick shaped objects wrapped in coffee packaging. More than 37 kilograms of suspected opium was turned over to the RCMP. London Free Press, A6

Watson on shaky radios

Mayor Jim Watson says he's concerned about the city's problems launching a new radio system months before police officers and firefighters are scheduled to come online in a year filled with Canada 150 events. (...) Watson said he has expressed his concern with staff about the new radio system being unstable. The city is paying Bell \$5.5 million annually for 10 years for the system, which was supposed to

GRC-RCMP



GENDARMERIE ROYALE DU CANADA / ROYAL CANADIAN MOUNTED POLICE

**Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
January 12, 2017 / le 12 janvier 2017**

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse
quotidienne peut également être accédée via [InfoMédia](#)

TOP STORIES / ACTUALITÉS

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS /
ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINEES

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

OTHER / AUTRES

TOP STORIES / ACTUALITÉS

RCMP listened to journalist phone calls in 1992

Senator Vernon White is defending the Royal Canadian Mounted Police's decision to listen to a journalist's phone conversations in 1992 in the aftermath of a deadly bomb attack in Yellowknife. According to White, former assistant commissioner for information and identification with the RCMP, the phone-tapping was justified. "It was a murder. Nine people were killed," he told Radio-Canada, highlighting the exceptional nature of the situation. White was referring to the September 18, 1992 bombing at Giant Mine, in which over 40 kilograms of explosives 230 metres below ground killed nine men. (...) Minister of Public Safety Ralph Goodale defended the RCMP earlier this year when asked if the force used phone tapping the way Montreal police had done with La Presse journalist Patrick Lagacé. He said that this kind of activity is not happening now at the RCMP, but added that he is not aware of what may have happened during previous governments. [CBC News](#) (2017-01-12); [Huffington Post Québec](#) (Radio-Canada) (2017-01-11)

**CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET
AUTOCHTONES**

Police injured helping residents escape fire

Three Nanaimo RCMP officers suffered smoke inhalation while helping tenants escape an apartment fire on Wednesday. Police responded to the Willow Grove Estates apartment complex at 501 6th St. about 3

purposes we need a lot of specific information to get it signed, so it can take a lot of time and we can't discuss those techniques," said police spokesperson Cst. Chuck Benoit, based on information from Staff Sgt. Rick Carey. "As a police service we investigate any criminal activities, so if it restarts into illegal activity inside then we move forward with what we've been doing in the past year," he said. On Friday police arrested two adults – a man and a woman – inside the shop. They are both facing multiple drug trafficking charges. Police also seized marijuana, THC edibles, THC gummies, THC pills, cell phones and an undisclosed amount of cash. Police haven't been identifying the people charged after the shops are raided. Benoit said that step isn't to protect those charged but to "keep the integrity of the investigation." "They're being charged. They're doing an illegal activity. It is an ongoing investigation, it's continuous. We're not done investigating all these shops," he said. [Metro News](#)

Future looks bright for Alberta's commercial cannabis producers

Aurora Cannabis is getting ready to open its second facility in Alberta to meet the current and future demand for cannabis. It already has a 55,000 square foot purpose-built space just west of Cremona to produce medical marijuana, and has added legal recreational pot to the production roster in preparation for legalization. The company is ready to be the go-to place for marijuana, trading on the TSX and featuring a handy mobile app for customers to place orders. Aurora Cannabis has big expansion plans for 2017. But all that is just the practice round. The real game will get underway in Edmonton this year when Aurora opens its new facility, conveniently located right at the airport. "It will be the largest cannabis production facility in the world, it will be 800,000 square feet and capable of producing 100,000 kilograms of cannabis per year," said Cam Battley, Executive Vice-President of Aurora Cannabis. The business of pot started in this country with medical marijuana, and demand for it is taking off. "There are currently in excess of 130,000 registered patients in Canada's medical cannabis system, these are patients with a prescription, and that number is growing at 10 per cent per month, so the demand on the medical side is significant and we need to expand to meet that demand," said Battley. (...) But the biggest area of growth for Aurora is expected to be the new recreational market, soon to be legal in Canada under new rules set to be introduced by the Trudeau government. "The anticipated market for that will be between three-and-a-half and five million Canadians," said Battley. Aurora Cannabis has plans to expand operations across Canada in the future, but chose Alberta as the starting point due to lower taxes and lower power costs under a deregulated system. Currently, Aurora employs 110 people, and will add 200 more when the new facility opens. [CTV News](#) (2017-01-11)

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

Personal privacy under threat by surveillance state

An opinion piece by lawyer Greg Fingas states, "The good news when it comes to the protection of privacy from Canada's surveillance state is that history has shown public opinion to be a powerful force against state overreach. Several times, Stephen Harper's Conservative government introduced "lawful access" legislation intended to make all digital communications subject to secret interception and decryption. Ministers pushed hot buttons ranging from terrorism to child pornography in an attempt to normalize total and unaccountable surveillance as the natural order of things. But each time, the legislation was beaten back by the weight of public outrage. An even more vocal public protest movement wasn't enough to stop the Conservatives from passing Bill C-51 (largely due to the Liberals' cowardly choice to support it). But discontent over its terms also represented a significant political force. (...) "Lawful access" may have been discarded as a label due to the public backlash when it was previously introduced. But rather than accepting the verdict of the public, the RCMP has rebranded substantially the same powers as a legislative response to "going dark." And a concerted campaign by both the federal minister responsible and law enforcement authorities has been met with relatively little public notice. Meanwhile, the Liberals' promises to revisit the worst abuses under C-51 seem to have been abandoned: All we have to show for over a year in office is a sad excuse for an oversight mechanism which is both limited in what information it can review, and bound to secrecy in reporting on what it discovers. So there's a distinct possibility that the state of the law may deteriorate even after the Conservatives' disregard for civil rights played a part in their being turfed from power." [Postmedia Network](#) (Leader-Post, A5, Star Phoenix)

Tomlinson, Jamie (PS/SP)

From: Justice Canada FPT <juscafpt@justice.gc.ca>
Sent: February-06-17 3:09 PM
To: [redacted]@dpcp.gouv.qc.ca'; [redacted]@gov.sk.ca'; [redacted]@gov.pe.ca';
 [redacted]@justice.gouv.qc.ca'; Dolhai, George; [redacted]@gov.nl.ca';
 [redacted]@gov.ns.ca'; [redacted]@gnb.ca'; [redacted]@leg.gov.mb.ca';
 [redacted]@novascotia.ca'; [redacted]@gov.sk.ca';
 [redacted]@msp.gouv.qc.ca'; Brown, Malcolm (PS/SP); [redacted]@gov.bc.ca';
 [redacted]@gov.nt.ca'; [redacted]@ontario.ca'; [redacted]@ontario.ca';
 [redacted]@ontario.ca'; [redacted]@gov.ab.ca'; [redacted]@gov.bc.ca';
Cc: [redacted]@gov.yk.ca'; Pentney, William; [redacted]@gov.nu.ca'
 [redacted]@Ontario.ca'; [redacted]@gov.sk.ca'; [redacted]@gov.ns.ca';
 [redacted]@novascotia.ca'; Chiasson, Carole (PS/SP); Rudick, Catherine;
 [redacted]@leg.gov.mb.ca'; [redacted]@gov.bc.ca';
 [redacted]@gov.sk.ca'; [redacted]@gnb.ca'; Fournier2, Diane (PS/SP);
 [redacted]@gov.ab.ca'; De Santis, Heather (PS/SP); [redacted]@gov.bc.ca';
 [redacted]@GOV.NU.CA'; Monette, Karine (PPSC); [redacted]@gov.bc.ca'; Sheridan,
 [redacted]@ontario.ca'; [redacted]@ontario.ca';
 [redacted]@gov.bc.ca'; [redacted]@msp.gouv.qc.ca';
 [redacted]@ontario.ca'; [redacted]@justice.gouv.qc.ca';
 [redacted]@dpcp.gouv.qc.ca'; [redacted]@gov.ab.ca';
 [redacted]@msp.gouv.qc.ca'; [redacted]@gov.sk.ca';
 [redacted]@ontario.ca'; [redacted]@gov.ab.ca'; [redacted]@gnb.ca';
 [redacted]@gov.sk.ca'; [redacted]@gov.nt.ca'; [redacted]@gov.sk.ca';
 [redacted]@gov.yk.ca'; Désormeaux, Suzanne; [redacted]@gov.pe.ca';
 [redacted]@gov.nl.ca'; [redacted]@gov.nu.ca'; Drouin, Nathalie G. (AssocDM/SMD);
 [redacted]@gov.ab.ca'; [redacted]@gnb.ca'; [redacted]@gov.sk.ca';
 [redacted]@gov.nu.ca'; [redacted]@gov.ab.ca'; [redacted]@gov.sk.ca';
 [redacted]@gnb.ca'; [redacted]@ontario.ca';
 [redacted]@mce.gouv.qc.ca'; [redacted]@gov.nt.ca';
 [redacted]@gov.sk.ca'; [redacted]@dpcp.gouv.qc.ca';
 [redacted]@gov.bc.ca'; [redacted]@gov.sk.ca'; [redacted]@gnb.ca';
 [redacted]@ontario.ca'; [redacted]@gnb.ca'; [redacted]@gov.sk.ca';
 [redacted]@ontario.ca'; [redacted]@gov.mb.ca'; [redacted]@ontario.ca';
 [redacted]@gov.sk.ca'; [redacted]@ontario.ca'; [redacted]@gov.ab.ca';
 [redacted]@gov.ab.ca'; [redacted]@gov.pe.ca'; [redacted]@gnb.ca';
 [redacted]@gov.ab.ca'; [redacted]@gov.nl.ca'; [redacted]@Ontario.ca';
 [redacted]@ontario.ca'; [redacted]@justice.gouv.qc.ca';
 [redacted]@gov.sk.ca'; [redacted]@gov.sk.ca'; [redacted]@gov.nt.ca';
 [redacted]@gnb.ca'; [redacted]@gov.ab.ca'; [redacted]@ontario.ca';
 [redacted]@ontario.ca'; [redacted]@ontario.ca';
 [redacted]@gnb.ca'; [redacted]@gov.ab.ca'; [redacted]@ontario.ca';
 [redacted]@gov.sk.ca'; [redacted]@gov.yk.ca'; [redacted]@dpcp.gouv.qc.ca';
 [redacted]@gov.sk.ca'; [redacted]@gov.nl.ca'; [redacted]@ontario.ca';
 [redacted]@ontario.ca'; [redacted]@novascotia.ca';
 [redacted]@dpcp.gouv.qc.ca'; [redacted]@ontario.ca';
 [redacted]@ontario.ca'; [redacted]@gov.yk.ca'; [redacted]@Ontario.ca';
 [redacted]@msp.gouv.qc.ca'; [redacted]@ontario.ca';
 [redacted]@gov.nl.ca'; [redacted]@gov.ab.ca'; [redacted]@gov.ns.ca';
 [redacted]@justice.gouv.qc.ca'; [redacted]@gov.bc.ca';
 [redacted]@gov.bc.ca'; [redacted]@gov.nt.ca'; [redacted]@gov.bc.ca';

Cc: [redacted]@ontario.ca'; [redacted]@gov.ab.ca'; [redacted]@gov.bc.ca';
[redacted]@gov.nu.ca'; [redacted]@dpcp.gouv.qc.ca'; [redacted]@gov.nt.ca';
s.14 [redacted]@gnb.ca'; [redacted]@gov.nl.ca'; [redacted]@gov.pe.ca';
s.19(1) [redacted]@novascotia.ca'; [redacted]@gov.pe.ca'; [redacted]@ontario.ca';
s.21(1)(a) [redacted]@ontario.ca'; Crosby, Adair; Benitah, Alex; MacLean, Alyson; Goldenberg,

André; Ritzen, Barbara; Zizic, Bojana; Lidstone, Bonnie; Becker, Bruce; Morency, Carole; Leclerc, Caroline; Bernier, Anny; Van Loon, Christina; Patry, Claudine; Welsh, Crystal; Ménard, Danièle; Piragoff, Donald; Saraka, Eden; Lieff, Elissa; Hendy, Elizabeth; Yombo, Etane; Lynch, Heather; 'Jacques.Boutin@tbs-sct.gc.ca'; Tomlinson, Jamie (PS/SP); Goldstone, Jennifer; Brennan, Jessica (STATCAN); McIntyre, Janet (Ext.); Wells, Joanna; 'Joanne.chretien@scics.gc.ca'; Klineberg, Joanne; De Mora, Joe; Mileto, Joe (Ext.); Boudreau, Johanne-Civil; Fong, Judy; Justice Canada FPT; Audcent, Karen; Martin, Karen; Monette, Karine (PPSC); Sabo, Kathryn; Thompson, Kathy (PS/SP); 'line.villeneuve@scics.gc.ca'; Biringer, Lisa; Belanger, Luc; 'luc.theriault@scics.gc.ca'; Angers, Lucie; Barr-Telford, Lynn (STATCAN); Hjartarson, Lynn; Scott, Marcie (PS/SP); Ross, Marie; Potter, Mark (PS/SP); Valin, Martine; 'matthew.graham@pco-bcp.gc.ca'; Taylor, Matthew; 'Matthieu.Letang-Keithlin@scics.gc.ca'; Klinger, Mona; Hébert, Nathalie; 'Nathalie.Houle@scics.gc.ca'; Kingston, Paula; Corriveau, Paulette C.; Di Duca, Pauline; Glushek, Phaedra; Collin, Pierre; McCurry, Pam; Rothschild, Ramona; 'tomina.rioux@pco-bcp.gc.ca'; Daly, Robert (PS/SP); Trombley, Robin; Guerra, Rose-Marie; Berzel, Ruth (PS/SP); Fakirani, Salim; Oliveira, Serge; 'Simon.Levesque@scics.gc.ca'; Lipinski, Stan; Bindman, Stephen; Mihorean, Steve; Giguère, Tina (PS/SP); Bruneau, Véronique (PS/SP); Hickey, Wendy; Clermont, Yvan (STATCAN)

Subject: Access to Basic Subscriber Information (R.v.Spencer) / Accès aux renseignements de base sur les abonnés et l'incidence de la décision R. c. Spencer

Attachments: CWG Consultation Doc.docx; FRE CWG Consultation Doc.docx; [redacted]

Dear Deputy Ministers,

[redacted]

Thank you.

Chers(es) sous-ministres,

[redacted]

Merci.

s.14

JUSTICE CANADA FPT

(Intergovernmental Relations | Relations intergouvernementales)

s.21(1)(a)

Department of Justice | Ministère de la Justice

284 Wellington Street | 284, rue Wellington

Room EMB 5240 | Pièce ECE 5240

Ottawa (Ontario) K1A 0H8

fax | téléc.: (613) 941-4165

Justice.Canada.FPT@Justice.GC.CA

Government of Canada | Gouvernement du Canada

Note: Justice Canada FPT makes an effort to ensure that our distribution lists are accurate. However, if you notice any errors or omissions, please send the correct information to Justice.Canada.FPT@justice.gc.ca. Also, please indicate any problems you might have in opening the documents attached to this email. Thank you for your cooperation.

À noter: Justice Canada FPT vise à s'assurer que nos listes de distribution sont adéquates. Cependant, si vous remarquez des erreurs ou des omissions, veuillez nous en informer par courriel à Justice.Canada.FPT@justice.gc.ca. De plus, veuillez nous indiquer si vous avez des problèmes à ouvrir les fichiers joints à ce message. Merci de votre collaboration.

FEDERAL/PROVINCIAL/TERRITORIAL COORDINATING
COMMITTEE OF SENIOR OFFICIALS (CRIMINAL JUSTICE)
CYBERCRIME WORKING GROUP

Access to Basic Subscriber Information
and the Impact of the Supreme Court of Canada's
Decision in *R. v. Spencer*

Consultation Document

December 16, 2016

Introduction

The evolution of cyberspace and the developments in digital communications in recent years have profoundly changed the way Canadians communicate and the way they go about their business. As many legal activities have moved into cyberspace, the arena for many crimes and terrorist activities has also migrated to a digital domain.

Law enforcement investigative techniques must keep pace with this new environment, including the need to identify suspects in an online context. The starting point for many criminal investigations is, of necessity, to lawfully obtain basic identifying information of a suspect in a timely manner. When an investigation includes a digital component, as most do, this identifying information can be found in relation to a suspect's subscriber account for telecommunications service.

Different terms can be used for this type of identifying information. Basic subscriber information (BSI) is commonly used in the telecommunications and cyber context. It can include a telecommunications subscriber's name, home address, phone number, and email address associated with a subscriber account for telecommunications service, and an Internet Protocol (IP) address. BSI data, however, in and of itself, never includes the content of private communications. In addition to BSI, this document considers related issues of access to other basic information, referred to as precursor/confirmatory information, and the need for basic information in emergencies and in relation to non-criminal policing duties, such as when police are responding to reports about missing persons.

The decision of the Supreme Court of Canada in *R. v. Spencer*

On June 13, 2014, the Supreme Court of Canada (SCC) released its judgment in the case of *R. v. Spencer*, a case about the ability of the police to obtain BSI associated with an IP address that they had identified in connection with the computer storage and online accessing of child pornography. In accordance with the prevailing practice, the police obtained the customer's name and address from the customer's telecommunications service provider (TSP) on request, without prior judicial authorization. It led them initially to the sister of Mr. Spencer, and ultimately to Mr. Spencer, the brother of the customer.

The SCC held that, under section 8 of the *Canadian Charter of Rights and Freedoms*, Mr. Spencer enjoyed a reasonable expectation of privacy in his identity in respect of his anonymous online activities. The common law authority of the police to ask questions and obtain information voluntarily was insufficient lawful authority to obtain the subscriber information in this case. However, the Court also stated that nothing in the decision diminished the existing common law authority of the police to obtain BSI in exigent circumstances (i.e., without additional authority in the form of a warrant or other reasonable law), and also held BSI could be provided pursuant to a reasonable law or where there is no reasonable expectation of privacy.

The operational impact of the *Spencer* decision

The *Spencer* decision has had a significant impact on the ability of police services to obtain BSI in a timely and consistent manner. TSPs, as well as some service providers in other industries like banks, retail stores, insurance companies, car rental firms, airlines and hotels, have taken a very cautious approach in responding to requests by the police to obtain customer identifying information and have often insisted on the police obtaining a court authorization before providing such information even if there is little or no expectation of privacy in the information. These actions have occurred in contexts that are often very different from and go well beyond the context of the decision in *Spencer*, which primarily centered on anonymous online activity and applicable privacy expectations.

However, there is currently no specific legal tool or legislation designed to provide law enforcement and national security agencies with timely and consistent access to BSI.¹ As a result, law enforcement agencies have to use tools already available in the *Criminal Code*, such as the general production order, which have been designed for a larger search scope. Such judicial orders are based on a “reasonable grounds to believe an offence has been committed” legal threshold, which is the same core threshold used to authorize use of search powers or to obtain the content of private communications, which actions are much more privacy invasive. In addition, this threshold is difficult and sometimes impossible to meet in the early stages of an investigation when police services may have the greatest need for ready access to BSI to advance an investigation. Police may only have “reasonable grounds to suspect” criminal activity has occurred. Even reasonable grounds to suspect may, in some cases, be a threshold that cannot be met at an early stage of an investigation. This challenge impacts a range of criminal investigations where BSI plays a significant role to further a lead.

Recently, in publicly released transparency reports from Telus and Rogers, both TSPs identify a reduction of voluntary disclosures to BSI from thousands of cases annually to zero² and reference that this change is a result of the decision in *R. v. Spencer*. For example, Telus states that their interpretation of *Spencer* means that “law enforcement agencies require a warrant to obtain the name and address information of our customers unless an individual’s life, health or security is at risk, or the information is readily available in a published telephone directory.”

Some service providers have even been refusing to simply confirm that they are the service provider for an individual (so that police know who to serve the production order on) or to tell police the general geographic location of the records (so that law enforcement can know which police agency is responsible for the investigation). This is referred to in this document as

¹ Although there is no specific legal tool or legislation designed to provide law enforcement and national security agencies with timely and effective access to BSI, the IP address and the telephone number are identifiers that may be obtained as part of transmission data. However, tools designed to access transmission data do not provide for access to BSI as a whole (i.e. customer name and address), but only to these particular identifiers given they are, in addition to being used in BSI, also related to the telecommunications functions of dialling, routing, addressing or signalling, and are transmitted to identify, activate or configure a device to establish or maintain access to telecommunication service. See sections 487.011 and 492.2(6) of the *Criminal Code*.

² Rogers: 29,438 in 2014, to 0 in 2015; Telus: 30,943 in 2014 to 0 in 2015, see <http://about.rogers.com/about/helping-our-customers/transparency-report> and <https://sustainability.telus.com/en/business-operations/transparency-report>

“precursor/confirmatory information”. This lack of basic confirmatory information impedes law enforcement from meeting current requirements for judicial authorization to obtain BSI through the use of general production orders.

Following *Spencer* and the response to the decision by TSPs, there have also been challenges for police in responding to international requests for BSI. In some cases, BSI challenges and delays have resulted in an inability for Canadian police services to effectively assist their counterparts and treaty partners in international investigations. This is a critical issue given that many crimes are now digital and the crimes show little recognition of borders, and require international law enforcement collaboration and joint force action.

Consultation with key stakeholders

At the request of Federal/Provincial/Territorial (FPT) Ministers Responsible for Justice and Public Safety, the FPT Cybercrime Working Group (CWG) has studied the impact of *Spencer* and came to the conclusion that a two-tiered legislative response is required to ensure an appropriate, consistent and rapid access to BSI by investigative agencies as follows:

- 1) authorizing BSI with a low expectation of privacy associated with it to be obtainable on demand by law enforcement, with certain safeguards (a legislated “administrative scheme”); and
- 2) creating a new type of specialized production order (judicial authorization based on reasonable grounds to suspect) for BSI with a higher expectation of privacy associated with it, such as the type of information that was at issue in *Spencer*.

Such an approach would need to be designed to reflect the varying levels of privacy interests associated with BSI access in different contexts. This would include ensuring lawful and timely access to BSI with little or no privacy interests associated with it through an administrative scheme (with legislated safeguards appropriate for the level of privacy interest implicated, if any); and access to BSI that engages greater privacy interests through a requirement for prior judicial authorization. In all contexts, how to ensure reasonable oversight, accountability and transparency measures would need to be examined. This kind of contextual consideration of the privacy interests in the circumstances would need to be carefully designed and informed by jurisprudence in not only *R. v. Spencer*, but also in other court cases that looked at these issues. It is also contemplated that this approach could include provisions for access to other basic information, referred to as precursor/confirmatory information, as well as addressing police needs for basic information in emergencies and in relation to non-criminal policing duties.

The purpose of this consultation document is to solicit views on a number of issues that relate to the development of a new reasonable law for access to BSI. Some of the goals of such a law would be to respect the right to a reasonable expectation of privacy in light of the decision in *R. v. Spencer* and other relevant court decisions, and to ensure consistent and timely access to BSI for law enforcement and other investigative agencies bearing in mind the common law authority of police to investigate crime. In addition to issues in relation to access to BSI, this consultation document is also soliciting views on the related issues of access to other basic information, referred to as precursor/confirmatory information, and the need for

basic information in emergencies and in relation to non-criminal policing duties, such as when police are responding to reports about missing persons, which activities have also been impacted by the decision in *R. v. Spencer*.

A proposal to provide for access to subscriber information by police was previously tabled in Parliament on multiple occasions³, most recently in former Bill C-30, the *Protecting Children from Internet Predators Act*, which died on the Order Paper with prorogation of the 1st Session of the 41st Parliament in September 2013. Past proposals in relation to BSI were heavily criticized, primarily due to concerns that the proposed safeguards for privacy were inadequate, and should have included judicial oversight. More recently, during the federal government's public consultations on national security, which engaged federal/provincial/territorial experts, privacy commissioners, media, the public and Parliamentarians, similar concerns were expressed.

What is BSI? How does it relate to the Internet?

BSI includes subscriber information for a telecommunications service, including Internet service, such as a name, address, phone number, and email address. It can sometimes be considered to include the subscriber's IP address, yet an IP address is different from these other identifiers in a number of respects. An IP address is a unique series of numbers that identifies a connection to the Internet for example when a computer is using the Internet Protocol to communicate over a network. It does not of itself reveal anything about the subscriber with whom it is associated and is not generally even known to the subscriber although it is often easily *knowable* by the subscriber or others who interact with the subscriber using the Internet Protocol. In other words, people don't necessarily know the IP address of people they are communicating with, although if they know how to look for it, they can often find out what it is. It can also form part of transmission data, as both an IP address and a telephone number fit within the definition of transmission data given their functions.⁴ While an IP address alone does not contain information about a subscriber, it can be associated with that individual's online activities, revealing intimate lifestyle information that was otherwise anonymous. As the SCC outlined in *R. v. Spencer*, the subscriber information, which was name and address associated with an IP address, and its association with a particular monitored online activity (possession and distribution of child pornography through file sharing), created a reasonable expectation of privacy under section 8 of the *Canadian Charter of Rights and Freedoms*. The SCC did not, however, indicate that there was a reasonable expectation of privacy in an IP address in and of itself.

³ See Bill C-30, 41st Parliament, 1st Session (*Protecting Children from Internet Predators Act*); Bill C-52, 40th Parliament, 3rd Session (*Investigating and Preventing Criminal Electronic Communications Act*); Bill C-47, 40th Parliament, 2nd Session (*Technical Assistance for Law Enforcement in the 21st Century Act*); and C-74, 38th Parliament, 1st Session (*Modernization of Investigative Techniques Act*) as well as several private members bills by Liberal M.P. Marlene Jennings re-introducing the contents of Bill C-74.

⁴ Transmission data is defined in the *Criminal Code*, s.492.2(6) as data that (a) relates to the telecommunication functions of dialling, routing, addressing or signalling; (b) is transmitted to identify, activate or configure a device, including a computer program, in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and (c) does not reveal the substance, meaning or purpose of the communication.

An investigation often starts with a known IP address, and law enforcement need to determine the identity of the subscriber with whom it is associated. However, sometimes an investigation starts with an apparent identity, such as an Internet post that contains a threat of violence and law enforcement need to ascertain the IP address associated with it so that they can attempt to find out who is really associated with the threat and where to find that person. In that scenario, law enforcement needs the service provider to produce the IP address. In order to potentially determine the identity of the person posting the threat, they would then need to obtain the customer name and address associated with the IP address.

Q.1 Should an IP address form part of the BSI data (i.e., name, address, phone number and email address)? Should it be treated differently from other BSI access? If so, how?

Why is Access to BSI Important?

BSI is sought across a wide range of criminal investigations, from kidnapping and child pornography to fraud and terrorism. It is also sought very frequently as it is the starting point and essential building block for many investigations. The inability for law enforcement to get reliable and timely access to BSI since the *Spencer* decision has led to investigative delays, increased investigative costs, and the inability to continue criminal investigations, thereby threatening public safety.

Police have the greatest need for BSI, and access it most frequently. However, it is also critical information for the wider community of investigators. Agencies such as Canada Border Services Agency (CBSA), the Canadian Security Intelligence Service (CSIS) and the Competition Bureau (CB) all make use of BSI when pursuing their investigative mandates.

BSI is often used by police at the earliest stages of an investigation to efficiently identify possible leads. Reliable and timely access to names and addresses in these cases help investigators corroborate source information (sometimes from informants), compile data, pursue leads, and move investigations forward. Without access to BSI, investigations will often be unable to proceed if, at the very early stages of an investigation, there is not sufficient information to meet the required reasonable grounds to believe threshold to obtain a general production order.

Not long ago, in the context of telephone numbers, the association of a name and address with a telephone number was readily and publicly available through telephone directories. In addition to BSI, other basic information was readily available in the past, for example in missing person investigations, police used to be able to obtain basic confirmations from TSPs on request, for example to confirm that the phone was active, when it was last used, whether it was on. Presently, this information is often not available as many TSPs request that police demonstrate that it is matter of life and death before providing any information, even general information of this nature, on request. While it may not be a matter of life and death, it may be a matter of some urgency but in such cases the information will not be provided if the TSPs does not agree with the police regarding the urgency. Another difficulty is that when the

collection of information does not relate to a crime (e.g., when there is an investigation to locate a missing person), a judicial authorization cannot be obtained as the provisions for investigative tools to use in criminal investigations under the *Criminal Code* do not apply.

The value of reliable and timely access to BSI is apparent in many types of investigations:

- In some frauds, the victim is tricked into sending money to the fraudster, who often targets multiple victims in a short period of time. If police can quickly obtain BSI for the IP address or phone number used to perpetrate the fraud, further victimization can be prevented.
- Drug trafficking cases often involve suspects who constantly change phones to evade detection. In these circumstances, police need to access BSI quickly or these individuals will always be one step ahead.
- In homicide investigations, police are most successful when the evidence is “fresh”. Quick access to BSI allows investigators to properly assign tasks, identify witnesses, and make decisions about the direction of the investigation.

The need for BSI related to a series of phone numbers or IP addresses also arises in connection with court authorizations to intercept a person’s private communications under Part VI of the *Criminal Code* and transmission data production orders to obtain stored transmission data such as incoming and outgoing telephone numbers or IP addresses under section 487.016 of the *Criminal Code*. For example, police need to confirm the BSI before submitting an affidavit to a Crown agent in support of an application for an authorization to intercept private communications. Now, as a result of *Spencer*, police are generally waiting for 30 days to be able to obtain BSI under a general production order, when in the past it was provided within hours, pursuant to common law authorities of police to investigate. This delay is problematic as police may no longer have the up-to-date information needed for the interception of private communications after such a delay.

Q.2 Should all investigatory agencies be able to obtain BSI? Should the conditions under which BSI is obtained be different depending on the investigatory agency? Should the framework for provision of BSI include a timeframe within which it must be provided?

Why is Access to Precursor/Confirmatory Information Important?

Since *Spencer*, many TSPs, and other service providers in the non-telecommunications context, are refusing to provide law enforcement with basic information, such as whether a TSP has in its possession any information relating to a particular phone number. In the past, this type of precursor/confirmatory information was provided to police on request based on long-standing common law powers of police to investigate crime. Some TSPs are also refusing to tell law enforcement what the general geographical location is that is associated with that account in order for law enforcement to determine which police service has jurisdiction to pursue the investigation. This kind of information is not designed to identify a person.

Other examples of service provider refusal to provide precursor/confirmatory information include:

- refusal to confirm whether other basic identifiers such as an International Mobile Equipment Identifier (IMEI) belongs to them;
- refusal to confirm whether a known person is a user of their service(s);
- refusal to confirm whether they have information about an account;
- refusal to confirm whether a cell phone was active in Canada on a particular date and time;
- refusal to provide general location (city or province) of an account holder so jurisdiction can be determined; and
- refusal to confirm whether an account is a personal or a business one.

Law enforcement has had to delay or abandon investigations due to this information not being forthcoming, particularly where judicial authorization requirements could not be met, either due to the preliminary stage of the investigation, and the standard associated with the general production order of reasonable grounds to believe, or the inability to confirm that the service provider has possession of the required data. The CWG is of the view that this limited, precursor/confirmatory information does not have a reasonable expectation of privacy associated with it, as it does not reveal intimate lifestyle information about an individual. As such, it should be obtainable as part of a legislated administrative scheme.

- Q.3 Is there a reasonable expectation of privacy associated with precursor/confirmatory information? If so, please explain the expectation of privacy associated with this information.**
- Q.4 What specific conditions should be included in an administrative scheme designed to compel provision of basic pre-cursor/confirmatory information? For example, should there be a designated timeframe to provide this information?**
- Q.5 Are administrative safeguards such as reporting and audit requirements, advisable or necessary for a scheme providing access to basic pre-cursor/confirmatory information? If you would recommend that such a scheme include safeguards, do you have any views as to which safeguards would be appropriate?**

Developing a Reasonable Law

Access to BSI in foreign jurisdictions

Laws in many foreign jurisdictions specifically permit law enforcement and national security agencies to obtain BSI. In many cases, this can occur without prior judicial authorization. These foreign jurisdictions include the United States, the United Kingdom, Australia, Germany, Sweden, Ireland, Denmark, Spain, Finland, the Netherlands and Norway.

The laws and regulations in these jurisdictions vary in how they limit and safeguard administrative access to BSI. Some jurisdictions give certain agencies access to BSI administratively but require other agencies to obtain judicial authorization first. In some cases, a general administrative scheme for obtaining BSI operates, but an order from a judge may be required under certain conditions. These conditions requiring a court order may include when BSI is stored as part of a data retention requirement, or when certain categories of BSI are sought, such as an IP address or other data unique to mobile cellular devices, such as an International Mobile Subscriber Identity (IMSI) number. Other limitations in getting administrative access to BSI include requirements for senior police officers to approve requests and limiting BSI access to certain types of crime, or requiring that prosecutors be involved in the process to obtain some types of BSI.

The difference between these regimes and the current Canadian context, where a general production order is often required to access BSI, results in unworkable delays in the context of international investigations, where promising leads on international criminal activity cannot be pursued due to the time that is required to obtain the BSI, which can be too long to make it useful. Another challenge arises from the judicial threshold of a general production order, requiring reasonable grounds to believe, which is not required in other jurisdictions for BSI, and may make it impossible for BSI needed for international investigations to be obtained.

Post-Spencer jurisprudence

Subsequent to the *Spencer* decision, lower courts have been called on to consider its application in a variety of contexts. The issue has frequently arisen in relation to access to cell phone BSI for a known cell phone number. The courts have consistently held that the account holder has no reasonable expectation of privacy in this information.⁵ For example, Mr. Justice Code of the Ontario Superior Court held that "... a consistent line of authority has held that there is no reasonable expectation of privacy in the name associated with a phone number. *Spencer* did not reverse these authorities."⁶

In another case, Mr. Justice Nordheimer of the same court held:

Information regarding a person's address and telephone number was, until the recent decline of telephone books, readily available to any person who simply looked up someone's name in those books. Even today, web based services such as Canada 411 still provide such information. It is also a fact that nowadays we routinely provide our telephone numbers and addresses to an almost unlimited number of businesses and government entities. To suggest that there is a reasonable expectation of privacy in such information is belied by the breadth of our release of that information to others.⁷

⁵ See *R. v. Latiff*, [2015] O.J. No. 1153 (SC); *R. v. Khan*, 2014 ONSC 5664; *R. v. Morrison*, Court File No: Brampton 2013/6310, Ont. CJ, decision by Gage J., reasons for Charter ruling released Dec.17, 2014; Endorsement in the matter of applications for a transmission data recorder warrant etc., by Clearwater J., Queen's Bench, Winnipeg Centre, May 21, 2015; *Re Subscriber Information*, 2015 ABPC 178 (July 15, 2015); *H.M.Q. v. Telus Communications Company*, 2015 ONSC 3964: "All of this leads me to the conclusion that cellular telephone customers do not have an expectation of privacy in their name and address as it is linked to their telephone number, by itself." (para. 37).

⁶ *R. v. Khan*, 2014 ONSC 5664, at para. 27.

⁷ *R. v. Latiff*, [2015] O.J. No. 1153 (SC) at para. 8.

A two-tiered solution to access BSI

The CWG is of the view that access to BSI should be provided for in a two-tiered legislative response.

The first tier would consist of an administrative scheme that would apply, at a minimum, to:

- requests for precursor/confirmatory information
- requests made in association with exigent circumstances; and
- requests made in relation to general non-criminal policing functions (e.g. missing persons, stolen property, etc.).

In light of the current jurisprudence, this first tier administrative scheme could also apply to requests for BSI associated with telephones/cell phones.

The second tier would involve judicial authorization, potentially in the form of a new, specific production order (at a reasonable grounds to suspect threshold), which would be required for BSI that has a greater expectation of privacy associated with it. In *Spencer*, a reasonable expectation of privacy was held to exist in connection with a subscriber's name and address associated with an IP address because of how the online activity associated with the IP address could reveal information of an intimate nature that was otherwise anonymous (browsing, file sharing etc.). One of the fundamental purposes of this consultation is to solicit views on where and how the line should be drawn between BSI that can properly be obtained through an administrative scheme and BSI that should ordinarily only be available with judicial authorization.

- Q.6 What are your views on the recommendation that BSI with greater privacy expectations (i.e., when linked to otherwise anonymous Internet activity) should be obtained by police through a new, specialized production order based on a reasonable grounds to suspect threshold, similar to existing provisions in the *Criminal Code* for access to transmission data and tracking data?**
- Q.7 How could privacy be assessed in determining whether BSI should be compelled through an administrative scheme or whether judicial authorization should be required to compel its production? For example, should judicial authorization be required for all Internet-related identifiers? Or should this assessment/determination be more contextual, such as considering if there is any intimate details of lifestyle and personal choices that would be revealed, that would otherwise be anonymous online?**
- Q.8 What specific criteria, including conditions and safeguards should be considered for the decision making process to apply an administrative scheme or seek judicial authorization for access to BSI? For example, should the process involve a determination based more on context (e.g., assessing privacy expectations) or should the process be more**

categorical (e.g., all Internet-based identifiers require judicial authorization) recognizing this more general approach could be considered to provide greater clarity but could also result in protections that are less tailored to the particular expectation of privacy?

- Q.9 How should access to BSI be approached in the context of going-forward authorizations, such as transmission data recorder warrants or Part VI authorizations for the interception of private communications? Should those *Criminal Code* powers expressly provide that the BSI be produced as part of those warrants and authorizations? If not, please elaborate.**
- Q.10 How should BSI associated with a phone number be made available? Would it be appropriate to develop a statutory administrative scheme to access telephone numbers and the name and address associated with them, to the exclusion of the content of communications?**
- Q.11 Do you have any views as to what conditions or safeguards should be contained in an administrative scheme as it relates to BSI associated with telephones, including cell phones?**
- Q.12 Do you consider that customer information similar to BSI, but in a non-telecommunications context, such as from banks or hotels, could appropriately be made available through a statutory administrative scheme? If so, how should this be done and what conditions or safeguards should be contained in such a scheme? If not, how should this information be obtained?**

Exigent circumstances

As mentioned earlier, requests for voluntary assistance in exigent circumstances have been questioned by some TSPs despite the SCC direction in *Spencer* that the authority to access customer information in exigent circumstances should be unimpeded. As outlined in Rogers' 2015 transparency report, 1,858 requests for BSI in exigent circumstances were rejected.⁸

The challenges associated with TSP provision of BSI in exigent circumstances can be illustrated by a specific instance. In this case, where a child abuse incident was being streamed by the perpetrator live over the Internet, cooperation was only obtained from the TSP when the police, while speaking on the telephone with the TSP, turned up the volume so that the child's cries could be heard over the telephone by the TSP. Only then did the TSP provide the BSI.

Some TSPs have indicated that they prefer not to have to make judgment calls about what constitutes exigent circumstances, but instead prefer clear direction in law. They have

⁸ <http://about.rogers.com/about/helping-our-customers/transparency-report>

indicated they would be willing to provide BSI if they were clearly statutorily authorized to do so.

Given these difficulties, the CWG is of the view that legislation is required to ensure that police are able to respond quickly in urgent situations. For example, situations involving imminent harm, and exigent circumstances, could use an administrative scheme to compel a TSP to provide BSI.⁹

- Q.13 Do you think that exigent circumstances (imminent harm) should be set out in legislation as part of an administrative scheme for access to BSI? If not, please elaborate.**
- Q.14 What specific conditions and safeguards should be considered for provisions designed for exigent circumstances? For example, should these provisions be limited to apply only to certain types of offences? Should they include public reporting, auditing requirements, or other safeguards?**
- Q. 15 Should provisions for such access include provisions for access to other information, which could be precursor/confirmatory information such as confirmation that a phone is active, or other information highly relevant in an emergency situation, such as information about location of a cell phone?**

Missing persons and other non-criminal policing functions

As part of their non-criminal policing duties, police can also need access to BSI. A few examples can further illustrate the situations that were referred to earlier. When a known person is reported missing, but before there is reason to believe a crime has occurred, police may ask a TSP to geolocate that person's phone. When a death occurs, police may need to ask for BSI in order to notify next of kin. If police learn of a risky "selfie" of a young person posted on social media, they may want to visit that youth to engage in some preventative education. In these types of situations, police do not have any basis to obtain a general production order, and in many such instances, time will be of the essence. The TSPs may not agree with the police that the situation is urgent, and may refuse to assist unless the police can demonstrate that it is a matter of life and death.

- Q.16 Do you think that an administrative scheme for access to BSI should include cases involving missing persons or other non-criminal policing functions? If not, please elaborate.**

⁹ Statutory exceptions to the need for prior judicial authorization, so that police are able to act quickly in emergencies, exist in other areas of the *Criminal Code*, for example in s. 184.4 in relation to the interception of private communications, and in s. 487.11 in relation to search warrants.

- Q.17 What specific conditions and safeguards should be considered for an administrative scheme for access to BSI in the context of missing persons and other non-criminal policing functions?**
- Q.18 Should provisions for such access include provisions for access to other information, which could be precursor/confirmatory information such as confirmation that a phone is active, or other information highly relevant in the context of a missing person, such as information about location of a cell phone?**

The Way Forward

Prior to the SCC decision in *Spencer*, there were challenges in accessing BSI in a consistent manner, as assistance was provided on a voluntary basis, and provided in a variety of ways. Post-*Spencer*, these challenges have increased because TSPs are concerned about the legalities of providing voluntary assistance. This is due to their concerns about applying the appropriate level of privacy protection that should be afforded to BSI, and any kind of information about subscribers, which has resulted in a desire to err on the side of caution in many instances.

Most countries with legal systems comparable to Canada's provide for access to BSI without judicial oversight. In many jurisdictions access to BSI is compelled under law through a statute, many of which provide restrictions relating to limiting access as deemed appropriate, in some cases to the type of investigation (such as serious crime) or the level of personnel (senior officials) or other limitations.

Any proposals to codify in law a framework for how investigatory agencies have access to BSI would need to ensure access could be provided in a manner that respected the SCC decision in *Spencer* and the *Canadian Charter of Rights and Freedoms*, and would not be overly burdensome for TSPs or for the agencies requesting the information.

Consolidated List of Consultation Questions

1. Should an IP address form part of the BSI data (i.e. name, address, phone number and email address)? Should it be treated differently from other BSI access? If so, how?
2. Should all investigatory agencies be able to obtain BSI? Should the conditions under which BSI is obtained be different depending on the investigatory agency? Should the framework for provision of BSI include a timeframe within which it must be provided?
3. Is there a reasonable expectation of privacy associated with pre-cursor/confirmatory information? If so, please explain the expectation of privacy associated with this information.
4. What specific conditions should be included in an administrative scheme designed to compel provision of basic pre-cursor/confirmatory information? For example, should there be a designated timeframe to provide this information?
5. Are administrative safeguards such as reporting and audit requirements, advisable or necessary for a scheme providing access to basic pre-cursor/confirmatory information? If you would recommend that such a scheme include safeguards, do you have any views as to which safeguards would be appropriate?
6. What are your views on the recommendation that BSI with greater privacy expectations (i.e., when linked to otherwise anonymous Internet activity) should be obtained by police through a new, specialized production order based on a reasonable grounds to suspect threshold, similar to existing provisions in the *Criminal Code* for access to transmission data and tracking data?
7. How could privacy be assessed in determining whether BSI should be compelled through an administrative scheme or whether judicial authorization should be required to compel its production? For example, should judicial authorization be required for all Internet-related identifiers? Or should this assessment/determination be more contextual, such as considering if there is any intimate details of lifestyle and personal choices that would be revealed, that would otherwise be anonymous online?
8. What specific criteria, including conditions and safeguards should be considered for the decision making process to apply an administrative scheme or seek judicial

- authorization for access to BSI? For example, should the process involve a determination based more on context (e.g., assessing privacy expectations) or should the process be more categorical (e.g., all Internet-based identifiers require judicial authorization) recognizing this more general approach could be considered to provide greater clarity but could also result in protections that are less tailored to the particular expectation of privacy?
9. How should access to BSI be approached in the context of going-forward authorizations, such as transmission data recorder warrants or Part VI authorizations for the interception of private communications? Should those *Criminal Code* powers expressly provide that the BSI be produced as part of those warrants and authorizations? If not, please elaborate.
 10. How should BSI associated with a phone number be made available? Would it be appropriate to develop a statutory administrative scheme to access telephone numbers and the name and address associated with them, to the exclusion of the content of communications?
 11. Do you have any views as to what conditions or safeguards should be contained in an administrative scheme as it relates to BSI associated with telephones, including cell phones?
 12. Do you consider that customer information similar to BSI, but in a non-telecommunications context, such as from banks or hotels, could appropriately be made available through a statutory administrative scheme? If so, how should this be done and what conditions or safeguards should be contained in such a scheme? If not, how should this information be obtained?
 13. Do you think that exigent circumstances (imminent harm) should be set out in legislation as part of an administrative scheme for access to BSI? If not, please elaborate.
 14. What specific conditions and safeguards should be considered for provisions designed for exigent circumstances? For example, should these provisions be limited to apply only to certain types of offences? Should they include public reporting, auditing requirements, or other safeguards?
 15. Should provisions for such access include provisions for access to other information, which could be precursor/confirmatory information such as confirmation that a phone

is active, or other information highly relevant in an emergency situation, such as information about location of a cell phone?

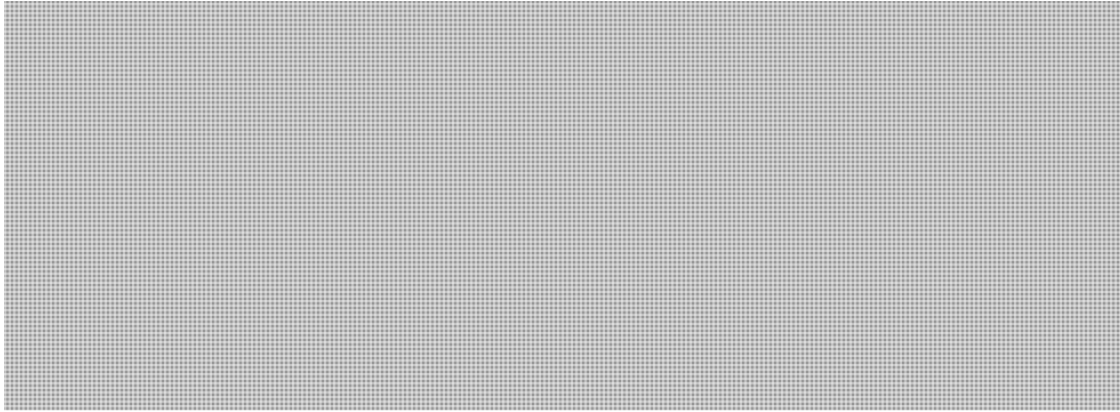
16. Do you think that an administrative scheme for access to BSI should include cases involving missing persons or other non-criminal policing functions? If not, please elaborate.
17. What specific conditions and safeguards should be considered for an administrative scheme for access to BSI in the context of missing persons and other non-criminal policing functions?
18. Should provisions for such access include provisions for access to other information, which could be precursor/confirmatory information such as confirmation that a phone is active, or other information highly relevant in the context of a missing person, such as information about location of a cell phone?

**Pages 139 to / à 140
are withheld pursuant to section
sont retenues en vertu de l'article**

14

**of the Access to Information
de la Loi sur l'accès à l'information**

s.14



COMDO / COMDO (PS/SP)

From: COMDO / COMDO (PS/SP)
Sent: Monday, February 06, 2017 4:03 PM
To: PS.F Media Monitoring / surveillance des médias F.SP
Subject: (UPDATE #4) FYI: Reporter tweets re. Standing Committee w/ RCMP Commissioner Bob Paulson

TondaMacC

Paulson: "I am afraid" of risks of militarization, increased uses of force avail to police vs preventive engagement w/ indiv'ls & commy's.

TondaMacC

Paulson: need more problem solving mentality w/ frontline officers. Asks would you bring carbines, all that gear, to deal w/ a shoplifter?

TondaMacC

Sen. Lang: asks for update on terrorism threat in Cda, foreign fighters.

TondaMacC

Paulson says he will avoid "throwing numbers around" like his colleague at [@csiscanada](#).

TondaMacC

Paulson says [#RCMP](#) is doubling efforts to work w/ local police on "criminal extremists..there's a "more caustic tone to political discourse"

TondaMacC

..which Paulson says is helping to encourage the radicalization of people. But Paulson downplays any suggestion of rise in that extremism.

TondaMacC

Paulson: police continue to investigate if there's evidence/pub interest in laying terror charge against Bissonette.

From: COMDO / COMDO (PS/SP)
Sent: Monday, February 06, 2017 3:03 PM
To: PS.F Media Monitoring / surveillance des médias F.SP
Subject: (UPDATE #3) FYI: Reporter tweets re. Standing Committee w/ RCMP Commissioner Bob Paulson

TondaMacC

Michaud: 43 files under investigation, several perhaps for number of other things, eg threat to life, may be addressed in a diff way.

TondaMacC

Paulson points to Via Rail terror plotters; charged, convicted for more serious offences not terror financing.

TondaMacC

Boniface asks re plan to implement mental health strategy: "As you know, culture can eat policy every day." Paulson: We have some work to do

TondaMacC

Paulson insists the cultural change is underway to address/de-stigmatize impacts of operational stress injuries.

TondaMacC

Paulson cites mandatory training, execs holding commanders to account for failing to treat PTSD seriously as evidence culture has changed.

TondaMacC

Sen. Marylou McPhedran says she's glad to see a woman at the senior table, wants specifics re how allegations of sexual misconduct handled.

TondaMacC

If I understood Craig MacMillan, mandatory consultation with #RCMP conduct authorities re sexual allegations have increased 29 per cent.

TondaMacC

Paulson: sexual misconduct "although very public, not that big a problem in the overall regime" on misconduct within the #RCMP.

TondaMacC

Senators McPhedran/Boniface and Lankin are a respectful but very tough panel of questioners of the #RCMP brass on workplace issues. #SECD

From: COMDO / COMDO (PS/SP)

Sent: Monday, February 06, 2017 2:47 PM

To: PS.F Media Monitoring / surveillance des médias F.SP

Subject: (UPDATE #2) FYI: Reporter tweets re. Standing Committee w/ RCMP Commissioner Bob Paulson

TondaMacC

Kenny & Paulson argue about #RCMP pay, why constables not up to par w/ Cdn counterparts. Paulson says he's asked for more \$\$ "Drop a dime."

TondaMacC

Chief HR officer Dubeau: #RCMP is 72nd for pay/benefits on a list of about 80-odd forces w/ >50 officers, other forces recruit fr RCMP.

TondaMacC

Dubeau says #RCMP has dropped entrance exam, requirement for univ grads, hoping to get more college students into Depot training.

TondaMacC

Dubeau: of 850 #RCMP cadets: 25% women 75% white male. 15% visible minorities 3% aboriginal "The labour market is just not there."

TondaMacC

Paulson: conditions coming together for all this - pay raise, resourcing, systems to prioritize work. (Another way of saying perfect storm?)

TondaMacC

Paulson: target for hiring female #RCMP members is 30%, now at 25% among recruits, won't have a big impact on 21% force-wide rate.

TondaMacC

Dubeau: force-wide target is for 20% visible minorities, 10% aboriginal members, then says he's not sure if he's mixed those up.

TondaMacC

Paulson: intelligence agencies working w/ #RCMP to improve recruitment among them all across the board.

TondaMacC

Lafrance says her mandate is to assess gender, language and ethnic diversity in the #RCMP, not only to boost women in force.

TondaMacC

Lafrance: "Time to switch from focusing on negative, but focus on positive" in #RCMP, not out to reinvent things, won't change overnight.

TondaMacC

Lafrance: I wouldn't have accepted job if didn't believe there was real appetite for change fr the top. Jaffer wants to see her mandate.

TondaMacC

Sen Jaffer: the environment has changed for us in last two weeks, "It's not a good time to be a Muslim." Asks Paulson what hes going to do.

TondaMacC

Sen Jaffer's q specifically addressed risk re sharing of info on Cdns w/ U.S.. Paulson: "We're being careful, we've seen this movie before."

TondaMacC

Jaffer raises @ArarMaher case & family. "No amount compensation w/ help them...I don't want another Maher Arar." Demands specifics.

TondaMacC

Paulson: we're making sure any info we share for purposes of existing laws "is caveated" as Justice O'Connor required post-Arar inquiry.

TondaMacC

Paulson insists guidelines on what #RCMP shares is fully transparent: "The books are open; come and look."

TondaMacC

Sen Dagenais asks if #RCMP mgrs are working to advance the unionization bill or prepare a new one (after senate amended last one).

TondaMacC

Paulson concedes #RCMP has talked to govt. (Not exactly clear whether a new one is in the works).

TondaMacC

Sen. Meredith appears grouchy that #RCMP has shared info re need for greater lawful access w/ Toronto Star & CBC, wants same.

TondaMacC

Paulson says point was to show real impact of clash btwn privacy rights and law enforcement's need for evidence.

TondaMacC

Paulson: police need to be able to validate conditions of peace bonds eg. if someone banned fr computer use, need to know if he's on or not

TondaMacC

Paulson: peace bonds just one tool in the box (Recall that Paulson is the one who made forceful pitch for lower thresholds post Oct '14)

TondaMacC

Ex OPP-chief Gwen Boniface, now a senator, asks Paulson who does intelligence-to-evidence right. Paulson: UK.

TondaMacC

Hey @cforcese..Paulson's quoting you at this cttee o, wrt the intelligence-to-evidence debate.

TondaMacC

Sen Raymonde Saint-Germain asks whether there is need for more collaboration btwn prov'l municipl fed police, in wake of QC shooting.

TondaMacC

#RCMP D/C Michaud points to good collaboration post shooting. Sen asks about beforehand. Michaud-no indication of any info of threat in adv.

TondaMacC

Michaud says while investigation still in early stages, there are no signs of miss

TondaMacC

Sen. Beyak: why only 1 conviction re terror financing, w/ 483 cases flagged in OSFI reports. Paulson: suspicious activity doesn't = crime.

From: COMDO / COMDO (PS/SP)

Sent: Monday, February 06, 2017 1:57 PM

To: PS.F Media Monitoring / surveillance des médias F.SP

Subject: (UPDATE) FYI: Reporter tweets re. Standing Committee w/ RCMP Commissioner Bob Paulson

TondaMacC

Sen. Colin Kenney calls #RCMP harassment settlement process, w/ 6 classes of payment, an "important step." Paulson: "it's much more than \$\$"

TondaMacC

Paulson says organizational changes have come about as a result of #RCMP's desire to deal w/ harassment issues.

TondaMacC

Asked about recruitment, Paulson: #RCMP operates w/ 4-5 per cent vacancy rate in positions nationwide. "I don't accept it as satisfactory"

TondaMacC

Paulson: force is trying to manage it, while arguing transparently for more resources.

TondaMacC

Paulson: #RCMP is trying to risk manage the vacancies. Kenny says "why are you ok w/ that?" BP "I'm not." CK "You sound awfully smug."

TondaMacC

Paulson and Kenny are arguing over what Paulson means. Paulson says he's trying to build an evidence-based case for more staffing resources.

From: COMDO / COMDO (PS/SP)

Sent: Monday, February 06, 2017 1:54 PM

To: PS.F Media Monitoring / surveillance des médias F.SP

Subject: FYI: Reporter tweets re. Standing Committee w/ RCMP Commissioner Bob Paulson

TondaMacC (Toronto Star reporter)

#RCMP Comm Bob Paulson & top brass at #SECD, introduces Louise LaFrance tapped to boost inclusiveness/diversity.

TondaMacC

Paulson: #RCMP has increased training in how to respond to active shooters, also in de-escalation, mandatory for all officers.

TondaMacC

Paulson: police officers are not doctors but should be able to recognize signs of mental illness in those they deal with.

TondaMacC

Paulson: RCMP is aware of risks of militarization of police, creating "us vs them" mentality, force knows it must remain close to comm'ys.

TondaMacC

Paulson: third-party assessment underway on impact of vacancies. re workplace health/safety: stress a real issue which we take seriously.

TondaMacC

Paulson: mgt put in place supports for those w/ mental health struggles. "No tolerance for outdated attitudes" that injuries "not real."

TondaMacC

You can expect the folks seeking to unionize #RCMP will forcefully counter Paulson when they testify after him.

TondaMacC

"Because we mostly get it right," Cdns can be proud of #RCMP, says Paulson.

++++++

Mo Hashash

Communications Duty Officer/ Agent de service des communications
Public Safety Canada / Sécurité publique Canada
Tel.: (613) 991-7010
Email/courriel: ps.comdo-comdo.sp@canada.ca

Today's News / Actualités
February 6, 2017 / le 6 février 2017
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / LES FEMMES ET LES FILLES
AUTOCHTONES DISPARUES ET ASSASSINEES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

Since Trump order, 200 have lost access to Nexus: public safety minister

The federal public safety minister says *about 200 people have been unable to use their Nexus cards to cross the American border since U.S. President Donald Trump ordered a temporary halt to immigration from certain countries.* Ralph Goodale says *none of the 200 are Canadian citizens and the government continues to work to make sure citizens are treated fairly at the border.* But he says *Nexus is a discretionary program to expedite processing at the border and each country has the right to withdraw the privilege.* The program allows citizens and permanent residents in both Canada and the U.S. to be pre-screened for clearance in a bid to speed up border crossings. But on Jan. 27, Trump banned those holding passports in seven specific countries from entering the U.S., and since

Dubeau: of 850 #RCMP cadets: 25% women 75% white male. 15% visible minorities 3% aboriginal "The labour market is just not there."

TondaMacC

Paulson: conditions coming together for all this - pay raise, resourcing, systems to prioritize work. (Another way of saying perfect storm?)

TondaMacC

Paulson: target for hiring female #RCMP members is 30%, now at 25% among recruits, won't have a big impact on 21% force-wide rate.

TondaMacC

Dubeau: force-wide target is for 20% visible minorities, 10% aboriginal members, then says he's not sure if he's mixed those up.

TondaMacC

Paulson: intelligence agencies working w/ #RCMP to improve recruitment among them all across the board.

TondaMacC

Lafrance says her mandate is to assess gender, language and ethnic diversity in the #RCMP, not only to boost women in force.

TondaMacC

Lafrance: "Time to switch from focusing on negative, but focus on positive" in #RCMP, not out to reinvent things, won't change overnight.

TondaMacC

Lafrance: I wouldn't have accepted job if didn't believe there was real appetite for change fr the top. Jaffer wants to see her mandate.

TondaMacC

Sen Jaffer: the environment has changed for us in last two weeks, "It's not a good time to be a Muslim." Asks Paulson what he's going to do.

TondaMacC

Sen Jaffer's q specifically addressed risk re sharing of info on Cdns w/ U.S.. Paulson: "We're being careful, we've seen this movie before."

TondaMacC

Jaffer raises @ArarMaher case & family. "No amount compensation w/ help them...I don't want another Maher Arar." Demands specifics.

TondaMacC

Paulson: we're making sure any info we share for purposes of existing laws "is caveated" as Justice O'Connor required post-Arar inquiry.

TondaMacC

Paulson insists guidelines on what #RCMP shares is fully transparent: "The books are open; come and look."

TondaMacC

Sen Dagenais asks if #RCMP mgrs are working to advance the unionization bill or prepare a new one (after senate amended last one).

TondaMacC

Paulson concedes #RCMP has talked to govt. (Not exactly clear whether a new one is in the works).

TondaMacC

Sen. Meredith appears grouchy that #RCMP has shared info re need for greater lawful access w/ Toronto Star & CBC, wants same.

TondaMacC

Paulson says point was to show real impact of clash btwn privacy rights and law enforcement's need for evidence.

Levert, Jean-Philippe (PS/SP)

From: Bardsley, Scott (PS/SP)
Sent: Wednesday, February 15, 2017 10:36 AM
To: Media Relations / Relations avec les médias (PS/SP)
Cc: Holland, Alyx (PS/SP); Brien, Dan (PS/SP); Peirce, Hilary (PS/SP); Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP)
Subject: RE: La Presse on cell phone access
Attachments: CBSA searches of cell phones and electronic devices at the border.docx

Can you please update the translation of our draft response with the attached revisions describing CBSA's operational procedures?

Please share it with CBSA, noting that we're open to modifying it based on CBSA's response.

Scott

From: Media Relations / Relations avec les médias (PS/SP)
Sent: Tuesday, February 14, 2017 5:07 PM
To: Bardsley, Scott (PS/SP); Media Relations / Relations avec les médias (PS/SP)
Cc: Holland, Alyx (PS/SP); Brien, Dan (PS/SP); Peirce, Hilary (PS/SP); Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP)
Subject: RE: La Presse on cell phone access

Will do.
JP Levert

From: Bardsley, Scott (PS/SP)
Sent: Tuesday, February 14, 2017 5:05 PM
To: Media Relations / Relations avec les médias (PS/SP)
Cc: Holland, Alyx (PS/SP); Brien, Dan (PS/SP); Peirce, Hilary (PS/SP); Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP)
Subject: RE: La Presse on cell phone access

Thanks again for this. I spoke with the reporter and he is ok with a response tomorrow morning.

Please let me know when CBSA's lines are ready. My colleague has obtained a policy summary and we have a good story to tell.

Scott

From: Media Relations / Relations avec les médias (PS/SP)
Sent: Tuesday, February 14, 2017 3:14 PM
To: Bardsley, Scott (PS/SP); Media Relations / Relations avec les médias (PS/SP)
Cc: Holland, Alyx (PS/SP); Brien, Dan (PS/SP); Peirce, Hilary (PS/SP); Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP)
Subject: RE: La Presse on cell phone access

Voilà!
JP Levert

From: Bardsley, Scott (PS/SP)
Sent: Tuesday, February 14, 2017 12:15 PM
To: Media Relations / Relations avec les médias (PS/SP)
Cc: Holland, Alyx (PS/SP); Brien, Dan (PS/SP); Peirce, Hilary (PS/SP); Tomlinson, Jamie (PS/SP); Baker3, Ryan

(PS/SP)

Subject: RE: La Presse on cell phone access

End of the afternoon would be great, thanks. And ok.

s.19(1)

Scott

From: Media Relations / Relations avec les médias (PS/SP)

Sent: Tuesday, February 14, 2017 12:14 PM

To: Bardsley, Scott (PS/SP); Media Relations / Relations avec les médias (PS/SP)

Cc: Holland, Alyx (PS/SP); Brien, Dan (PS/SP); Peirce, Hilary (PS/SP); Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP)

Subject: RE: La Presse on cell phone access

Will do. When do you need the lines by?

Also, CBSA will provide a translated version of their response.

JP

From: Bardsley, Scott (PS/SP)

Sent: Tuesday, February 14, 2017 12:10 PM

To: Media Relations / Relations avec les médias (PS/SP)

Cc: Holland, Alyx (PS/SP); Brien, Dan (PS/SP); Peirce, Hilary (PS/SP); Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP)

Subject: RE: La Presse on cell phone access

To complement that work, can you please also task a translation of MO's current lines on cell phone searches? (attached)

They don't yet have information related Q1 below, but are a good start.

Scott

From: Media Relations / Relations avec les médias (PS/SP)

Sent: Tuesday, February 14, 2017 11:44 AM

To: Bardsley, Scott (PS/SP); Media Relations / Relations avec les médias (PS/SP)

Cc: Holland, Alyx (PS/SP); Brien, Dan (PS/SP); Peirce, Hilary (PS/SP); Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP)

Subject: RE: La Presse on cell phone access

Will do.

JP Levert

From: Bardsley, Scott (PS/SP)

Sent: Tuesday, February 14, 2017 11:42 AM

To: Media Relations / Relations avec les médias (PS/SP)

Cc: Holland, Alyx (PS/SP); Brien, Dan (PS/SP); Peirce, Hilary (PS/SP); Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP)

Subject: La Presse on cell phone access

Dear Media Relations,

██████████ from La Presse ██████████ @lapresse.ca, ██████████ called with a variety of questions related to Canadian and American border guards' access to cell phones and social media accounts.

Can you please ask CBSA to prepare lines for later this afternoon on:

1. Their protocols/procedures for how they search cell phones or other electronic devices (e.g. are they documented, does an officer need reasonable grounds to suspect, etc.)
2. Are such searches limited to the data on the device itself? (e.g. can they use an unlocked phone to browse someone's social media accounts via the internet?)
3. If there are any statistics on how often they conduct such searches.
4. Does CBSA have the authority to ask someone for their social media account password? Does it?

I understand that he already has an existing request with a CBSA media relations officer in Quebec, so work on some of these questions may already be underway.

Scott

CBSA searches of cell phones and electronic devices at the border

CBSA officers are trained to conduct all border examinations with as much respect for privacy as possible.

Formatted: Normal, Indent: Left: 0"

Their policy is to not routinely examine the contents of cell phone or other electronic devices. Officers may only conduct a search if there are multiple indicators that evidence of contraventions may be found on a device. Their initial examinations are cursory in nature and only increase in intensity based on emerging indicators.



Officers must disable the device's wireless and internet connectivity to help ensure that the examination is only of material stored on the device. They cannot compel a person to log into external accounts.





Formatted: Normal, No bullets or numbering

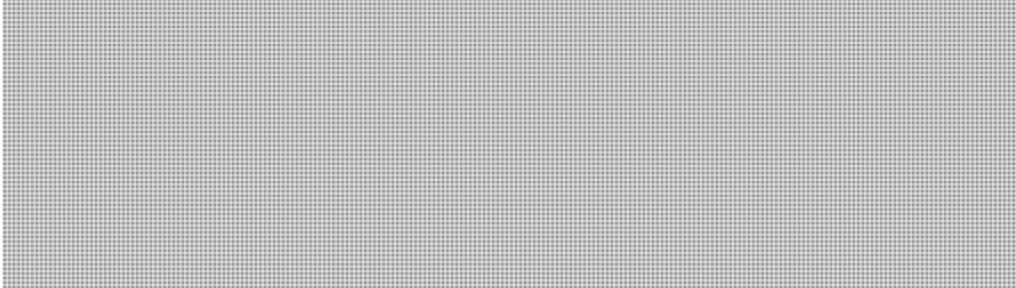
Background on CBSA authorities

Formatted: Normal, Indent: Left: 0"

Formatted: Font: Bold

Formatted: Indent: Left: 0.13", Hanging: 0.25"

- Canadian courts have generally recognized that people should have reduced expectations of privacy at border points. In this special context, privacy and other Charter rights are limited to allow the enforcement of immigration, taxation and security policy.
- All persons, including Canadian citizens, seeking entry to Canada must present to the CBSA and may be subject to a more in-depth exam (secondary inspection).
- Secondary inspections are a part of the normal cross-border travel process and border services officers are trained to perform these examinations in a courteous, respectful and professional manner.
- As with other goods crossing the border, travellers are legally obligated under the Customs Act to present their electronic devices for inspection by the CBSA.
- 
- Electronic devices and media, including laptops, cell phones and other devices are classified as 'goods' in the context of the border and CBSA officers have the lawful authority to examine them as part of a routine examination.
- 



Fouilles des téléphones cellulaires et des appareils électroniques par l'ASFC à la frontière

- Les tribunaux canadiens ont généralement reconnu que les gens devraient avoir des attentes réduites en matière de protection des renseignements personnels aux postes frontaliers. Dans ce contexte particulier, les droits en matière de protection des renseignements personnels et autres droits prévus par la Charte sont limités afin de permettre l'application des politiques en matière d'immigration, de fiscalité et de sécurité.
- Toutes les personnes, y compris les citoyens canadiens qui cherchent à entrer au Canada doivent se présenter à l'ASFC et peuvent faire l'objet d'un examen plus approfondi (inspection secondaire).
- Les inspections secondaires font partie du processus de déplacement transfrontalier normal et les agents des services frontaliers sont formés afin d'effectuer ces examens d'une manière courtoise, respectueuse et professionnelle.
- Comme pour les autres marchandises qui traversent la frontière, les voyageurs sont légalement tenus en vertu de la *Loi sur les douanes* de présenter leurs appareils électroniques aux fins d'inspection par l'ASFC.



- Les appareils et supports électroniques, y compris les ordinateurs portatifs, les téléphones cellulaires et d'autres appareils, entrent dans la catégorie des « marchandises » dans le contexte de la frontière et les agents de l'ASFC ont le pouvoir légal de les examiner dans le cadre d'un examen de routine.



Levert, Jean-Philippe (PS/SP)

From: Giolti, Patrizia <Patrizia.Giolti@cbsa-asfc.gc.ca>
Sent: Thursday, February 16, 2017 7:50 PM
To: Christine O'Nions
Cc: Lindblad, Anabel; CBSA-ASFC-Media Relations; Media Relations / Relations avec les médias (PS/SP); CBSA-ASFC_Issues_Management-Gestion_des_questions;
Subject: Communications Issues Management / Communications Gestion des Enjeux (PS/SP)
For awareness - media query electronic devices

Hello - media query for your awareness...thanks

Reporter: ██████████ CBC

Issue: electronic devices and the CBSA - in the U.S., Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) conducted a Privacy Impact Assessment in 2009 for Border Searches of Electronic Devices.

Questions and answers:

Has CBSA conducted a Privacy Impact Assessment of its own for border searches of electronic devices? If so, could CBSA share a copy of the PIA? If a PIA has not been conducted, why not? If not already answered, under what circumstances does CBSA conduct a search of an electronic device? Are there any formal policies or procedures in place that dictate when, how, and by whom a search is conducted?

- The CBSA has not completed a PIA for the examination of electronic devices at the border; however, it has begun the process internally. We are not in a position to provide timelines at this time. Border Services Officers (BSOs) are currently guided by an Operational Bulletin that explains the current legislative framework as well as current CBSA policies regarding the examination of electronic devices.
- The CBSA is committed to maintaining the balance between an individual's right to privacy and the safety and security of Canadians. As such, BSOs are trained to conduct all border examinations with as much respect for privacy as possible.
- All persons, including Canadian citizens, seeking entry to Canada must present themselves to the CBSA and may be subject to a more in-depth exam (secondary inspection).
- Secondary inspections are a part of the normal cross-border travel process and border services officers are trained to perform these examinations in a courteous, respectful and professional manner. As with other goods crossing the border, travellers are legally obligated under the Customs Act to present their electronic devices for inspection by the CBSA.
- Electronic devices and media, including laptops, cell phones and other devices are classified as 'goods' in the context of the border and CBSA officers have the lawful authority under section 99 of the Customs Act to examine them as part of a routine examination.
- Examination of digital devices and media must always be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods. While examination conducted under the authority of section 99 of the Customs Act do not require reasonable grounds to suspect or believe that a contravention has

occurred, it is the CBSA's policy that such examinations should only occur where there is a multiplicity of indicators, or further to the discovery of undeclared, prohibited, or falsely reported goods. Initial examinations of digital devices and media should be cursory in nature and increase in intensity based on emerging indicators

- The examination of electronic goods is a tool used to uncover a range of border-related offences, ranging from electronic receipts proving that goods were undervalued or undeclared, to the interception of prohibited goods contained within the devices themselves (child pornography, obscenity, etc.).

Does CBSA keep statistics on the number of border searches of electronic devices it conducts? If so, how many border searches of electronic devices did CBSA conduct each year for the last five years?

The CBSA does not keep this statistic

Does CBSA copy data from the devices that it searches? If so...

- o Where is this data stored?
- o How long is the data retained?
- o Who has access to the data?
- o Is this data shared with other agencies in Canada?
- o Is the data shared with agencies in the US?
- o Of the number of searches conducted last year, how many times was data copied?

The CBSA may only collect data for customs purposes and may only disclose customs information if authorized to do so under section 107 of the Customs Act.

Does the CBSA ask travellers for the passwords to their social media accounts?

- No. CBSA officers shall only examine what is stored within a device and is therefore being imported. Officers are not to read emails or consult social media accounts on the traveller's digital device unless the information is already downloaded and has been opened (usually marked as read) and is therefore stored on the device. As such, CBSA officers shall disable wireless and Internet connectivity (i.e. set to airplane mode) when possible to limit the ability of the device to connect to remote hosts or services.
- That being said, individuals also have the obligation under section 13 of the Customs Act to present and open their goods if requested to do so by a BSO. Because a password can be required to open and examine documents on an electronic device, it can be compelled to allow for the traveller's obligations to be fulfilled. Failure to provide a password can result in the detention or seizure of the electronic device.
- The CBSA is committed to maintaining the balance between an individual's right to privacy and the safety and security of Canadians. As such, BSOs are trained to conduct all border examinations with as much respect for privacy as possible.

Levert, Jean-Philippe (PS/SP)

From: Bardsley, Scott (PS/SP)
Sent: Friday, February 17, 2017 9:59 AM
To: Media Relations / Relations avec les médias (PS/SP)
Cc: Brien, Dan (PS/SP); Baker3, Ryan (PS/SP); Peirce, Hilary (PS/SP); Tomlinson, Jamie (PS/SP)
Subject: RE: 'How would you know what your rights are?': Secret policies govern cellphone searches at the Canadian border

Ok, thanks! I have sent him a note asking him to correct his characterization that "the Canadian government has not made public its policies on how those searches are conducted — or even revealed if formal policies exist at all.... In the absence of a formal policy...".

Scott

From: Media Relations / Relations avec les médias (PS/SP)
Sent: Friday, February 17, 2017 9:30 AM
To: Bardsley, Scott (PS/SP); Media Relations / Relations avec les médias (PS/SP)
Cc: Brien, Dan (PS/SP); Baker3, Ryan (PS/SP); Peirce, Hilary (PS/SP); Tomlinson, Jamie (PS/SP)
Subject: RE: 'How would you know what your rights are?': Secret policies govern cellphone searches at the Canadian border

Oups!

Here you go:

Reporter: [REDACTED] CBC

Issue: electronic devices and the CBSA - in the U.S., Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) conducted a Privacy Impact Assessment in 2009 for Border Searches of Electronic Devices.

Questions and answers:

Has CBSA conducted a Privacy Impact Assessment of its own for border searches of electronic devices? If so, could CBSA share a copy of the PIA? If a PIA has not been conducted, why not? If not already answered, under what circumstances does CBSA conduct a search of an electronic device? Are there any formal policies or procedures in place that dictate when, how, and by whom a search is conducted?

- The CBSA has not completed a PIA for the examination of electronic devices at the border; however, it has begun the process internally. We are not in a position to provide timelines at this time. Border Services Officers (BSOs) are currently guided by an Operational Bulletin that explains the current legislative framework as well as current CBSA policies regarding the examination of electronic devices.
- The CBSA is committed to maintaining the balance between an individual's right to privacy and the safety and security of Canadians. As such, BSOs are trained to conduct all border examinations with as much respect for privacy as possible.
- All persons, including Canadian citizens, seeking entry to Canada must present themselves to the CBSA and may be subject to a more in-depth exam (secondary inspection).
- Secondary inspections are a part of the normal cross-border travel process and border services officers are trained to perform these examinations in a courteous, respectful and professional manner. As with other

goods crossing the border, travellers are legally obligated under the Customs Act to present their electronic devices for inspection by the CBSA.

- Electronic devices and media, including laptops, cell phones and other devices are classified as 'goods' in the context of the border and CBSA officers have the lawful authority under section 99 of the Customs Act to examine them as part of a routine examination.
- Examination of digital devices and media must always be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods. While examination conducted under the authority of section 99 of the Customs Act do not require reasonable grounds to suspect or believe that a contravention has occurred, it is the CBSA's policy that such examinations should only occur where there is a multiplicity of indicators, or further to the discovery of undeclared, prohibited, or falsely reported goods. Initial examinations of digital devices and media should be cursory in nature and increase in intensity based on emerging indicators
- The examination of electronic goods is a tool used to uncover a range of border-related offences, ranging from electronic receipts proving that goods were undervalued or undeclared, to the interception of prohibited goods contained within the devices themselves (child pornography, obscenity, etc.).

Does CBSA keep statistics on the number of border searches of electronic devices it conducts? If so, how many border searches of electronic devices did CBSA conduct each year for the last five years?

The CBSA does not keep this statistic

Does CBSA copy data from the devices that it searches? If so...

- o Where is this data stored?
- o How long is the data retained?
- o Who has access to the data?
- o Is this data shared with other agencies in Canada?
- o Is the data shared with agencies in the US?
- o Of the number of searches conducted last year, how many times was data copied?

The CBSA may only collect data for customs purposes and may only disclose customs information if authorized to do so under section 107 of the Customs Act.

Does the CBSA ask travellers for the passwords to their social media accounts?

- No. CBSA officers shall only examine what is stored within a device and is therefore being imported. Officers are not to read emails or consult social media accounts on the traveller's digital device unless the information is already downloaded and has been opened (usually marked as read) and is therefore stored on the device. As such, CBSA officers shall disable wireless and Internet connectivity (i.e. set to airplane mode) when possible to limit the ability of the device to connect to remote hosts or services.
- That being said, individuals also have the obligation under section 13 of the Customs Act to present and open their goods if requested to do so by a BSO. Because a password can be required to open and examine documents on an electronic device, it can be compelled to allow for the traveller's obligations to be fulfilled. Failure to provide a password can result in the detention or seizure of the electronic device.

The CBSA is committed to maintaining the balance between an individual's right to privacy and the safety and security of Canadians. As such, BSOs are trained to conduct all border examinations with as much respect for privacy as possible.

s.19(1)

From: Bardsley, Scott (PS/SP)
Sent: Friday, February 17, 2017 9:17 AM
To: Media Relations / Relations avec les médias (PS/SP)
Cc: Brien, Dan (PS/SP); Baker3, Ryan (PS/SP); Peirce, Hilary (PS/SP); Tomlinson, Jamie (PS/SP)
Subject: RE: 'How would you know what your rights are?': Secret policies govern cellphone searches at the Canadian border

We're good on La Presse. It's the CBC piece by [REDACTED] below that I'm interested in.

Scott

From: Media Relations / Relations avec les médias (PS/SP)
Sent: Friday, February 17, 2017 9:14 AM
To: Bardsley, Scott (PS/SP); Media Relations / Relations avec les médias (PS/SP)
Cc: Brien, Dan (PS/SP); Baker3, Ryan (PS/SP); Peirce, Hilary (PS/SP); Tomlinson, Jamie (PS/SP)
Subject: RE: 'How would you know what your rights are?': Secret policies govern cellphone searches at the Canadian border

Hi Scott,
I sent you the French version of CBSA's response yesterday morning. (See below and attached)
Do you need the English one?

Thanks,
JP Levert

Please see CBSA's approved response for LaPresse below.
CBSA is asking if PSC or CBSA should provide the response, but I know that you provided one last night.

Please advise.

Thanks,

JP Levert

Reporter : [REDACTED] La Presse

Issue: Electronic devices

Quels sont les protocoles ou procédures sur la fouille des cellulaires ou autres appareils électroniques (p. ex. les fouilles sont-elles documentées, l'agent doit-il avoir des motifs raisonnables de soupçonner... etc.)

L'Agence des services frontaliers du Canada (ASFC) peut seulement aborder son rôle. L'ASFC s'engage à maintenir l'équilibre entre le droit des personnes à la vie privée et la sécurité des Canadiens. Par conséquent, les agents des services frontaliers reçoivent de la formation pour mener toutes les inspections à la frontière dans le plus grand respect possible pour la vie privée des personnes.

Toutes les personnes qui veulent entrer au Canada doivent se présenter à un point d'entrée et se soumettre à une inspection approfondie, au besoin.

L'inspection secondaire fait partie du processus normal du passage à la frontière. Les agents des services frontaliers sont formés pour l'effectuer de façon courtoise, respectueuse et professionnelle. Comme pour toute marchandise passant la frontière, les voyageurs sont tenus de remettre leurs appareils électroniques à l'ASFC aux fins d'inspection en vertu de la Loi sur des douanes.

Les appareils et les médias électroniques, y compris les ordinateurs portables, les cellulaires et les autres appareils, sont classés comme étant des « marchandises » à la frontière et les agents de l'ASFC sont autorisés en vertu de l'article 99 de la Loi sur les douanes à les examiner dans le cadre de leurs inspections de routine.

L'examen d'appareils ou de supports numériques doit toujours être motivé par un lien clair avec l'application ou l'exécution de la législation frontalière, prévue dans le mandat de l'ASFC, qui régit la circulation transfrontalière des personnes et des marchandises. Malgré le fait que les inspections en vertu de l'article 99 de la Loi sur les douanes n'exigent pas la présence de motifs raisonnables de soupçonner ou de croire qu'il y aurait une infraction, l'ASFC a comme politique d'effectuer des examens d'appareils électroniques que lorsqu'ils sont en présence d'une multiplicité d'indicateurs, ou par suite de la découverte de marchandises non déclarées, faussement déclarées ou prohibées.

Les fouilles se limitent-elles aux données stockées sur l'appareil? Par exemple, les agents peuvent-ils utiliser l'appareil déverrouillé pour consulter les comptes de médias sociaux de la personne sur Internet?)

Les agents de l'ASFC examinent uniquement ce qui est stocké dans l'appareil et ont alors été importés. Ils ne doivent pas lire les courriels ou consulter les comptes de médias sociaux sur l'appareil du voyageur, sauf si ceux-ci ont déjà été téléchargés et ouverts (habituellement marqués comme « lus ») et sont ainsi stockés sur l'appareil. C'est ainsi qu'avant de procéder à l'examen d'appareils et de supports numériques, les agents doivent, si possible, désactiver les fonctions de communication sans fil et par Internet (en activant le mode Avion) afin d'empêcher l'appareil de se connecter à un hôte ou à des services distants.

Y-a-t-il des statistiques sur la fréquence de ces fouilles?

L'ASFC ne détient pas ces statistiques.

L'ASFC peut-elle exiger d'une personne le mot de passe de ses comptes sur les médias sociaux? Le fait-elle?

Les personnes sont aussi tenues, en vertu de l'article 13 de la Loi sur les douanes, de présenter et d'ouvrir leurs marchandises à la demande d'un agent des services frontaliers. Comme un mot de passe peut être requis pour ouvrir et examiner des documents sur un appareil électronique, les voyageurs peuvent être sommés de les fournir afin de satisfaire à leurs obligations. Le refus de fournir un mot de passe peut mener à la détention ou à la saisie de l'appareil électronique.

L'ASFC s'engage à maintenir l'équilibre entre le droit des personnes à la vie privée et la sécurité des Canadiens. Par conséquent, les agents des services frontaliers reçoivent de la formation pour mener toutes les inspections à la frontière dans le plus grand respect possible pour la vie privée des personnes.

Jean-Philippe Levert

Communications Officer | Agent de communications
Issues Management Team, Public Affairs Division | Gestion des enjeux, Affaires publiques
Public Safety Canada | Sécurité publique Canada
T (New) : 613-991-0657 | F : 613-954-4779
Bb: 613-220-5201



From: Bardsley, Scott (PS/SP)
Sent: Friday, February 17, 2017 6:49 AM
To: Media Relations / Relations avec les médias (PS/SP)
Cc: Brien, Dan (PS/SP); Baker3, Ryan (PS/SP); Peirce, Hilary (PS/SP); Tomlinson, Jamie (PS/SP)
Subject: Fw: 'How would you know what your rights are?': Secret policies govern cellphone searches at the Canadian border

Dear Media Relations,

Can we please find out what is the status of CBSA's reply to this story and what the questions were? The reporter suggests it's still in progress.

Scott

published: 2017-02-17 05:00 (EST)

received: 2017-02-17 05:35 (EST)

CBC.ca: Top Stories

Words: 1,076

'How would you know what your rights are?': Secret policies govern cellphone searches at the Canadian border

When you travel to the U.S., customs agents can search your smartphone, laptop and other electronic devices at will - a longtime policy that has attracted renewed scrutiny in light of President Donald Trump's controversial immigration ban.

What you may not realize is Canadian customs agents can do the same.

But unlike the U.S., the Canadian government has not made public its policies on how those searches are conducted - or even revealed if formal policies exist at all.

Legal experts say that lack of transparency makes it difficult for travellers to know their rights when a Canadian border agent asks to conduct a digital search.

"The border is a place that makes people nervous. You are not inclined to assert your rights, if you even know what they are, which many people don't," says Rob Currie, a law professor at Dalhousie University and director of the Law & Technology Institute at the Schulich School of Law. "And in this case, how would you know what your rights are?"

What is known is that the Canada Border Services Agency (CBSA) doesn't need a warrant to search your phone or laptop, which both fall under the Customs Act's broader definition of "goods."

But how that search is conducted - whether agents can compel you to turn over your password, say, or make a copy of the data on your device - remains unclear.

The U.S. government, on the other hand, published its policy on electronic device searches in 2009.

"I don't know if it's simply not available, not advertised or literally does not exist," says lawyer Micheal Vonn, policy director of the British Columbia Civil Liberties Association (BCCLA).

"And I don't know that it ... would be to their benefit to put any of that in writing."

CBSA did not respond to multiple requests for comment, including an emailed list of questions about its border search policies, such as how often electronic-device searches take place.

'An invitation to abuse'

In the absence of a formal policy, it's not clear:

- How a Canadian customs officer decides to search a traveller's phone, laptop or electronic device, and how that search is conducted.
- Under what circumstances data is copied or download from a device, how long the data is retained and with which agencies the data is shared.
- How searches of electronic devices are tracked, if they are tracked at all.

If search-related decisions are made at the discretion of an officer - rather than based on a formal policy - it gives "a lot of latitude" to the front line, according to Vonn. "And when you're talking about people's rights, you must shape discretion. Not to do so is an invitation to abuse," she said.

The U.S. Department of Homeland Security - which includes Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) - conducted a review of its practices in 2009. It is available for anyone to access online.

The review, known as a privacy impact assessment, outlines how U.S. customs agencies perform searches, what they do with the data copied from devices, how long the data is retained for, and the circumstances under which seized data can be shared with U.S. and international law enforcement agencies.

The Office of the Privacy Commissioner of Canada says it has never received a similar privacy impact assessment from CBSA, according to spokesperson Tobi Cohen.

'Interim guidelines' offer a glimpse

Perhaps the closest thing to an official CBSA policy on device searches are internal interim guidelines dating from June 2015, obtained via access-to-information legislation and shared with the BCCLA by an unidentified source.

At that time, CBSA told officers that "although there is no defined threshold for grounds to examine such devices, CBSA's current policy is that such examinations should not be conducted as a matter of routine."

Officers could request passwords - though not for information stored "remotely or online." And if a traveller refuses, the device could be detained for a forensic examination.

"Could they copy it all and go through it all?" asks Vonn. "Yes. I have no understanding that there's any impediment to them doing it if they can get in."

Currie, however, suspects that border agents would still need a warrant to perform a forensic search, but couldn't say for sure - and the issue hasn't been tested in court.

CBSA also recommended at the time that officers not arrest a traveller "solely for refusing to provide a password" - pending the outcome of a highly publicized court case - even though the agency believed "such actions appear to be legally supported." (The court case was resolved last August through a guilty plea and \$500 fine, meaning some of these troublesome questions never played out in a judicial setting.)

As a result, both Vonn and Currie say it's not clear whether CBSA still favours this recommendation.

"We've been really urging people not to take this as the state of play," Vonn says.

Who's going to challenge the government?

There are a few reasons, according to legal experts, for the lack of clarity.

One is that there has been a lack of constitutional challenges in Canada, which would have the potential to force CBSA to reveal more about its practices in court - namely around compelling travellers to hand over their passwords and for the searches themselves, which are two separate issues, Currie says.

Part of the problem is that most people don't have an incentive to launch a potentially costly and time-consuming legal challenge, says Vonn.

"Who, in the ordinary spectrum of people who are just crossing the border because they need to for business, or they need to go to a conference, or they want to go shopping - who's going to take that on? Almost nobody."

Another reason is CBSA might argue that guidance governing electronic-device searches already exists - albeit as decades-old law, written before smartphones and computers were commonplace, which has been re-interpreted to apply to present-day technology.

Under this interpretation, the search of a phone is equivalent to the search of a suitcase, as both are "goods," even if one is capable of holding much more personal information.

As a result, says Currie, CBSA's approach to searching electronic devices is "based around these very broad search powers that they have in the Customs Act - most of which were written in the 70s and were not designed to accommodate the privacy interest in these devices."

For the online article click [here](#).

Sent from my BlackBerry 10 smartphone on the Rogers network.

s.19(1)

Levert, Jean-Philippe (PS/SP)

From: Media Relations / Relations avec les médias (PS/SP)
Sent: Tuesday, February 21, 2017 5:32 PM
To: Bardsley, Scott (PS/SP); Media Relations / Relations avec les médias (PS/SP)
Cc: Brien, Dan (PS/SP); Peirce, Hilary (PS/SP); Holland, Alyx (PS/SP); Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP)
Subject: RE: Query on electronic devices

Hi Scott

As requested, here is the CBSA's response to two of [REDACTED]'s questions. They plan to send this to him right away and develop further responses for the other questions later (but as soon as possible).

Questions:

As I understand it, the Interim Guidelines from June 2015 published by the BCCLA are also the official guidelines still in use today. However, those interim guidelines contain the following paragraph:

"Until further instructions are issued, CBSA officers shall not arrest a traveller for hindering (Section 153.1 of the Customs Act) or for obstruction (paragraph 129(1)(d) of IRPA) solely for refusing to provide a password. Though such actions appear to be legally supported, a restrained approach will be adopted until the matter is settled in ongoing court proceedings."

No further instructions have been issued and this approach is still being applied. As such, the attached policy guidelines are still in force with respect to examinations of electronic goods as well as for arrest guidelines.

Could CBSA clarify whether or not this "restrained approach" is still the current approach?

Could I have a copies of both the Operational Bulletin, and the aforementioned current CBSA policies regarding the examination of electronic devices that guide the current approach?

No additional CBSA policies have been issued. The Operational Bulletin issued in 2015 remains in force today (see attached)

Thanks
-Andrew

Andrew Gowing
Senior Advisor & Spokesperson | Conseiller principal et porte-parole
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : (613) 991-1689
Blackberry : (613) 808-5414
Email | Courriel : Andrew.Gowing@Canada.ca

From: Bardsley, Scott (PS/SP)
Sent: Tuesday, February 21, 2017 8:43 AM
To: Media Relations / Relations avec les médias (PS/SP)
Cc: Brien, Dan (PS/SP); Peirce, Hilary (PS/SP); Holland, Alyx (PS/SP); Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP)
Subject: FW: Query on electronic devices

Dear PS Media Relations,

Can you please flag to CBSA that MO would like to see a copy their response to [REDACTED] (below) for awareness? Thanks,

Scott

From: [redacted] [mailto:[redacted]@cbc.ca]
Sent: Tuesday, February 21, 2017 8:36 AM
To: Bardsley, Scott (PS/SP)
Subject: Fwd: Query on electronic devices

Hi Scott—

Hope you had a good weekend. I sent a few follow-up questions to CBSA this morning, and just wanted to flag them for you as well in case PS has anything to add.

Thanks,
[redacted]

----- Forwarded message -----

From: [redacted]@cbc.ca>
Date: Tue, Feb 21, 2017 at 8:02 AM
Subject: Re: Query on electronic devices
To: "Giolti, Patrizia" <Patrizia.Giolti@cbsa-asfc.gc.ca>

Hi Patrizia—

Thanks for sending this response along, and apologies for not replying directly on Friday (I was offsite and wanted to prioritize updating our story with the little time I had).

I do have a few more questions I'm hoping you can answer by end of day today, but let me as soon as you can if this isn't reasonable.

- Can you elaborate on what the PIA will cover?
- As I understand it, the Interim Guidelines from June 2015 published by the BCCLA are also the official guidelines still in use today. However, those interim guidelines contain the following paragraph:

"Until further instructions are issued, CBSA officers shall not arrest a traveller for hindering (Section 153.1 of the Customs Act) or for obstruction (paragraph 129(1)(d) of IRPA) solely for refusing to provide a password. Though such actions appear to be legally supported, a restrained approach will be adopted until the matter is settled in ongoing court proceedings."

Could CBSA clarify whether or not this "restrained approach" is still the current approach?

- Could I have a copies of both the Operational Bulletin, and the aforementioned current CBSA policies regarding the examination of electronic devices that guide the current approach?
- In your previous response, you mentioned that "The CBSA may only collect data for customs purposes and may only disclose customs information if authorized to do so under section 107 of the Customs Act." Does this mean that CBSA can copy, store, and share data collected from an electronic device? And if so, how long is such data retained?
- Finally, what rights exactly does CBSA believe Canadians have at borders? What about foreign travellers?

Thanks,
[redacted]

On Fri, Feb 17, 2017 at 8:59 AM, Giolti, Patrizia <Patrizia.Giolti@cbsa-asfc.gc.ca> wrote:

Hello [REDACTED] following your questions on electronic devices and the CBSA, please note below. Should you have other questions please do not hesitate to connect with us.

Best, Patrizia

s.19(1)

Questions and answers:

Has CBSA conducted a Privacy Impact Assessment of its own for border searches of electronic devices? If so, could CBSA share a copy of the PIA? If a PIA has not been conducted, why not? If not already answered, under what circumstances does CBSA conduct a search of an electronic device? Are there any formal policies or procedures in place that dictate when, how, and by whom a search is conducted?

- The CBSA has not completed a PIA for the examination of electronic devices at the border; however, it has begun the process internally. We are not in a position to provide timelines at this time. Border Services Officers (BSOs) are currently guided by an Operational Bulletin that explains the current legislative framework as well as current CBSA policies regarding the examination of electronic devices.
- The CBSA is committed to maintaining the balance between an individual's right to privacy and the safety and security of Canadians. As such, BSOs are trained to conduct all border examinations with as much respect for privacy as possible.
- All persons, including Canadian citizens, seeking entry to Canada must present themselves to the CBSA and may be subject to a more in-depth exam (secondary inspection).
- Secondary inspections are a part of the normal cross-border travel process and border services officers are trained to perform these examinations in a courteous, respectful and professional manner. As with other goods crossing the border, travellers are legally obligated under the Customs Act to present their electronic devices for inspection by the CBSA.
- Electronic devices and media, including laptops, cell phones and other devices are classified as 'goods' in the context of the border and CBSA officers have the lawful authority under section 99 of the Customs Act to examine them as part of a routine examination.
- Examination of digital devices and media must always be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods. While examination conducted under the authority of section 99 of the Customs Act do not require reasonable grounds to suspect or believe that a contravention has occurred, it is the CBSA's policy that such examinations should only occur where there is a multiplicity of indicators, or further to the discovery of undeclared, prohibited, or falsely reported goods. Initial examinations of digital devices and media should be cursory in nature and increase in intensity based on emerging indicators

- The examination of electronic goods is a tool used to uncover a range of border-related offences, ranging from electronic receipts proving that goods were undervalued or undeclared, to the interception of prohibited goods contained within the devices themselves (child pornography, obscenity, etc.).

Does CBSA keep statistics on the number of border searches of electronic devices it conducts? If so, how many border searches of electronic devices did CBSA conduct each year for the last five years?

The CBSA does not keep this statistic

Does CBSA copy data from the devices that it searches? If so...

- o Where is this data stored?
- o How long is the data retained?
- o Who has access to the data?
- o Is this data shared with other agencies in Canada?
- o Is the data shared with agencies in the US?
- o Of the number of searches conducted last year, how many times was data copied?

The CBSA may only collect data for customs purposes and may only disclose customs information if authorized to do so under section 107 of the Customs Act.

Does the CBSA ask travellers for the passwords to their social media accounts?

- No. CBSA officers shall only examine what is stored within a device and is therefore being imported. Officers are not to read emails or consult social media accounts on the traveller's digital device unless the information is already downloaded and has been opened (usually marked as read) and is therefore stored on the device. As such, CBSA officers shall disable wireless and Internet connectivity (i.e. set to airplane mode) when possible to limit the ability of the device to connect to remote hosts or services.
- That being said, individuals also have the obligation under section 13 of the Customs Act to present and open their goods if requested to do so by a BSO. Because a password can be required to open and examine documents on an electronic device, it can be compelled to allow for the traveller's obligations to be fulfilled. Failure to provide a password can result in the detention or seizure of the electronic device.

- The CBSA is committed to maintaining the balance between an individual's right to privacy and the safety and security of Canadians. As such, BSOs are trained to conduct all border examinations with as much respect for privacy as possible.

s.19(1)

--
[redacted]
Reporter, CBC News

. office: [redacted]
. cell: [redacted]
. twitter: @ [redacted]
. email: [redacted]@cbc.ca | [redacted]@gmail.com
. pgp: [https://keybase.io/\[redacted\]](https://keybase.io/[redacted])
. pgp fingerprint: [redacted]
. secure drop: <https://securedrop.cbc.ca/>

--
[redacted]
Senior Technology Reporter, CBC News

. office: [redacted]
. cell: [redacted]
. twitter: @ [redacted]
. email: [redacted]@cbc.ca | [redacted]@gmail.com
. pgp: [https://keybase.io/\[redacted\]](https://keybase.io/[redacted])
. pgp fingerprint: [redacted]
. secure drop: <https://securedrop.cbc.ca/>

Levert, Jean-Philippe (PS/SP)

From: Giolti, Patrizia <Patrizia.Giolti@cbsa-asfc.gc.ca>
Sent: Tuesday, February 21, 2017 3:05 PM
To: Media Relations / Relations avec les médias (PS/SP); Easton, Erika-Kirsten
Cc: Gowing, Andrew (PS/SP); Levert, Jean-Philippe (PS/SP)
Subject: RE: Query on electronic devices

Thanks – we are on it and will share once ready. thanks

From: Media Relations / Relations avec les médias (PS/SP) [mailto:ps.mediarelations-relationsaveclesmedias.sp@canada.ca]
Sent: February 21, 2017 2:54 PM
To: Giolti, Patrizia; Easton, Erika-Kirsten
Cc: Gowing, Andrew (PS/SP); Levert, Jean-Philippe (PS/SP)
Subject: RE: Query on electronic devices

Good afternoon,

I'm following up on this call.

Thank you,

Karine

From: Media Relations / Relations avec les médias (PS/SP)
Sent: Tuesday, February 21, 2017 9:06 AM
To: Giolti, Patrizia; Easton, Erika-Kirsten
Cc: Gowing, Andrew (PS/SP); Levert, Jean-Philippe (PS/SP)
Subject: FW: Query on electronic devices

Good morning colleagues,

The Minister Office would like to see your response to [REDACTED]'s follow-up questions on the search of electronic devices. You can forward the response to us.

Thank you,

Karine

From: [REDACTED] [mailto:[REDACTED]@cbc.ca]
Sent: Tuesday, February 21, 2017 8:36 AM
To: Bardsley, Scott (PS/SP)
Subject: Fwd: Query on electronic devices

Hi Scott—

Hope you had a good weekend. I sent a few follow-up questions to CBSA this morning, and just wanted to flag them for you as well in case PS has anything to add.

Thanks,
[REDACTED]

----- Forwarded message -----

From: [REDACTED]@cbc.ca>
Date: Tue, Feb 21, 2017 at 8:02 AM
Subject: Re: Query on electronic devices
To: "Giolti, Patrizia" <Patrizia.Giolti@cbsa-asfc.gc.ca>

s.19(1)

Hi Patrizia—

Thanks for sending this response along, and apologies for not replying directly on Friday (I was offsite and wanted to prioritize updating our story with the little time I had).

I do have a few more questions I'm hoping you can answer by end of day today, but let me as soon as you can if this isn't reasonable.

- Can you elaborate on what the PIA will cover?
- As I understand it, the Interim Guidelines from June 2015 published by the BCCLA are also the official guidelines still in use today. However, those interim guidelines contain the following paragraph:

"Until further instructions are issued, CBSA officers shall not arrest a traveller for hindering (Section 153.1 of the Customs Act) or for obstruction (paragraph 129(1)(d) of IRPA) solely for refusing to provide a password. Though such actions appear to be legally supported, a restrained approach will be adopted until the matter is settled in ongoing court proceedings."

Could CBSA clarify whether or not this "restrained approach" is still the current approach?

- Could I have a copies of both the Operational Bulletin, and the aforementioned current CBSA policies regarding the examination of electronic devices that guide the current approach?
- In your previous response, you mentioned that "The CBSA may only collect data for customs purposes and may only disclose customs information if authorized to do so under section 107 of the Customs Act." Does this mean that CBSA can copy, store, and share data collected from an electronic device? And if so, how long is such data retained?
- Finally, what rights exactly does CBSA believe Canadians have at borders? What about foreign travellers?

Thanks,
[REDACTED]

On Fri, Feb 17, 2017 at 8:59 AM, Giolti, Patrizia <Patrizia.Giolti@cbsa-asfc.gc.ca> wrote:

Hello [REDACTED] following your questions on electronic devices and the CBSA, please note below. Should you have other questions please do not hesitate to connect with us.

Best, Patrizia

Questions and answers:

Has CBSA conducted a Privacy Impact Assessment of its own for border searches of electronic devices? If so, could CBSA share a copy of the PIA? If a PIA has not been conducted, why not? If not already answered, under what circumstances does CBSA conduct a search of an electronic device? Are there any formal policies or procedures in place that dictate when, how, and by whom a search is conducted?

- The CBSA has not completed a PIA for the examination of electronic devices at the border; however, it has begun the process internally. We are not in a position to provide timelines at this time. Border Services Officers (BSOs) are currently guided by an Operational Bulletin that explains the current legislative framework as well as current CBSA policies regarding the examination of electronic devices.
- The CBSA is committed to maintaining the balance between an individual's right to privacy and the safety and security of Canadians. As such, BSOs are trained to conduct all border examinations with as much respect for privacy as possible.
- All persons, including Canadian citizens, seeking entry to Canada must present themselves to the CBSA and may be subject to a more in-depth exam (secondary inspection).
- Secondary inspections are a part of the normal cross-border travel process and border services officers are trained to perform these examinations in a courteous, respectful and professional manner. As with other goods crossing the border, travellers are legally obligated under the Customs Act to present their electronic devices for inspection by the CBSA.
- Electronic devices and media, including laptops, cell phones and other devices are classified as 'goods' in the context of the border and CBSA officers have the lawful authority under section 99 of the Customs Act to examine them as part of a routine examination.
- Examination of digital devices and media must always be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods. While examination conducted under the authority of section 99 of the Customs Act do not require reasonable grounds to suspect or believe that a contravention has occurred, it is the CBSA's policy that such examinations should only occur where there is a multiplicity of indicators, or further to the discovery of undeclared, prohibited, or falsely reported goods. Initial examinations of digital devices and media should be cursory in nature and increase in intensity based on emerging indicators
- The examination of electronic goods is a tool used to uncover a range of border-related offences, ranging from electronic receipts proving that goods were undervalued or undeclared, to the interception of prohibited goods contained within the devices themselves (child pornography, obscenity, etc.).

Does CBSA keep statistics on the number of border searches of electronic devices it conducts? If so, how many border searches of electronic devices did CBSA conduct each year for the last five years?

The CBSA does not keep this statistic

Does CBSA copy data from the devices that it searches? If so...

- o Where is this data stored?
- o How long is the data retained?
- o Who has access to the data?
- o Is this data shared with other agencies in Canada?
- o Is the data shared with agencies in the US?
- o Of the number of searches conducted last year, how many times was data copied?

The CBSA may only collect data for customs purposes and may only disclose customs information if authorized to do so under section 107 of the Customs Act.

Does the CBSA ask travellers for the passwords to their social media accounts?

- No. CBSA officers shall only examine what is stored within a device and is therefore being imported. Officers are not to read emails or consult social media accounts on the traveller's digital device unless the information is already downloaded and has been opened (usually marked as read) and is therefore stored on the device. As such, CBSA officers shall disable wireless and Internet connectivity (i.e. set to airplane mode) when possible to limit the ability of the device to connect to remote hosts or services.
- That being said, individuals also have the obligation under section 13 of the Customs Act to present and open their goods if requested to do so by a BSO. Because a password can be required to open and examine documents on an electronic device, it can be compelled to allow for the traveller's obligations to be fulfilled. Failure to provide a password can result in the detention or seizure of the electronic device.
- The CBSA is committed to maintaining the balance between an individual's right to privacy and the safety and security of Canadians. As such, BSOs are trained to conduct all border examinations with as much respect for privacy as possible.

--

[REDACTED] Reporter, CBC News

. office: [REDACTED]
. cell: [REDACTED]
. twitter: @ [REDACTED]
. email: [REDACTED]@cbc.ca | [REDACTED]@gmail.com
. pgp: <https://keybase.io> [REDACTED]
. pgp fingerprint: [REDACTED]
. secure drop: <https://securedrop.cbc.ca/>

s.19(1)

--

[REDACTED] Reporter, CBC News

. office: [REDACTED]
. cell: [REDACTED]
. twitter: @ [REDACTED]
. email: [REDACTED]@cbc.ca | [REDACTED]@gmail.com
. pgp: <https://keybase.io> [REDACTED]
. pgp fingerprint: [REDACTED]
. secure drop: <https://securedrop.cbc.ca/>

Levert, Jean-Philippe (PS/SP)

From: Media Relations / Relations avec les médias (PS/SP)
Sent: Tuesday, February 21, 2017 8:56 AM
To: Bardsley, Scott (PS/SP); Media Relations / Relations avec les médias (PS/SP)
Cc: Brien, Dan (PS/SP); Peirce, Hilary (PS/SP); Holland, Alyx (PS/SP); Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP)
Subject: RE: Query on electronic devices

Hi Scott,

s.19(1)

I will follow-up with CBSA.

Karine

From: Bardsley, Scott (PS/SP)
Sent: Tuesday, February 21, 2017 8:43 AM
To: Media Relations / Relations avec les médias (PS/SP)
Cc: Brien, Dan (PS/SP); Peirce, Hilary (PS/SP); Holland, Alyx (PS/SP); Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP)
Subject: FW: Query on electronic devices

Dear PS Media Relations,

Can you please flag to CBSA that MO would like to see a copy their response to [REDACTED] (below) for awareness? Thanks,

Scott

From: [REDACTED] [mailto:[REDACTED]@cbc.ca]
Sent: Tuesday, February 21, 2017 8:36 AM
To: Bardsley, Scott (PS/SP)
Subject: Fwd: Query on electronic devices

Hi Scott—

Hope you had a good weekend. I sent a few follow-up questions to CBSA this morning, and just wanted to flag them for you as well in case PS has anything to add.

Thanks,
[REDACTED]

----- Forwarded message -----

From: [REDACTED]@cbc.ca>
Date: Tue, Feb 21, 2017 at 8:02 AM
Subject: Re: Query on electronic devices
To: "Giolti, Patrizia" <Patrizia.Giolti@cbsa-asfc.gc.ca>

Hi Patrizia—

Thanks for sending this response along, and apologies for not replying directly on Friday (I was offsite and wanted to prioritize updating our story with the little time I had).

I do have a few more questions I'm hoping you can answer by end of day today, but let me as soon as you can if this isn't reasonable.

- Can you elaborate on what the PIA will cover?
- As I understand it, the Interim Guidelines from June 2015 published by the BCCLA are also the official guidelines still in use today. However, those interim guidelines contain the following paragraph:

"Until further instructions are issued, CBSA officers shall not arrest a traveller for hindering (Section 153.1 of the Customs Act) or for obstruction (paragraph 129(1)(d) of IRPA) solely for refusing to provide a password. Though such actions appear to be legally supported, a restrained approach will be adopted until the matter is settled in ongoing court proceedings."

Could CBSA clarify whether or not this "restrained approach" is still the current approach?

- Could I have a copies of both the Operational Bulletin, and the aforementioned current CBSA policies regarding the examination of electronic devices that guide the current approach?
- In your previous response, you mentioned that "The CBSA may only collect data for customs purposes and may only disclose customs information if authorized to do so under section 107 of the Customs Act." Does this mean that CBSA can copy, store, and share data collected from an electronic device? And if so, how long is such data retained?
- Finally, what rights exactly does CBSA believe Canadians have at borders? What about foreign travellers?

Thanks,

s.19(1)

On Fri, Feb 17, 2017 at 8:59 AM, Giolti, Patrizia <Patrizia.Giolti@cbsa-asfc.gc.ca> wrote:

Hello following your questions on electronic devices and the CBSA, please note below. Should you have other questions please do not hesitate to connect with us.

Best, Patrizia

Questions and answers:

Has CBSA conducted a Privacy Impact Assessment of its own for border searches of electronic devices? If so, could CBSA share a copy of the PIA? If a PIA has not been conducted, why not? If not already answered, under what circumstances does CBSA conduct a search of an electronic device? Are there any formal policies or procedures in place that dictate when, how, and by whom a search is conducted?

- The CBSA has not completed a PIA for the examination of electronic devices at the border; however, it has begun the process internally. We are not in a position to provide timelines at this

time. Border Services Officers (BSOs) are currently guided by an Operational Bulletin that explains the current legislative framework as well as current CBSA policies regarding the examination of electronic devices.

- The CBSA is committed to maintaining the balance between an individual's right to privacy and the safety and security of Canadians. As such, BSOs are trained to conduct all border examinations with as much respect for privacy as possible.
- All persons, including Canadian citizens, seeking entry to Canada must present themselves to the CBSA and may be subject to a more in-depth exam (secondary inspection).
- Secondary inspections are a part of the normal cross-border travel process and border services officers are trained to perform these examinations in a courteous, respectful and professional manner. As with other goods crossing the border, travellers are legally obligated under the Customs Act to present their electronic devices for inspection by the CBSA.
- Electronic devices and media, including laptops, cell phones and other devices are classified as 'goods' in the context of the border and CBSA officers have the lawful authority under section 99 of the Customs Act to examine them as part of a routine examination.
- Examination of digital devices and media must always be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods. While examination conducted under the authority of section 99 of the Customs Act do not require reasonable grounds to suspect or believe that a contravention has occurred, it is the CBSA's policy that such examinations should only occur where there is a multiplicity of indicators, or further to the discovery of undeclared, prohibited, or falsely reported goods. Initial examinations of digital devices and media should be cursory in nature and increase in intensity based on emerging indicators
- The examination of electronic goods is a tool used to uncover a range of border-related offences, ranging from electronic receipts proving that goods were undervalued or undeclared, to the interception of prohibited goods contained within the devices themselves (child pornography, obscenity, etc.).

Does CBSA keep statistics on the number of border searches of electronic devices it conducts? If so, how many border searches of electronic devices did CBSA conduct each year for the last five years?

The CBSA does not keep this statistic

Does CBSA copy data from the devices that it searches? If so...

- o Where is this data stored?
- o How long is the data retained?
- o Who has access to the data?

- o Is this data shared with other agencies in Canada?
- o Is the data shared with agencies in the US?
- o Of the number of searches conducted last year, how many times was data copied?

The CBSA may only collect data for customs purposes and may only disclose customs information if authorized to do so under section 107 of the Customs Act.

Does the CBSA ask travellers for the passwords to their social media accounts?

- No. CBSA officers shall only examine what is stored within a device and is therefore being imported. Officers are not to read emails or consult social media accounts on the traveller's digital device unless the information is already downloaded and has been opened (usually marked as read) and is therefore stored on the device. As such, CBSA officers shall disable wireless and Internet connectivity (i.e. set to airplane mode) when possible to limit the ability of the device to connect to remote hosts or services.
- That being said, individuals also have the obligation under section 13 of the Customs Act to present and open their goods if requested to do so by a BSO. Because a password can be required to open and examine documents on an electronic device, it can be compelled to allow for the traveller's obligations to be fulfilled. Failure to provide a password can result in the detention or seizure of the electronic device.
- The CBSA is committed to maintaining the balance between an individual's right to privacy and the safety and security of Canadians. As such, BSOs are trained to conduct all border examinations with as much respect for privacy as possible.

s.19(1)

--

[Redacted]
Reporter, CBC News

. office: [Redacted]
. cell: [Redacted]
. twitter: @ [Redacted]
. email: [Redacted]@cbc.ca | [Redacted]@gmail.com
. pgp: [https://keybase.io/\[Redacted\]](https://keybase.io/[Redacted])
. pgp fingerprint: [Redacted]
. secure drop: <https://securedrop.cbc.ca/>

s.19(1)

--



Reporter, CBC News

- . office: [redacted]
- . cell: [redacted]
- . twitter: @ [redacted]
- . email: [redacted]@cbc.ca | [redacted]@gmail.com
- . pgp: [https://keybase.io/\[redacted\]](https://keybase.io/[redacted])
- . pgp fingerprint: [redacted]
- . secure drop: <https://securedrop.cbc.ca/>

Levert, Jean-Philippe (PS/SP)

From: Dorion, Nicholas <Nicholas.Dorion@cbsa-asfc.gc.ca>
Sent: Friday, February 24, 2017 3:31 PM
To: O'Nions, Christine (Christine.O'Nions@pco-bcp.gc.ca)
Cc: Media Relations / Relations avec les médias (PS/SP); Communications Issues Management / Communications Gestion des Enjeux (PS/SP); CBSA-ASFC-Media Relations
Subject: For PCO Awareness - CBSA Approved Response - GN

Hi Christine,

For PCO awareness. A CBSA approved response to Global News on search of electronic devices.

Merci! Nicholas

Media: [REDACTED] | National Online Journalist | Global News |
Issue: Electronic device search

Email:

I am seeking comment and information regarding CBSA's policy on border officer protocol and powers when it comes to travellers' cellphones and other personal devices.

Questions:

Q1: Please fully explain what is included in the right to "Inspect your ... electronics (including laptops and cell phones)? What are passengers' rights?"

A1:

All persons, including Canadian citizens, seeking entry to Canada must present themselves to the CBSA and may be subject to a more in-depth exam (secondary inspection).

Secondary inspections are a part of the normal cross-border travel process and border services officers are trained to perform these examinations in a courteous, respectful and professional manner. As with other goods crossing the border, travellers are legally obligated under the Customs Act to present their electronic devices for inspection by the CBSA.

Electronic devices and media, including laptops, cell phones and other devices are classified as 'goods' in the context of the border and CBSA officers have the lawful authority under section 99 of the Customs Act to examine them as part of a routine examination.

Examination of digital devices and media must always be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods. While examination conducted under the authority of section 99 of the Customs Act do not require reasonable grounds to 000178

suspect or believe that a contravention has occurred, it is the CBSA's policy that such examinations should only occur where there is a multiplicity of indicators, or further to the discovery of undeclared, prohibited, or falsely reported goods. Initial examinations of digital devices and media should be cursory in nature and increase in intensity based on emerging indicators

The examination of electronic goods is a tool used to uncover a range of border-related offences, ranging from electronic receipts proving that goods were undervalued or undeclared, to the interception of prohibited goods contained within the devices themselves (child pornography, obscenity, etc.).

Q2: Are CBSA officers permitted to ask for or demand passcodes to such devices?

When they do have access to a traveller's device, do they have the ability or permission to download or document any sort of data or information from the device?

A2: CBSA officers may only request and make note of passwords required to gain access to information or files if the information or file is known or suspected to exist within the digital device or media being examined.

Passwords are not to be sought to gain access to any type of account (including any social, professional, corporate, or user accounts), files or information that might potentially be stored remotely or on-line.

Q3: What if the password is not divulged?

A3:

The CBSA is committed to maintaining the balance between an individual's right to privacy and the safety and security of Canadians. As such, BSOs are trained to conduct all border examinations with as much respect for privacy as possible.

If a traveller refuses to provide a password to allow examination of the digital device, media or the documents contained therein, or if there are technical difficulties that prevent a CBSA officer from examining the digital device or media, the device or media may be detained by the CBSA officer under the authority of Section 101 of the *Customs Act* or under the authority of subsection 140 (1) of the *Immigration and Refugee Protection Act* (IRPA).

CBSA officers shall not arrest a traveller for hindering or for obstruction solely for refusing to provide a password. Though such actions appear to be legally supported, a restrained approach will be adopted until the matter is settled in ongoing court proceedings.

Q4: Are there plans to examine CBSA's policy on this?

A4: No further instructions have been issued and this approach is still being applied. As such, policy guidelines are still in force with respect to examinations of electronic goods as well as for arrest guidelines.

s.19(1)

Levert, Jean-Philippe (PS/SP)

From: O'Nions, Christine <Christine.O'Nions@pco-bcp.gc.ca>
Sent: Tuesday, March 07, 2017 5:07 PM
To: Bailey, Esme
Cc: Archipow, Nancy; CBSA-ASFC-Media Relations; Media Relations / Relations avec les médias (PS/SP); Communications Issues Management / Communications Gestion des Enjeux (PS/SP)
Subject: Re: For PCO awareness: Media calls electronic searches

Give me a minute

613 853-1042.

From: Bailey, Esme
Sent: Tuesday, March 7, 2017 4:59 PM
To: O'Nions, Christine
Cc: Archipow, Nancy; CBSA-ASFC-Media Relations; Media Relations / Relations avec les médias (PS/SP); 'ps.communicationsissuesmanagement-communicationsgestiondesenjeux.sp@canada.ca'
Subject: For PCO awareness: Media calls electronic searches

Hello,

For awareness. We will be providing the following responses regarding electronic searches.

Thanks,

Esme

Media: [REDACTED] / Ming Pao

Contact [REDACTED]@mingpaotor.com<mailto:[REDACTED]@mingpaotor.com> /

Issue: Electronic devices

Questions:

Q1: We would like to hear more specific cases. We won't disclose any personal information, like the name of that person. We would like to know in details what drive officers to check phone or laptop, the searching process and findings, and the end result of it (ie what

charges were laid? Have any travelers faced direct deportations?)

Q2. Under what circumstances, border agents will search travelers' phones and laptops?

Q3. What content inside the phones and laptops will cause denial of entry to Canada? Can you please provide some examples?

A1-3. All persons, including Canadian citizens, seeking entry to Canada must present themselves to the CBSA and may be subject to a more in-depth exam (secondary inspection).

Secondary inspections are a part of the normal cross-border travel process and border services officers are trained to perform these examinations in a courteous, respectful and professional manner. As with other goods crossing the border, travellers are legally obligated under the Customs Act to present their electronic devices for inspection by the CBSA.

Electronic devices and media, including laptops, cell phones and other devices are classified as 'goods' in the context of the border and CBSA officers have the lawful authority under section 99 of the Customs Act to examine them as part of a routine examination.

Examination of digital devices and media must always be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods. While examination conducted under the authority of section 99 of the Customs Act do not require reasonable grounds to suspect or believe that a contravention has occurred, it is the CBSA's policy that such examinations should only occur where there is a multiplicity of indicators, or further to the discovery of undeclared, prohibited, or falsely reported goods. Initial examinations of digital devices and media should be cursory in nature and increase in intensity based on emerging indicators

The examination of electronic goods is a tool used to uncover a range of border-related offences, ranging from electronic receipts proving that goods were undervalued or undeclared, to the interception of prohibited goods contained within the devices themselves (child pornography, obscenity, etc.).

Admissibility

- All persons must demonstrate they meet the requirements to enter and/or stay in Canada.
- Admissibility of all travellers is decided on a case-by-case basis and based on the information made available to the border services officer at the time of entry.

- Several factors are used in determining admissibility into Canada, including involvement in criminal activity, in human rights violations, in organized crime, security, health or financial reasons.

Q4. Do agents just look at content stored inside the phone? or they will look into online social websites, such as Facebook and Twitter?

A4. CBSA officers may only request and make note of passwords required to gain access to information or files if the information or file is known or suspected to exist within the digital device or media being examined.

Passwords are not to be sought to gain access to any type of account (including any social, professional, corporate, or user accounts), files or information that might potentially be stored remotely or on-line.

Q5. What happen if people do not comply?

A5. The CBSA is committed to maintaining the balance between an individual's right to privacy and the safety and security of Canadians. As such, BSOs are trained to conduct all border examinations with as much respect for privacy as possible.

If a traveller refuses to provide a password to allow examination of the digital device, media or the documents contained therein, or if there are technical difficulties that prevent a CBSA officer from examining the digital device or media, the device or media may be detained by the CBSA officer under the authority of Section 101 of the Customs Act or under the authority of subsection 140 (1) of the Immigration and Refugee Protection Act (IRPA).

CBSA officers shall not arrest a traveller for hindering or for obstruction solely for refusing to provide a password. Though such actions appear to be legally supported, a restrained approach will be adopted until the matter is settled in ongoing court proceedings.

Q6. What if the content are not written in English, ie Chinese? Will it take longer time to check?

A6. Depending on the nature of the content reviewed and the availability of on-site translation services, additional delays may occur.

Officers progressively intensify their examinations of goods (including electronic goods) based on emerging indicators until they are satisfied that all requirements under CBSA-mandated program legislation have been met. A request for translation will not occur unless the officer has identified indicators of non-compliance and chooses to intensify the examination in order to negate those concerns.

s.19(1)

Media: [REDACTED] / Barrister & Solicitor / [REDACTED]
Phone: [REDACTED] / Direct Line: [REDACTED] / Email:
[REDACTED] <mailto:[REDACTED]>

Questions:

Q1: Please fully explain what is included in the right to "Inspect your ... electronics (including laptops and cell phones)? What are passengers' rights?

A1:

All persons, including Canadian citizens, seeking entry to Canada must present themselves to the CBSA and may be subject to a more in-depth exam (secondary inspection).

Secondary inspections are a part of the normal cross-border travel process and border services officers are trained to perform these examinations in a courteous, respectful and professional manner. As with other goods crossing the border, travellers are legally obligated under the Customs Act to present their electronic devices for inspection by the CBSA.

Electronic devices and media, including laptops, cell phones and other devices are classified as 'goods' in the context of the border and CBSA officers have the lawful authority under section 99 of the Customs Act to examine them as part of a routine examination.

Examination of digital devices and media must always be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods. While examination conducted under the authority of section 99 of the Customs Act do not require reasonable grounds to suspect or believe that a contravention has occurred, it is the CBSA's policy that such examinations should only occur where there is a multiplicity of indicators, or further to the discovery of undeclared, prohibited, or falsely reported goods. Initial examinations of digital devices and media should be cursory in nature and increase in intensity based on emerging indicators.

The examination of electronic goods is a tool used to uncover a range of border-related offences, ranging from electronic receipts proving that goods were undervalued or undeclared, to the interception of prohibited goods contained within the devices themselves (child pornography, obscenity, etc.).

Q2: Are CBSA officers permitted to ask for or demand passcodes to such devices?

When they do have access to a traveller's device, do they have the ability or permission to download or document any sort of data or information from the device?

A2: CBSA officers may only request and make note of passwords required to gain access to information or files if the information or file is known or suspected to exist within the digital device or media being examined.

Passwords are not to be sought to gain access to any type of account (including any social, professional, corporate, or user accounts), files or

information that might potentially be stored remotely or on-line.

Q3: What if the password is not divulged?

A3:

The CBSA is committed to maintaining the balance between an individual's right to privacy and the safety and security of Canadians. As such, BSOs are trained to conduct all border examinations with as much respect for privacy as possible.

If a traveller refuses to provide a password to allow examination of the digital device, media or the documents contained therein, or if there are technical

difficulties that prevent a CBSA officer from examining the digital device or media, the device or media may be detained by the CBSA officer under the

authority of Section 101 of the Customs Act or under the authority of subsection 140 (1) of the Immigration and Refugee Protection Act (IRPA).

CBSA officers shall not arrest a traveller for hindering or for obstruction solely for refusing to provide a password. Though such

actions appear to be legally supported, a restrained approach will be adopted until the matter is settled in ongoing court proceedings.

Q4: Are there plans to examine CBSA's policy on this?

A4: No further instructions have been issued and this approach is still being applied. As such, policy guidelines are still in force with respect to examinations of electronic goods as well as for arrest guidelines.

Esme Bailey

Senior Communications Advisor, Corporate Affairs Branch

Canada Border Services Agency / Government of Canada

esme.bailey@cbsa-asfc.gc.ca<mailto:esme.bailey@cbsa-asfc.gc.ca> / Tel: 613-948-4013 / TTY : 866-335-3237

Conseillère principale en communications, Direction générale des services intégrés Agence des services frontaliers du Canada / Gouvernement du Canada esme.bailey@asfc-cbsa.gc.ca<mailto:esme.bailey@asfc-cbsa.gc.ca> / Tél. : 613-948-4013 / ATS : 866-335-3237

Levert, Jean-Philippe (PS/SP)

From: Guibert-Wolff, Line <Line.Guibert-Wolff@cbsa-asfc.gc.ca>
Sent: Friday, March 17, 2017 3:28 PM
To: Brunette, Lynn: PCO / BCP; Lindblad, Anabel: PCO / BCP
Cc: CBSA-ASFC-Media Relations; Media Relations / Relations avec les médias (PS/SP); Communications Issues Management / Communications Gestion des Enjeux (PS/SP); Easton, Erika-Kirsten; Raider, Marc; Archipow, Nancy
Subject: For PCO Awareness/ Media query - Cell phone searches / Global News

Good afternoon,

For PCO awareness, a CBSA approved response to the Global news query on cell phone searches.

Thank you.

s.19(1)

Media: [REDACTED] / Global News

Contact: [REDACTED] E-mail: [REDACTED]@globalnews.ca

Deadline: 2017-03-16 – 17:00 ET.

Issue: Cell phone Searches

Questions: Information on policies on examining electronic devices.

Response: We can tell you that all persons, including Canadian citizens, seeking entry to Canada must present themselves and their goods to the CBSA and may be subject to a more in-depth exam (secondary inspection).

Secondary inspections are a part of the normal cross-border travel process and border services officers are trained to perform these examinations in a courteous, respectful and professional manner. As with other goods crossing the border, travellers are legally obligated under the Customs Act to present their electronic devices for inspection by the CBSA.

Electronic devices and media, including laptops, cell phones and other devices are classified as 'goods' in the context of the border and CBSA officers have the lawful authority under section 99 of the Customs Act to examine them as part of a routine examination.

Examination of digital devices and media must always be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods. While examination conducted under the authority of section 99 of the Customs Act do not require reasonable grounds to suspect or believe that a contravention has occurred, it is the CBSA's policy that such examinations should only occur where there is a multiplicity of indicators, or further to the discovery of

undeclared, prohibited, or falsely reported goods. Initial examinations of digital devices and media should be cursory in nature and increase in intensity based on emerging indicators.

The examination of electronic goods is a tool used to uncover a range of border-related offences, ranging from electronic receipts proving that goods were undervalued or undeclared, to the interception of prohibited goods contained within the devices themselves (child pornography, obscenity, etc.).

On Passwords

CBSA officers may only request and make note of passwords required to gain access to information or files if the information or file is known or suspected to exist within the digital device or media being examined. Passwords are not to be sought to gain access to any type of account (including any social, professional, corporate, or user accounts), files or information that might potentially be stored remotely or on-line.

Balancing Privacy and the safety and security of Canadians

The CBSA is committed to maintaining the balance between an individual's right to privacy and the safety and security of Canadians. As such, BSOs are trained to conduct all border examinations with as much respect for privacy as possible.

If a traveller refuses to provide a password to allow examination of the digital device, media or the documents contained therein, or if there are technical difficulties that prevent a CBSA officer from examining the digital device or media, the device or media may be **detained** by the CBSA officer under the authority of Section 101 the *Customs Act* or under the authority of subsection 140 (1) of the *Immigration and Refugee Protection Act (IRPA)*.

CBSA officers shall not arrest a traveller for hindering or for obstruction solely for refusing to provide a password. Though such actions appear to be legally supported, a restrained approach will be adopted until the matter is settled in ongoing court proceedings.

Line A. Guibert-Wolff

Media Spokesperson | Porte-parole

Corporate Affairs Branch | Direction générales des services intégrés

Canada Border Services Agency | Agence des services frontaliers du Canada

Government of Canada | Gouvernement du Canada

line.guibert-Wolff@cbsa-asfc.gc.ca

Tel | Tél. : 613-952-0522 / Facsimile | Télécopieur 613-952-1797

Teletypewriter | Téléimprimeur 1-866-335-3237



SENATE DELAYED ANSWER – RÉPONSE DIFÉRÉE DU SÉNAT

To / À Public Safety

Date March 29, 2017

Question No. / Question N°

DA-0226

Senator / Sénateur (trice)

Senator Jaffer

Date of Question / Date de la question

March 28, 2017

Deadline / Date d'échéance

April 12, 2017

Your Minister has been identified as the lead respondent for answering the question below.

Votre ministre a été choisi pour être le principal répondant à la question ci-dessous.

If you have no information on this subject or you consider that another Minister should take the lead, please advise us within 24 hours.

Si vous n'avez pas d'information sur ce sujet ou croyez qu'un autre ministre devrait être choisi comme responsable, veuillez nous aviser dans les prochaines 24 heures.

The answer should be prepared in both official languages on the attached form. The answer should be no more than 200 words (no tables, charts, etc).

La réponse devrait figurer dans les deux langues officielles sur le formulaire joint en annexe. Elle ne devrait pas compter plus de 200 mots (pas de tableaux, de graphiques, etc.).

Please ensure that the Minister's signature is included with the response.

Veuillez vous assurer que la réponse comporte la signature du ministre.

EXCERPT FROM SENATE DEBATES / EXTRAIT DES DÉBATS DU SÉNAT:

Hon. Mobina S. B. Jaffer: Honourable senators, my question is to the leader in the Senate.

Leader, one of the things during the last election that many of us were very appreciative of was the focus that with the security agenda would come human rights. Perhaps wrongly, but I was under the impression that Bill C-51 would definitely be on the government's agenda. We're almost hitting two years, and we do not see much happening on the security agenda.

On March 20, Minister Goodale released a commentary on Bill C-22, which will establish a national security and intelligence committee for parliamentarians. This is just an oversight committee; it does not look at issues of Bill C-51 directly.

But in this commentary, the minister said he outlined several changes to the bill made because of the feedback during consultations; that is, Bill C-22. I am glad to say that the minister is willing to accept feedback on this bill. The committee of parliamentarians must have the tools needed to balance the need for security with respect for human rights. It is all well and good that we should have an oversight committee.

Leader, I get phone calls on a regular basis from people who are still arrested, interrupted and harassed under Bill C-51, two years later. When is the government going to look after this issue?

Hon. Peter Harder (Government Representative in the Senate): Again, I thank the honourable senator for her question. She raises an important matter that has been the subject of public debate and indeed, as she referenced, in the last election as well.

With respect to the precise timing of the government's legislative intentions, I will inquire and report back to the Senate.

Senator Jaffer: Thank you. I appreciate that, leader. I do appreciate that you understand the challenges the communities face.

But another bill is not being given enough attention, and that's Bill C-13, regarding lawful access, which the Privacy Commissioner of Canada has suggested also needs to be reviewed.

When you are inquiring, may I please ask that you find out what the status is? When is the government going to bring forward legislation to balance human rights and security under Bill C-51? And when will it look at reviewing Bill C-13?

Senator Harder: I will do so.

Senator Jaffer: Thank you.

L'honorable Mobina S. B. Jaffer : Honorables sénateurs, ma question s'adresse au leader du gouvernement au Sénat.

Monsieur le leader, pendant la campagne électorale, bien des gens avaient apprécié le fait que les droits de la personne iraient de pair avec le programme en matière de sécurité. Peut-être à tort, j'avais l'impression que le projet de loi C-51 ne manquerait pas de figurer sur la liste des tâches du gouvernement. Après presque deux ans, il ne semble pas se passer grand-chose sur le plan de la sécurité.

Le 20 mars, le ministre Goodale a émis un commentaire au sujet du projet de loi C-22, qui vise la création d'un comité de parlementaires sur la sécurité nationale et le renseignement. Il ne s'agit que d'un comité de surveillance, qui n'examinera pas directement les problèmes liés au projet de loi C-51.

Toutefois, dans son commentaire, le ministre a indiqué que quelques changements avaient été apportés au projet de loi C-22 à la suite des commentaires obtenus lors des consultations. Je suis heureuse de constater que le ministre est disposé à accepter les commentaires concernant ce projet de loi. Le comité de parlementaires doit disposer des outils nécessaires pour bien établir un équilibre entre le besoin de sécurité et le respect des droits de la personne. Je crois que ce comité de surveillance sera le bienvenu.

Monsieur le leader, je reçois régulièrement des appels téléphoniques de la part de personnes qui, deux ans plus tard, se font encore arrêter, interrompre ou harceler à cause du projet de loi C-51. Quand le gouvernement s'occupera-t-il de ce problème?

L'honorable Peter Harder (représentant du gouvernement au Sénat) : Je remercie encore une fois la sénatrice de sa question, qui porte sur un sujet important ayant fait l'objet d'un débat public, y compris pendant la dernière campagne électorale, comme elle l'a dit.

En ce qui concerne le moment exact où le gouvernement compte légiférer, je vais m'informer et transmettre ultérieurement la réponse au Sénat.

La sénatrice Jaffer : Merci. Je l'apprécie, monsieur le leader. Je suis contente que vous compreniez les problèmes que vivent les gens.

Cependant, il y a un autre projet de loi qui ne reçoit pas assez d'attention, et c'est le projet de loi C-13, concernant l'accès légal. Selon le commissaire à la protection de la vie privée du Canada, ces dispositions juridiques devraient, elles aussi, être examinées.

Lorsque vous vous informerez, pourriez-vous chercher à savoir quel est l'état de ce dossier également? Quand le gouvernement a-t-il l'intention de déposer un projet de loi destiné à trouver le juste équilibre entre les droits de la personne et la sécurité dans le projet de loi C-51? Quand le gouvernement a-t-il l'intention d'examiner le projet de loi C-13?

Le sénateur Harder : Je poserai la question.

La sénatrice Jaffer : Merci.



Public Safety Sécurité publique
Canada Canada

Deputy Minister Sous-ministre

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: APR 13 2017

File No.: 1304-421 / PS-015823

MEMORANDUM FOR THE MINISTER

RESPONSE TO ORAL SENATE QUESTION DA-0226

(Signature required)

ISSUE

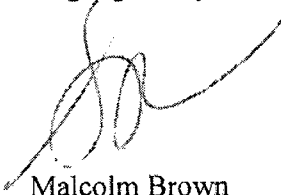
During the March 28, 2017, Question Period in the Senate, Senator Mobina Jaffer enquired about consultations on Bill C-51, *Anti-Terrorism Act, 2015* and former Bill C-13, *Protecting Canadians from Online Crime Act (TAB A)*.

The enclosed response was prepared by the Department (**TAB B**).

The Privy Council Office had requested a response by April 12, 2017.

RECOMMENDATION

It is recommended that you sign the attached response, provided in both official languages, at your earliest convenience.



Malcolm Brown

Enclosures: (2)

Prepared by: Dana Robinson

Canada



Government of Canada
Privy Council Office

Gouvernement du Canada
Bureau du Conseil privé

SENATE DELAYED ANSWER RÉPONSE DIFÉRÉE DU SÉNAT

| | | |
|---------------------------------|--|------------------------|
| NO. / N ^o DA-0226 | BY / DE Senator / Sénateur(trice) Mobina S. B. Jaffer | DATE March 28, 2017 |
|---------------------------------|--|------------------------|

Reply by the Minister of Public Safety and Emergency Preparedness
Réponse du ministre de la Sécurité publique et de la Protection civile

Hon. Ralph Goodale

PRINT NAME OF MINISTER / INSCRIRE LE NOM DU MINISTRE

SIGNATURE

SUBJECT / SUJET

Legislative Review—Human Rights/L'examen législatif—Les droits de la personne

REPLY / RÉPONSE

English:

The Government remains committed to repealing the problematic elements of Bill C-51, the *Anti-Terrorism Act, 2015* as part of achieving the Government's dual objective of keeping Canadians safe while safeguarding rights and freedoms.

Already, the Government has introduced Bill C-22 to establish a committee of parliamentarians that will scrutinize the work of Canada's national security and intelligence agencies; created the Passenger Protect Inquiries Office as part of continuing efforts to improve the redress system for the no-fly list; and committed \$35 million over five years, with \$10 million per year ongoing, to establish an Office of Community Outreach and Counter-Radicalization.

The Government will also be making a number of additional improvements, including better defining rules regarding terrorist propaganda, ensuring that the right to advocate and protest is properly protected, and mandating statutory review of national security legislation.

Moreover, the Government has engaged in unprecedented consultations with key stakeholders, academics, experts and Canadians about national security issues. Consultation topics went beyond the *Anti-Terrorism Act, 2015*, and included lawful access as well as stakeholder engagement on concerns surrounding the former Bill C-13. As part of the Government's commitment to openness and transparency, the submissions received are available online at open.canada.ca. The Government is currently analyzing the submissions and advancing policy development in response.

The Government will be releasing a report on the results of the consultations and intends to propose legislative changes in the coming months.

Français :

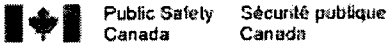
Le gouvernement demeure résolu à abroger les éléments problématiques du projet de loi C-51, la *Loi antiterroriste de 2015*, dans le but d'atteindre le double objectif du gouvernement de garder les Canadiens en sécurité tout en protégeant leurs droits et leurs libertés.

Déjà, le gouvernement a introduit le projet de loi C-22 afin de créer un comité de parlementaires qui examinera le travail des organismes de sécurité nationale et de renseignement du Canada; a créé le Bureau des demandes de renseignements du Programme de protection des passagers dans le cadre des efforts continus visant à améliorer le programme de rectification pour la liste d'interdiction de vol ; et a engagé 35 millions de dollars sur cinq ans, avec 10 millions de dollars par année sur une base permanente, pour la création d'un bureau de la sensibilisation des collectivités et de la lutte contre la radicalisation menant à la violence.

Le gouvernement fera également des améliorations supplémentaires, y compris une meilleure définition des règles concernant la propagande terroriste, en veillant à ce que le droit de défendre une cause et manifester soit adéquatement protégé et il exigera un examen obligatoire de la législation de sécurité nationale.

De plus, le gouvernement a engagé des consultations sans précédent auprès des intervenants clés, des universitaires, des experts et des Canadiens sur les questions de sécurité nationale. Les thèmes des consultations sont allés au-delà de la *Loi antiterroriste de 2015* afin d'inclure des sujets tels que l'accès légal ainsi que sur la mobilisation des intervenants à l'égard des préoccupations liées au projet de loi C-13. Dans le cadre de l'engagement du gouvernement envers l'ouverture et la transparence, les soumissions reçues sont disponibles en ligne à ouvert.canada.ca. Le gouvernement analyse actuellement les soumissions et fait progresser l'élaboration des politiques en conséquence.

Le gouvernement publiera un rapport sur les résultats des consultations et projette de proposer des modifications législatives dans les prochains mois.



PACB
Branch / Direction générale

**REÇU AU BUREAU
DU SM**
AVR 12 2017
**RECEIVED IN
DM'S OFFICE**

Routing Slip / Bordereau d'acheminement

CCM File No / No de dossier CCM : PS-015823

DRAGON / RDIMS / SGDDI : _____

ADM's Quality Control / Contrôle de qualité du cabinet du SMA : _____

| Title / Titre : Senate Delayed DA-0226 – Senator Jaffer – Bill C-51/Bill C-22 – March 28, 2017 | | <u>ACTION REQUIRED / MESURES À PRENDRE</u> | | |
|--|----------------|--|--|--------------------------|
| Name / Nom | Date | Initials / Initiales | Approval or signature / Approbation ou signature (via) | Information (cc) |
| Originator / Auteur Dana Robinson Julie McAteer | April 11/17 | DR | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Director / Directeur Élise Renaud | April 11, 2017 | [Signature] | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Director General / Directeur général Jean Cintrat | APR 11 2017 | [Signature] | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Chief Audit Executive / Dirigeant principale de la vérification Denis Gorman | | | <input type="checkbox"/> | <input type="checkbox"/> |
| Director General Communications / Directeur général des communications Jamie Tomlinson | | | <input type="checkbox"/> | <input type="checkbox"/> |
| Executive Director & Senior General Counsel LS / Directeur exécutif et Avocat général principal SJ Michael Sousa | | | <input type="checkbox"/> | <input type="checkbox"/> |
| A/Assistant Deputy Minister PACB / Sous-ministre adjoint SACP Jill Wherrett | APR 12 2017 | JW | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Assistant Deputy Minister CSCCB / Sous-ministre adjointe SSCLCC Kathy Thompson | | | <input type="checkbox"/> | <input type="checkbox"/> |
| Chief Financial Officer and Assistant Deputy Minister CMB / Dirigeant principal des finances et Sous-ministre adjoint SGM | | | <input type="checkbox"/> | <input type="checkbox"/> |
| Assistant Deputy Minister EMPB / Sous-ministre adjointe SGUP Lori MacDonald | | | <input type="checkbox"/> | <input type="checkbox"/> |
| Senior Assistant Deputy Minister NCSB / Sous-ministre adjoint principale SSCN Monik Beaugard | | | <input type="checkbox"/> | <input type="checkbox"/> |
| Associate Deputy Minister / Sous-ministre déléguée Gina Wilson | 20-APR-17 | [Signature] | <input type="checkbox"/> | <input type="checkbox"/> |
| Deputy Minister / Sous-ministre Malcolm Brown | | [Signature] | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Minister / Ministre The Honourable / L'honorable Ralph Goodale | | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

**SIGN
HERE**

CBSA Quarterly Media Analysis | Analyse médiatique trimestriel de l'ASFC

2017-04-01 – 2017-06-30



Table of Contents / Table des matières



1. **Asylum Seekers / demandeurs d'asile**
2. **Removals & Deportations / renvoi et expulsions**
3. **Bill C38, C23 / projet de loi C38, C23**
4. **Oversight / organisme de surveillance**
5. **Fraudulent Passports / passport frauduleuse**
6. **Immigration Detention / détention liée à l'immigration**
7. **Airports / aéroports (Ottawa, Toronto, Montreal & Vancouver)**
8. **Port Runners / coureurs de ports**
9. **Lifting of Visa Requirements for Mexico / annulation du visa obligatoire pour le Mexique**
10. **Opioids at the Border / les opioïdes à la frontière**
11. **Reporting requirements for boaters / exigences en matière de déclaration pour les plaisanciers privés (C233)**

parliamentarians to oversee agencies with security and intelligence responsibilities, including the border agency. However, the government has signalled that some kind of specially designed means of reviewing the border agency is also in the works. Cappe, Privy Council clerk for three years during Jean Chretien's tenure as prime minister, is looking at existing review and oversight of the agency, including any gaps, as well as potential models for more comprehensive monitoring. Canadian Press (Cape Breton Post) (2017-05-18)

Don't change lawful access rules, Parliamentary committee recommends

Liberal-dominated parliamentary committee says the government shouldn't change the current lawful access regime that limits the ability of police to get at telecom subscriber information and encrypted data unless they have a warrant. The recommendation came this week from the House of Commons' public safety and national security committee as part of a broad review of the country's national security framework. Last year the Trudeau government launched a public consultation into federal national security policy, which included the parliamentary committee's work. The government hasn't given an indication yet of when a new policy will be issued. Today a spokesperson for the Canadian Wireless Telecommunications Association (CTWA) which represents most of the country's wireless carriers, said the group had no comment on the committee's recommendations because government policy hasn't changed. The parliamentary committee also made other national-security related recommendations including increasing the funding of all public safety and national security review bodies, limiting the powers of the Canadian Security and Intelligence Service (CSIS) and more oversight over federal national security bodies. IT World Canada (2017-05-04)

Time to rein in security overreach

An editorial states "In opposition, the Liberals took a strange stand on the Harper government's draconian anti-terror legislation, formerly Bill C-51. They agreed to support the bill, with the proviso that, if they won the election, they would rein in its worst excesses. Well, they won - but nearly halfway through their first mandate, the reining-in has yet to begin... While the Trudeau government has been troublingly phlegmatic on security reform, it did introduce a welcome bill last summer to create a parliamentary committee on security and intelligence, which would provide much-needed democratic oversight of our ever-expanding security apparatus. But the new report recognizes that, while necessary, the effort is on its own insufficient to guard against abuses and hold our security establishment to account. Canada's sprawling security apparatus is currently monitored by three meagre watchdogs, each strictly tethered to its own jurisdiction. Critics have long maintained that these bodies have neither the mandate nor the resources to do their job. Moreover, certain organizations, such as the Canada Border Services Agency, fall within the jurisdiction of none of these watchdogs and escape scrutiny altogether. The committee rightly calls on the government to create an oversight body for CBSA, to improve funding to all of the watchdogs and to form a so-called super watchdog to harmonize the efforts of Canada's patchwork of oversight bodies, a longstanding recommendation of many security experts." Toronto Star (2017-05-04)

Commons committee calls for rollback of key C-51 anti-terror measures

A House of Commons committee is calling for repeal of a provision that allows Canada's spy agency to violate constitutional rights in the name of disrupting threats. In a report Tuesday, the Liberal-dominated public safety committee also recommended requiring a judge's approval for any Canadian Security Intelligence Service disruption operations that break Canadian law. In addition, the MPs said the scope of activities subject to recently enacted information-sharing powers should be narrowed to make them consistent with other national security legislation... **It calls for a new, independent review body for the Canada Border Services Agency**, gateways between all national security review bodies to allow information exchange and joint investigations, as well as more funding for these watchdogs. Canadian Press (Times and Transcript, B4) (2017-05-03)

Terrorisme: Ottawa va restreindre les pouvoirs de ses espions

James Bond pourrait devoir remballer sa quincaillerie. Du moins, c'est ce que propose le Comité parlementaire sur la sécurité publique et nationale, qui suggère à Justin Trudeau une quarantaine de mesures pour mieux encadrer les pouvoirs antiterroristes canadiens, notamment ceux des espions. La Loi antiterroriste adoptée par le précédent gouvernement conservateur en 2015, peu avant l'élection, avait suscité une vague d'indignation. Le C-51 octroyait au Service canadien du renseignement de

Today's News / Actualités
April 3, 2017 / le 3 avril 2017
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / LES FEMMES ET LES FILLES
AUTOCHTONES DISPARUES ET ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

Ottawa Power Rankings - Our weekly guide to the political winners and losers on Parliament Hill
An opinion piece states "... WHO'S DOWN... **Ralph Goodale** - Yes, the public safety minister has stuff to do. He's a key minister on the border-crossing file; the RCMP is his to worry about. But Federal Court Chief Justice Paul Crampton wasn't buying the argument, made by federal lawyers in a sensitive immigration case, that **Goodale** was simply too busy to make a timely decision. Crampton ruled no minister "can take as many years as they see fit to respond to requests made pursuant to validly enacted legislation." Get to it, minister." [Macleans](#)

Why warrantless access to Internet information is back on the lawmaking agenda

An opinion piece states "The federal government has yet to release its response to last year's national-security consultation, but at least one thing is increasingly apparent. Lawful access, the regulations that govern police access to Internet- and telecom-subscriber information, will be back **on Public Safety Minister Ralph Goodale's legislative agenda**. The details of the complex new rules that would grant warrantless access to some telecom and Internet information system are still a work in progress, but the final outcome is sure to raise concerns with privacy advocates as well as telecom and Internet providers.

A cybercrime working group comprised of senior officials from federal, provincial and territorial governments have spent months developing the new lawful-access framework. It recently held two invitation-only consultations on the issue with Canadian telecom and Internet companies as well as civil society groups and academic experts. I participated in the latter event, which was held under Chatham House rules that allow for disclosure of the content of the meeting without attribution to specific commentators." [Globe and Mail](#)

[BACK TO TOP / HAUT DE LA PAGE](#)

TOP STORIES / MANCHETTES

Flooding prompts evacuations in 2 Manitoba First Nations

Two Manitoba communities have been partly evacuated due to flooding affecting areas across the southern and central parts of the province. Residents of Peguis First Nation and Sioux Valley Dakota Nation had to leave their homes in recent days. The Canadian Red Cross is working with both communities, provincial officials said. Peguis Chief Glenn Hudson said 135 residents are in Winnipeg on Monday, and some 300 houses are affected directly or indirectly in the community about 180 kilometres north of Winnipeg. Sioux Valley Chief Vince Tacan said between 10 and 15 houses along a creek were evacuated Sunday evening as high water threatened a bridge used to access the homes. Evacuees are staying in Brandon, Man., he said... Local states of emergency have been declared in nine Manitoba communities: Prairie Lakes, Grassland, Brenda-Waskada, Dufferin, Grey, La Broquerie and Two Borders, and the Town of Carman, as well as Peguis. The culprit in many cases is ice jams, a flood update from the province said Monday. The jams can happen when run-off begins before river ice melts, and the flooding they cause is difficult to predict, the province said. A flood watch has been issued for the lower Assiniboine River from Portage la Prairie to Headingley due to possible ice issues. [CBC News](#); [Radio-Canada](#)

Flood 2017: Manitoba's hotspots and where the worst is yet to come

When the low-capacity Fisher River spills over its banks at Peguis, flood forecasters call it spring. But it's a lot stranger to see the normally placid Boyne River threaten homes in Carman, Man. So far, the 2017 flood season has brought southern and central Manitoba a mix of the surprising and the mundane, thanks to ice jams that create sudden trouble spots and perennially problematic rivers just being themselves. Here's where the flooding is the worst right now, where it's no longer a major threat - and where it's most likely to worsen in the coming days and weeks. [CBC News](#)

Someone is spying on cellphones in the nation's capital - A CBC/Radio-Canada investigation has found cellphone trackers at work near Parliament Hill and embassies

A months-long CBC News/Radio-Canada investigation has revealed that someone is using devices that track and spy on cellphones in the area around Parliament Hill. The devices are known as IMSI catchers and have been used by Canadian police and security authorities, foreign intelligence and even organized crime. The devices, sometimes known by the brand name of one model, StingRay, work by mimicking a cellphone tower to interact with nearby phones and read the unique ID associated with the phone — the International Mobile Subscriber Identity, or IMSI. That number can then be used to track the phone and by extension the phone's user. In some instances, IMSI catchers can even be used to gain access to a phone's text messages and listen in on calls... We also showed our results to an expert in Canadian security. He knows a lot about IMSI catchers and comes from a Canadian security agency. We agreed to conceal his identity in order not to jeopardize that security work. The expert found the results of our

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Tuesday, April 04, 2017 8:46 AM
To: Cyber Security / Sécurité cybernétique (PS/SP)
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique - 2017-04-04

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique April 4, 2017 / le 4 avril 2017

Print Media / Médias imprimés

Why warrantless access to Internet information is back on the legislative agenda

An opinion piece by security expert Michael Geist states, "The federal government has yet to release its response to last year's national-security consultation, but at least one thing is increasingly apparent. Lawful access, the regulations that govern police access to Internet- and telecom-subscriber information, will be back on **Public Safety Minister Ralph Goodale's** legislative agenda. The details of the complex new rules that would grant warrantless access to some telecom and Internet information systems are still a work in progress, but the final outcome is sure to raise concerns with privacy advocates as well as telecom and Internet providers..." Globe and Mail, B4

Canada taps Israel for expertise on cyber issues

The federal government sought advice and assistance last fall from Israel to toughen Canada's cybersecurity defences and to find ways Ottawa could encourage private sector investments in cybersecurity, the National Post has learned. Documents obtained by the Post detail meetings last September between the top members of Israel's National Cyber Directorate, a unit inside the Prime Minister's Office, and senior federal officials, including Daniel Jean, the national security adviser to Prime Minister Justin Trudeau... The key group of meetings between Canadian and Israeli officials took place in Ottawa on Sept. 8. They were hosted by Public Safety Canada. Representatives of several federal departments took part in some or all of the meetings... Since that meeting with the Israelis, **Public Safety Canada** has quietly published the results of consultations it held with about 2,000 stakeholders, academics, experts and members of the public on cyber issues. The "Cyber Review Consultations Report," posted online March 9 by **Public Safety Canada**, spells out potential recommendations for action by the private sector, law enforcement agencies and the government. "The Government of Canada can provide much needed leadership by creating, adopting and modelling best practices for cyber security, and making efforts to transfer this knowledge to the private sector," said the review, which was prepared by AC-Nielsen of Canada Co. Review participants told **Public Safety Canada** that both federal and provincial anti-cybercrime initiatives need more money and resources. There were also suggestions that government offer incentives and tax credits to encourage best practices. Postmedia Network (Edmonton Journal, N4; Ottawa Citizen, National Post, Vancouver Sun, Calgary Herald)

Cyber Caliphate releasing hit list

ISIS masterminds have drawn up a hit list of 8,700 people the death cult has targeted for death - including Canadians. And the jihadis are telling their fanatical followers: "kill them wherever you find them." According to The UK Sun, the pro-ISIS United Cyber Caliphate (UCC) hacking group has unveiled a twisted video threatening the U.S., Donald Trump, Canadians, Brits and thousands of others. And the sickos are threatening to release the list and addresses of its intended victims, triggering lone wolf attackers to go on murderous rampages. Politicians, celebrities, religious leaders and anti-ISIS Muslims around the world are said to make up the list. Toronto Sun, A13; International Business Times

Ex-Mountie takes job with China's Huawei

A senior Mountie has retired from Canada's national police force to take a job with a Chinese corporation that Ottawa officials have sometimes shunned as an espionage risk. RCMP assistant commissioner Pierre Perron, a 35-year Mountie, was the national police force's chief information officer until he retired in March. He has been hired by Huawei Technologies as a brand ambassador for the Shenzhen-based company's police information technology initiative. Globe and Mail, A5

Commission Chamberland - La surveillance des sources, un grave problème démocratique

"La chasse aux sources, c'est du quatre saisons au Québec, et c'est un grave problème démocratique", a lancé le directeur du Devoir, Brian Myles, aux côtés des patrons de Radio-Canada et de La Presse, lors du premier jour des

audiences de la commission Chamberland, qui enquête sur la protection de la confidentialité des sources journalistiques. Les trois médias ont souligné le fait que, dans le système actuel, la presse est tenue dans l'ombre quand un policier fait une demande auprès d'un juge de paix pour avoir accès à des informations sur les sources d'un reporter. " On n'est même pas représentés ", a déploré Éric Trottier, éditeur adjoint du quotidien La Presse. Rappelons que la Commission d'enquête sur la protection de la confidentialité des sources journalistiques a été mise sur pied par le gouvernement du Québec en novembre dernier après que des cas de surveillance de journalistes par la police ont été révélés. Pour Brian Myles, la surveillance " a plus été faite pour débusquer les taupes que pour faire déboucher les enquêtes ". Selon lui, les membres des médias ont servi de cheval de Troie pour identifier " des gens qui parlaient un peu trop ". Le Devoir, B8 ; La Presse Canadienne (Le Nouvelliste, * La Voix de l'Est); * La Presse+ ; * Agence QMI (Le Journal de Montréal, Le Journal de Québec) ; * Montreal Gazette

U.S. man accused of importing child porn

A 43-year-old American citizen faces child pornography charges after a seizure by agents at a border crossing between Saskatchewan and the United States. Brandon Eugene Johnson, 43, of Knoxville, Tenn., has been charged with one count each of possession of child porn and importation of child porn. He appeared Monday in Estevan provincial court. According to the Saskatchewan Internet Child Exploitation (ICE) unit in a news release, a search by Canada Border Services Agency (CBSA) officers at the North Portal border crossing "resulted in the discovery of suspected child pornography on electronic devices." A man was arrested and turned over to the ICE unit, which "confirmed the suspect images as child pornography." According to the CBSA, border officers seized child porn from travellers in Saskatchewan on six different occasions last year. Star Phoenix, A5

Arrest made in PharmaNet breach

Police have arrested a man suspected of gaining unauthorized access to B.C.'s PharmaNet system and using patients' personal information for fraudulent purposes. The Crown has yet to lay charges, but the government says about 20,500 patients might have been affected by the privacy breach - nearly three times as many as initially thought. Times Colonist, A3; Postmedia Network (The Province, A8; Vancouver Sun); Globe and Mail, S2

Attention aux publications sur le Web

Le gouvernement du Québec tente de sensibiliser les jeunes sur l'importance de leur publication sur Internet afin de leur éviter de mauvaises surprises... La tournée provinciale vise à mettre en garde les étudiants sur la liberté de leurs renseignements personnels, au vol d'identité et à protéger leur réputation. Le Quotidien, 2

Online Media / Médias en ligne

Someone is spying on cellphones in the nation's capital - A CBC/Radio-Canada investigation has found cellphone trackers at work near Parliament Hill and embassies

A months-long CBC News/Radio-Canada investigation has revealed that someone is using devices that track and spy on cellphones in the area around Parliament Hill. The devices are known as IMSI catchers and have been used by Canadian police and security authorities, foreign intelligence and even organized crime. The devices, sometimes known by the brand name of one model, StingRay, work by mimicking a cellphone tower to interact with nearby phones and read the unique ID associated with the phone — the International Mobile Subscriber Identity, or IMSI. That number can then be used to track the phone and by extension the phone's user. In some instances, IMSI catchers can even be used to gain access to a phone's text messages and listen in on calls... We also showed our results to an expert in Canadian security. He knows a lot about IMSI catchers and comes from a Canadian security agency. We agreed to conceal his identity in order not to jeopardize that security work. The expert found the results of our investigation disturbing. "That an MP or a person who works on Parliament Hill could be exposed, that they could be a victim of this type of attack— it undermines our sovereignty," he said... We reached out to police, security agencies, embassies and the federal government to ask if they were involved in the IMSI catchers we detected. The Department of National Defence said it had no knowledge of IMSI catchers being used on the dates we saw activity. The **Department of Public Safety**, the Ottawa Police Service, the RCMP and CSIS all gave similar responses: They don't discuss specific investigative techniques but they do follow the law, respect the Charter of Rights and Freedoms and adhere to the appropriate judicial processes. CBC News

'Serious' hack attacks from China targeting UK firms

UK firms have been warned about "serious" cyber attacks originating in China that seek to steal trade secrets. The gang behind the attacks has compromised technology service firms and plans to use them as a proxy for attacks, security firms have said. The group, dubbed APT10, is using custom-made malware and spear phishing to gain access to target companies. The National Cyber Security Centre and cyber units at PwC and BAE Systems collaborated to identify the group. "Operating alone, none of us would have joined the dots to uncover this new campaign of indirect attacks," said Richard Horne, cyber security partner at PwC. Known victims. A detailed report drawn up by the three organisations

reveals that the group has been active since 2014 but ramped up its attacks in late 2016. In particular, said the report, it targeted firms who ran key IT functions on behalf of large UK companies. [BBC News](#); [Infosecurity-Magazine](#)

This Map Shows the UK's Surveillance Exports

IMSI catchers, intrusion software, internet monitoring solutions: UK companies provide it all. The UK is a worldwide exporter of surveillance technology. From devices that Hoover up phone calls and text messages, to hardware for monitoring internet traffic, Her Majesty's Government has granted myriad licenses to ship spying gear over the past few years. Some of the recipient countries will have legitimate uses for such products, but many—Egypt, Turkey, Saudi Arabia—also have abhorrent human rights records, especially when it comes to abusing powerful surveillance tech. [Motherboard](#)

Aviation tech heavyweights join forces on cybersecurity

SITA has linked up with Airbus to provide a cybersecurity service designed specifically for the air transport industry. In 2016, SITA identified cybersecurity as one of its five priorities. Its Airline IT Trends Survey 2016 found that 91% of airlines were planning to invest in this area over the next three years. [Tnooz](#)

IAAF says athlete database hacked by Russia-linked group

The governing body of track and field has been hacked by Fancy Bears, the group that previously attacked the World Anti-Doping Agency. The IAAF said Monday it believes the hack "has compromised athletes' Therapeutic Use Exemption (TUE) applications stored on IAAF servers" during an unauthorized remote access to its network on Feb. 21. [Associated Press](#) (Toronto Star)

Parents of alleged Yahoo hacker distraught over arrest and media portrayal of 'kind' son

The parents of an alleged "hacker-for-hire" connected to a massive international data breach maintain that their son is innocent, and a "scapegoat" in a case that is tearing them apart. "It's like someone cut off our roots, and took out our hearts," said Akhmet Tokbergenov, the father of Karim Baratov, 22, who faces charges laid by the U.S. Justice Department related to computer hacking, economic espionage and several other offences. [CBC News](#)

Don't pay ransoms. But if you must, here's where to buy the Bitcoins

Ransomware grew into a \$1 billion industry last year, and ransom payments now account for nearly 10 percent of the entire Bitcoin economy. [CSO](#)

Most Brits Would Feel 'Safer' Without Encryption

Two-thirds of the British public claim the ability of police to intercept and read communications between terrorists is more important than privacy, according to a new study. [Infosecurity-Magazine](#)

Lazarus Group Exposed with Major New North Korea Link

Security experts have lifted the lid on the notorious Lazarus Group pegged for the Bangladesh Bank attack, linking it to countless watering hole attacks on financial and crypto-currency firms round the world and, most interestingly, suggesting a strong connection to North Korea. [Infosecurity-Magazine](#); [CSO](#)

Cybersécurité : McAfee est de retour

Sécurité : Intel Security c'est fini. Le fondateur se sépare de sa division cybersécurité, qui redevient McAfee. La société conserve 49% de la nouvelle structure. McAfee est désormais valorisé à hauteur de 4,2 milliards de dollars. [ZDNet France](#)

Blockchain : Bercy lance une consultation publique

La blockchain prend ses distances avec le bitcoin et la technologie de registre décentralisé intéresse de nombreux secteurs. Si les banques sont évidemment sur le pied de guerre, d'autres activités voient un intérêt au développement de cet outil de validation des transactions qui permet de se passer d'une autorité centrale. [ZDNet France](#)

Old attack code is new weapon for Russian hackers

for as long as they keep working. In that tradition, researchers have found evidence suggesting a cyberespionage group is still successfully using tools and infrastructure that was first deployed in attacks 20 years ago. [CSO](#)

President Donald Trump signed a resolution on Monday that officially repeals Obama-era broadband privacy rules.

Trump's signature comes a few days after both houses of Congress narrowly voted to stop the rules, which were adopted last year but had not yet taken effect. The rules would have required broadband and wireless companies to get your permission before sharing sensitive information about you, such as the websites you visit, the apps you use or even your location. [CNet News](#)

*Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité
publique. We can be reached at / Vous pouvez nous contacter à: PS.PSPMediaCentre-
CentredesmediasPSP.SP@Canada.ca*

Sent to: !Cyber Security Media Summary Dist List #1; !Cyber Security Media Summary Dist List #2; !Cyber Security Media
Summary Dist List #3; !Cyber Security Media Summary Dist List #4



Canadian
Security
Intelligence
Service

Service
canadien du
renseignement
de sécurité

Daily Media Summary / Revue de presse quotidienne
Canadian Security Intelligence Service / Service canadien du renseignement de sécurité
April 4, 2017 / le 4 avril 2017

CSIS IN THE NEWS / LE SCRS DANS LES NOUVELLES

MINISTER / MINISTRE

SECURITY AND LAW ENFORCEMENT / SÉCURITÉ ET EXÉCUTION DE LA LOI

BORDER ISSUES / ENJEUX FRONTALIERS

CYBER AND TECHNOLOGY / CYBER ET TECHNOLOGIE

MILITARY ISSUES / ENJEUX MILITAIRES

PUBLIC SERVICE / FONCTION PUBLIQUE

LEGISLATION AND POLICIES / LÉGISLATION ET POLITIQUES

OTHER / AUTRES

CSIS IN THE NEWS / LE SCRS DANS LES NOUVELLES

Someone is spying on cellphones in the nation's capital

A months-long CBC News/Radio-Canada investigation has revealed that someone is using devices that track and spy on cellphones in the area around Parliament Hill. The devices are known as IMSI catchers and have been used by Canadian police and security authorities, foreign intelligence and even organized crime. The devices, sometimes known by the brand name of one model, StingRay, work by mimicking a cellphone tower to interact with nearby phones and read the unique ID associated with the phone - the International Mobile Subscriber Identity, or IMSI. That number can then be used to track the phone and by extension the phone's user. In some instances, IMSI catchers can even be used to gain access to a phone's text messages and listen in on calls. We wanted to know more about who might be using the IMSI catcher or catchers that we detected, so we asked the U.S. supplier of the CryptoPhone to analyze the alerts we were getting. ESD America specializes in counterintelligence and its clients include U.S. Homeland Security. "Consistently you've been seeing IMSI catcher activity, definitely," said CEO and co-founder Les Goldsmith, when we took our results to the company's Las Vegas office. Based on the configurations suggested by CBC's results, he believes the IMSI catchers detected in Ottawa could be foreign made. "We're seeing more IMSI catchers with different configurations and we can build a signature. So we're seeing IMSI catchers that are more likely Chinese, Russian, Israeli and so forth," he said. We also showed our results to an expert in Canadian security. He knows a lot about IMSI catchers and comes from a Canadian security agency. We agreed to conceal his identity in order not to jeopardize that security work. The expert found the results of our investigation disturbing. "That an MP or a person

certainly would be open to any suggestions or advice about how it might be upgraded or improved to make sure that we are getting accurate information." Globe and Mail, A1

Why warrantless access to Internet information is back on the legislative agenda

An opinion piece written by Michael Geist, Canada Research Chair in Internet and E-commerce Law at the University of Ottawa, states "The federal government has yet to release its response to last year's national-security consultation, but at least one thing is increasingly apparent. Lawful access, the regulations that govern police access to Internet- and telecom-subscriber information, will be back on **Public Safety Minister Ralph Goodale's** legislative agenda. The details of the complex new rules that would grant warrantless access to some telecom and Internet information systems are still a work in progress, but the final outcome is sure to raise concerns with privacy advocates as well as telecom and Internet providers. A cybercrime working group comprised of senior officials from federal, provincial and territorial governments have spent months developing the new lawful-access framework. It recently held two invitation-only consultations on the issue with Canadian telecom and Internet companies as well as civil society groups and academic experts. I participated in the latter event, which was held under Chatham House rules that allow for disclosure of the content of the meeting without attribution to specific commentators. Many in the privacy and telecom fields had assumed that the lawful-access issue was settled in 2014. The government established several new warrants that opened the door to preserving subscriber information and granted law enforcement additional access to the data. When combined with the Supreme Court of Canada Spencer decision that affirmed a reasonable expectation of privacy in subscriber information, Canadian law enforcement was seen to have the necessary legal tools to combat cybercrime with courtapproved access to Internet and telecom information. The consultation meetings left no doubt that law enforcement is not satisfied with the current system, however. It is seeking significant reforms that would require telecom and Internet companies to disclose some subscriber information without court oversight. Police officers point to a sizable jump in the number of warrant requests following the Spencer decision as the justification for easing the rules of access. Working-group officials emphasized that no final decisions have been made, but much of the internal debate has shifted from whether more reforms are needed to what information could be required to be disclosed without court oversight and what should be subject to a warrant." Globe and Mail, B4

SECURITY AND LAW ENFORCEMENT / SÉCURITÉ ET EXÉCUTION DE LA LOI

Cyber Caliphate releasing hit list

ISIS masterminds have drawn up a hit list of 8,700 people the death cult has targeted for death - including Canadians. And the jihadis are telling their fanatical followers: "kill them wherever you find them." According to The UK Sun, the pro-ISIS United Cyber Caliphate (UCC) hacking group has unveiled a twisted video threatening the U.S., Donald Trump, Canadians, Brits and thousands of others. And the sickos are threatening to release the list and addresses of its intended victims, triggering lone wolf attackers to go on murderous rampages. Politicians, celebrities, religious leaders and anti-ISIS Muslims around the world are said to make up the list. Toronto Sun, A13; International Business Times (2017-04-04)

La STM prête à faire face à un attentat

Le métro de Montréal serait prêt à faire face à une explosion comme celle qui a fait 11 morts hier en Russie. «La STM est en lien constant avec les organismes de sécurité, selon des protocoles bien établis. Nous ne pouvons toutefois dévoiler la teneur de ces protocoles ou des mesures prises, pour des questions de sécurité», a indiqué Amélie Régis, porte-parole de la Société de Transport de Montréal (STM). Une position confirmée par Michel Juneau-Katsuya, expert en espionnage, contre-espionnage et terrorisme. «On ne sait jamais comment les choses vont se dérouler, est-ce qu'on est prêt? La réponse est oui, les services essentiels du transport et de la Ville ont planifié et fait des exercices. Est-ce qu'on va pouvoir empêcher des victimes supplémentaires, ça dépendra de l'événement.» Le Journal de Québec, 23 (Le Journal de Montréal)

Ex-Mountie takes job with China's Huawei

**Daily Media Summary / Revue de presse quotidienne
Public Safety Canada / Sécurité publique Canada
April 4, 2017 / le 4 avril 2017**

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse quotidienne
peut également être accédée via [InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / LES FEMMES ET LES FILLES
AUTOCHTONES DISPARUES ET ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRE

INTERNATIONAL

MINISTER / MINISTRE

China extradition talks 'long way' off

Canada remains far from formally discussing an extradition treaty with China, the new ambassador to Beijing says. "We are a long, long way from negotiations, let alone agreeing to such an agreement," said John McCallum, two weeks after taking up Canada's top diplomatic posting in Beijing... The lack of such a deal has not, however, stopped Canada from sending people back to China, without receiving any assurances that they will not be tortured or otherwise mistreated. The Canada Border Services Agency has deported 1,386 people to China over the past three years, according to agency statistics recently provided to The Globe. **Public Safety Minister Ralph Goodale defended** Canada's removal process Monday when asked how the government can be sure that those deported to China will not be treated badly. **"There's a due process that is followed in every case," Mr. Goodale said. "I certainly would be open to any suggestions or advice about how it might be upgraded or improved to make sure that we are getting accurate information."** [Globe and Mail](#), A1

As Stanley hearing gets underway, Regina groups rally against SARM resolution on self-defence

The Saskatchewan Coalition Against Racism and Colonialism No More rallied Monday against what they called "the racist violence and misconceptions that SARM appears to be stoking," after the rural umbrella group's resolution to lobby for the relaxation of property self-defence laws... "To me there's an overt tone of racism when it comes to SARM resolutions," said Dodie Ferguson, rally co-organizer, citing official figures that show rural crime rates falling in the province's south. Ferguson added that she welcomed official voices who said they would not support the SARM move, such as Federal Minister for **Public Safety Ralph Goodale** and Saskatchewan Minister for Justice Gordon Wyant, saying it proved they were "doing their homework"... Ferguson said she understands SARM's campaign around improving rural policing, but said the Kindersley resolution and concerns about RCMP response times were very separate matters. Postmedia Network (Leader-Post. A7; StarPhoenix)

Why warrantless access to Internet information is back on the legislative agenda

An opinion piece by security expert Michael Geist states, "The federal government has yet to release its response to last year's national-security consultation, but at least one thing is increasingly apparent. Lawful access, the regulations that govern police access to Internet- and telecom-subscriber information, will be back on **Public Safety Minister Ralph Goodale's** legislative agenda. The details of the complex new rules that would grant warrantless access to some telecom and Internet information systems are still a work in progress, but the final outcome is sure to raise concerns with privacy advocates as well as telecom and Internet providers..." Globe and Mail, B4

Do Your Job

A letter to the editor states, Re: "Back door wide open," Mark Bonokoski, March 30. **Public Safety Minister Ralph Goodale says: "I guess what the Conservatives are saying is maybe we should line up the RCMP at the border, link arms and shoo people away."** Actually, it's Canadians saying that. And yes, maybe the RCMP should be lining up arms-linked at the border as then they'd be doing their jobs, unlike **Mr. Goodale** who isn't doing his. We need less talk on border security and more action from **Minister Goodale.** Winnipeg Sun, A8

[BACK TO TOP / HAUT DE LA PAGE](#)

TOP STORIES / MANCHETTES

*** Des craintes d'une « catastrophe imminente »**

Les inspecteurs de l'aviation civile sont inquiets des changements récents visant le programme de surveillance sur la sécurité aérienne et ont un mauvais pressentiment qu'un accident d'aviation majeur pourrait survenir prochainement au Canada. C'est ce que révèle un sondage Abacus Data Study mené auprès des inspecteurs de l'aviation, rendu public lundi par l'Association des pilotes fédéraux du Canada (APFC), à la veille de l'étude sur la sécurité aérienne que doit entreprendre le comité permanent des transports, de l'infrastructure et des collectivités. Le Droit, 9

*** Volunteers in Manitoba town scramble to halt flooding from nearby river**

The threat of flooding from an ice-choked river has prompted a big southern Manitoba town to declare a state of emergency. Officials in Carman say rising water on the Boyne River is causing flooding and sewer backups in the community of 3,400, about 90 kilometres southwest of Winnipeg. Canadian Press (Daily Star, 12); Winnipeg Sun, A4

*** Flooding forces nearly 200 from homes**

Water from the Fisher River was slowly receding Monday at Peguis First Nation after flooding caused by ice jams forced evacuations from more than 80 homes in the community during the weekend. Chief Glenn Hudson said the floodwater has receded only about 15 centimetres and the community, located about 180 kilometres north of Winnipeg, has been inundated with water. Winnipeg Free Press, 4; Winnipeg Sun, A4

GRC-RCMP



GENDARMERIE ROYALE DU CANADA / ROYAL CANADIAN MOUNTED POLICE

**Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
April 4, 2017 / le 4 avril 2017**

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse quotidienne peut également être accédée via [InfoMédia](#)

TOP STORIES / ACTUALITÉS

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

OTHER / AUTRES

TOP STORIES / ACTUALITÉS

Someone is spying on cellphones in the nation's capital - A CBC/Radio-Canada investigation has found cellphone trackers at work near Parliament Hill and embassies

A months-long CBC News/Radio-Canada investigation has revealed that someone is using devices that track and spy on cellphones in the area around Parliament Hill. The devices are known as IMSI catchers and have been used by Canadian police and security authorities, foreign intelligence and even organized crime. The devices, sometimes known by the brand name of one model, StingRay, work by mimicking a cellphone tower to interact with nearby phones and read the unique ID associated with the phone — the International Mobile Subscriber Identity, or IMSI. That number can then be used to track the phone and by extension the phone's user. In some instances, IMSI catchers can even be used to gain access to a phone's text messages and listen in on calls... We also showed our results to an expert in Canadian security. He knows a lot about IMSI catchers and comes from a Canadian security agency. We agreed to conceal his identity in order not to jeopardize that security work. The expert found the results of our investigation disturbing. "That an MP or a person who works on Parliament Hill could be exposed, that they could be a victim of this type of attack— it undermines our sovereignty," he said... We reached out to police, security agencies, embassies and the federal government to ask if they were involved in the IMSI catchers we detected. The Department of National Defence said it had no knowledge of IMSI catchers being used on the dates we saw activity. The Department of Public Safety, the Ottawa Police Service, the RCMP and CSIS all gave similar responses: They don't discuss specific investigative techniques but they do follow the law, respect the Charter of Rights and Freedoms and adhere to the appropriate judicial processes. [CBC News](#) (2017-04-03)

An opinion piece states, "A survey dealing with pay showed the RCMP ranked 72 out of 82 police services in Canada. The RCMP top brass are well paid, but the rank and file are not. It's time for a change. Quebec and Ontario have had their own provincial police service for more than 100 years. It works well. It is now time for the RCMP to get out of contract policing of provinces and go back to their original status as a federal police service. Policing is a provincial responsibility." [Calgary Herald](#), A9

Why warrantless access to Internet information is back on the lawmaking agenda

An opinion piece states "The federal government has yet to release its response to last year's national-security consultation, but at least one thing is increasingly apparent. Lawful access, the regulations that govern police access to Internet- and telecom-subscriber information, will be back on Public Safety Minister Ralph Goodale's legislative agenda. The details of the complex new rules that would grant warrantless access to some telecom and Internet information system are still a work in progress, but the final outcome is sure to raise concerns with privacy advocates as well as telecom and Internet providers. A cybercrime working group comprised of senior officials from federal, provincial and territorial governments have spent months developing the new lawful-access framework. It recently held two invitation-only consultations on the issue with Canadian telecom and Internet companies as well as civil society groups and academic experts. I participated in the latter event, which was held under Chatham House rules that allow for disclosure of the content of the meeting without attribution to specific commentators." [Globe and Mail](#) (2017-04-03)

Are Marc and Jodie Emery bad for the weed movement?

An opinion piece states, "'I'd still like to be the Starbucks of weed,'" says Jodie Emery, fresh from her first strip-search jail stint. After an arrest in Toronto, she's back in Vancouver, sipping a latte inside a busy West Hastings Street cafe. Across the street is her grungy Cannabis Culture headquarters. Which, because of certain Ontario court bail conditions laid down in March, she cannot visit. She clings to her dream of building a retail network into "the most recognized brand in retail storefronts and lounges." A string of Cannabis Culture franchises across Canada. Shelves filled with top-notch pot. Smoking lounges. Special appearances with herself, the photogenic, friendly face behind the family brand. Free dab hits courtesy of her husband, the irascible Marc (a dab, for the uninitiated, is a highly concentrated form of cannabis, usually smoked directly from a hot surface or flame).(...) They are by no means contrite. They remain outspoken. But if the Emerys are true to their word and they stay away from illicit, unregulated marijuana sales, they may do the pro-pot movement a big favour. Because they weren't helping anymore." [Maclean's](#) (2017-04-03)

Parents dreading legal weed should chill out

An opinion piece states, "The annual worldwide celebration of marijuana smoking, a.k.a. 4/20, has always struck me as a little bit awkward. This is because the day on which it falls and from which it gets its name - April 20 - also happens to be the birthday of Adolf Hitler, a man whose memory (for most) does not inspire the kind of good vibes one hopes to achieve at a weed festival. Hitler, as a 4/20 reveller might put it, was not a chill dude. The federal Liberal party, on the other hand, is doing its best to prove that it's packed full of chill dudes and of course, dudettes. (It's 2017, after all.) Last month, amid criticism that they lack progressive chops, the Libs announced plans to table legislation that may very well give Canada a brand new, Hitler-free 4/20 all its own. To be more specific, if things go as planned for Trudeau's Liberals, marijuana will be officially legal in the great white north on July 1, 2018. Goodbye 4/20. Hello Cannabis Day. I mean Canada Day. The fireworks will be so trippy, the hamburgers so juicy, and the parents of teenagers: so un-chill. After all, one of the most common criticisms levelled at legal weed is that it will negatively impact Canadian youth. That it will turn teenagers' minds to putty and persuade even the most prudish poindexter to trade in his good sense for a ride on the reefer train, because when something previously illegal suddenly turns legit, well, who can resist?" [Toronto Star](#), A5

Candidly Canada: Legalizing marijuana is step forward

An opinion piece states, "With rising temperatures up north, Canada isn't only reaching new highs in spring weather, but also in its forward-thinking policies. According to the CBC, Canada's liberal government will announce legislation this month that will nationally legalize marijuana by next summer. Provinces will have the right to decide how the marijuana is distributed and sold, what prices are appropriate and what age to sell to." [Volante Online](#) (2017-04-03)

Levert, Jean-Philippe (PS/SP)

From: [REDACTED]
Sent: Friday, April 07, 2017 9:26 AM
To: [REDACTED] Baker3, Ryan (PS/SP)
Cc: Media Relations / Relations avec les médias (PS/SP)
Subject: Re: URGENT-- Canada's top spy agencies work out deal on 'threat disruption' operations

s.15(1) - Subv

Here is what we provided:

Thank you again for your questions and interest in CSE's work. We understand that you've also been in touch with CSIS and that they will be providing you with the MoU document before your deadline today.

Regarding CSE assistance to CSIS, Part C of CSE's mandate, known as the "assistance mandate" authorizes CSE to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties. In order for CSE to provide assistance, the requesting agency must have the legal authority to conduct the activity in question, which may require them to obtain a warrant from a court. When providing assistance, CSE is operating under the legal authority of the requesting agency.

Some general examples of the type of assistance CSE can provide include collecting and processing communications, providing linguistic support, or designing technical solutions. In providing assistance, CSE must, first and foremost, comply with all relevant laws of Canada that are applicable to the requesting agency, including the *Privacy Act*, the *Criminal Code*, and the *Canadian Charter of Rights and Freedoms*.

Bill C-51 did not change any of CSE's existing mandate, including the fact that CSE cannot and does not target Canadians or persons in Canada in its foreign signals intelligence or cyber security and information assurance work.

The CSE/CSIS MOU was drafted in order to clearly establish the process and circumstances where CSIS will consult and notify CSE of any threat reduction measures that may impact CSE activities, as well as request assistance from CSE while exercising their lawful authorities.

The MOU in no way expands or enhances existing authorities, and by formalizing-existing processes, will serve to facilitate independent review of CSIS and CSE's respective activities. For these reasons, the memorandum was approved by the responsible Assistant Deputy Ministers and would not have required ministerial level approval or awareness. -

From: [REDACTED]
Sent: Friday, April 7, 2017 9:23 AM
To: 'Baker3, Ryan (PS/SP)'; [REDACTED]
Cc: 'Media Relations / Relations avec les médias (PS/SP)'

000209

Subject: RE: URGENT-- Canada's top spy agencies work out deal on 'threat disruption' operations

Yes, that was what was provided to the reporter last week.

From: Baker3, Ryan (PS/SP) [mailto:ryan.baker3@canada.ca]

Sent: 7-Apr-17 9:10 AM

s.15(1) - Subv

To: [REDACTED]

Cc: Media Relations / Relations avec les médias (PS/SP)

Subject: RE: URGENT-- Canada's top spy agencies work out deal on 'threat disruption' operations

Hi [REDACTED]

I think you can stand down. MO has the following from CSIS.

- While I cannot provide specific details about operational matters, as part of our mandate, under Section 17 of the CSIS Act, CSIS enters into cooperative relationships with domestic partners in the interests of national security. All of CSIS' relationships are undertaken in accordance with the CSIS Act, Ministerial Direction, and robust internal policy.
- As our Director has stated publicly, with respect to warranted threat reduction measures, CSIS has not, to date, used the newly acquired warranted threat reduction measures since the legislation came into effect in June 2015. Therefore, CSE has not provided any warranted threat reduction assistance to CSIS.

Ryan Baker

Director, Public Affairs / Directeur, Affaires publiques

Public Safety Canada / Sécurité publique Canada

Tel: (613) 991-3549

Mobile: (613) 796-9750

Ryan.Baker3@canada.ca

From: Baker3, Ryan (PS/SP)

Sent: Friday, April 07, 2017 9:07 AM

To: [REDACTED]

Cc: Media Relations / Relations avec les médias (PS/SP)

Subject: FW: URGENT-- Canada's top spy agencies work out deal on 'threat disruption' operations

Importance: High

Good morning,

Do you have media lines on this issue? Our MO is in front of the media at 11 a.m. We'd appreciate whatever you have.

Thanks,

Ryan

Ryan Baker

Director, Public Affairs / Directeur, Affaires publiques

Public Safety Canada / Sécurité publique Canada

Tel: (613) 991-3549

Mobile: (613) 796-9750

Ryan.Baker3@canada.ca

published: 2017-04-07

received: 2017-04-07 01:25 (EST)

Toronto Star.com

NEWS | TORONTO STAR, Words: 801

Canada's top spy agencies work out deal on 'threat disruption' operations

by: Alex BoutilierTonda MacCharles

OTTAWA- Canada's two most powerful intelligence agencies have crafted a formal deal to cooperate on using controversial powers to disrupt domestic threats to the country's security, the Star has learned.

Documents obtained by the Star show the spy agency Canadian Security Intelligence Service (CSIS) and the electronic signals-gathering agency Communications Security Establishment (CSE) signed an agreement in July 2016 on how CSE will assist with "threat reduction" activities.

For example, if CSIS were to jam electronic communications, thwart a suspected terrorist's travel plans or financing efforts, or crash a group's or individual's website, it would notify CSE it was intending to act.

The power to actively intervene to disrupt threats to Canadian national security, rather than simply collect information on them, was granted to CSIS in the previous Conservative government's contentious anti-terrorism law, Bill C-51.

The legislation allows CSIS to actively disrupt perceived threats to national security, with few limits to the power except obtaining a warrant. The agreement with CSE allows for the combination of CSIS's expertise in human intelligence and field work with the technical sophistication of Canada's premier electronic intelligence agency.

But while CSIS has already used that new power approximately two dozen times, the Star has learned the agency put a halt to at least some disruption activities since the Liberals took power in November, 2015.

CSIS has the power to collect intelligence on Canadian citizens who are deemed a threat to national security whether they are on Canadian soil or abroad. On the other hand, CSE is explicitly prohibited from directing its electronic intelligence-gathering powers at Canadian citizens; its job is to gather signals intelligence on foreigners deemed a threat.

A senior government source, who spoke on the condition of anonymity, told the Star that CSIS has made the deliberate decision not to pursue more serious threat reduction activities that would require judicial warrants until it is clear what, if any, legislative changes will be made to the agency's powers.

Senior CSIS officials decided it wouldn't be appropriate while Prime Minister Justin Trudeau's government is undertaking a broad national security review. The Liberals promised during the federal campaign to amend C-51, the controversial anti-terrorism law that gave CSIS the new powers, to strengthen protections for Canadians' Charter rights. So far the only change introduced is a bill that, when passed, would create more parliamentary oversight of national security agencies.

Until it is clear what direction the government is taking on the boosted powers granted to CSIS, the source said, the spy agency has adopted a cautious approach.

Meanwhile, a lot of work has gone into setting out how CSE and CSIS would work together on threat reduction.

"Significant work has been done between both organizations (CSIS and CSE) with regard to Bill C-51 and specifically in developing an MoU (memorandum of understanding) for assistance on threat reduction activities," read documents, stamped "top secret" and obtained under access to information law.

000211

Minutes from a June 2016 meeting between senior executives from the two agencies show the deal was signed at that meeting.

A copy of the memorandum of understanding, also released under access law, sets out the rules governing when CSIS has to notify CSE of threat reduction activities, or request the electronic spying agency's help on more technical operations.

The agreement between CSIS and CSE fleshes out how the agencies must coordinate to avoid stepping on each other's toes when CSIS is in the field.

CSIS has signed similar agreements with the RCMP to make sure it doesn't conflict with police operations, and with Global Affairs Canada to ensure the government is aware of any foreign policy or "strategic outcomes" as a result of CSIS flexing its muscle.

The agreement explicitly sets out a CSIS obligation to notify its partner agencies when CSIS plans to disrupt a threat in any way that could potentially affect a CSE investigation.

Under the law, the mandates of the agencies are distinctly different.

However, the memorandum of understanding recognizes there are times when there may be overlap, and seeks to prevent mistakes, said the source.

CSIS must now notify CSE and the RCMP well before acting, and those two agencies are required to give CSIS their perspective - say, whether it would impede an ongoing investigation - "in a timely manner."

The concern, said the source, is that if one agency was not in the loop and happened to be monitoring the same website or the electronic communications on the other end, it could potentially get a misleading picture of the monitored situation or activity.

CSE is empowered to aid CSIS - or law enforcement agencies like the RCMP - with specialized technological support as long as CSIS or the police is acting under its own legal mandate, say with a judicial warrant in hand for the surveillance or disruption.

Sent from my BlackBerry 10 smartphone on the Rogers network.



Public Safety Sécurité publique
Canada Canada

Deputy Minister Sous-ministre

Ottawa, Canada
K1A 0P6

SUBJECT: Minister's Briefing
DATE: Monday, April 10, 2017
LOCATION: 238-S Centre Block

SECRET / Confidence of the Queen's Privy Council
(with attachments)

DATE: **AVR - 7 2017**
 APR - 7 2017

File No.: PS-015943
RDIMS No.: 2192178

MEMORANDUM FOR THE MINISTER

MINISTER'S BRIEFING
MONDAY, APRIL 10, 2017

(Information only)

ISSUE

Attached is the briefing book for your briefing on Monday, April 10, 2017, from 4:00 p.m. to 7:00 p.m.



Malcolm Brown

Enclosure: (1)

Prepared by: Marc Lafrance

Canada

Public Safety
CanadaSécurité publique
Canada**SECRET / Confidence of the Queen's Privy Council (with attachments)**

Minister's Briefing Breffage du ministre

Monday, April 10, 2017 - 4:00 p.m. to 6:30 p.m. / Le lundi 10 avril 2017 - 16h00 à 18h30

Room 238-S, Centre Block / Salle 238-S, Édifice du centre

AGENDA / ORDRE DU JOUR

| ITEM / POINT | SUBJECT / SUJET | PARTICIPANTS | DURATION / DURÉE |
|--------------|-----------------|--|-----------------------------------|
| 1 | | <p>LEAD / RESPONSABLE</p> <p>John Davies <i>Director General, National Security Policy Directorate, NCSB</i></p> <p>Sophie Beecher <i>Director, National Security Policy, NCSB</i></p> <p>OTHERS / AUTRES</p> <p>William Pentney <i>Deputy Minister, Justice</i></p> <p>Normand Wong <i>Counsel, Policy Advisor, Justice</i></p> <p>Michel Coulombe <i>Director, CSIS</i></p> <p>Peter Henschel <i>Deputy Commissioner, Specialized Policing Services RCMP</i></p> | <p>4:00 5:15 (75 min)</p> |
| | | <p>LEAD / RESPONSIBLE</p> <p>John Davies <i>Director General, National Security Policy Directorate, NCSB</i></p> <p>Sophie Beecher <i>Director, National Security Policy, NCSB</i></p> <p>OTHERS / AUTRES</p> <p>William Pentney <i>Deputy Minister, Justice</i></p> <p>Michel Coulombe <i>Director, CSIS</i></p> <p>Debra Robinson <i>Director General, Legal Services, CSIS</i></p> <p>Gilles Michaud <i>Deputy Commissioner, Federal Policing, RCMP</i></p> | <p>5:15 6:30 (75 min)</p> |

TAB 1

TAB A

**Pages 217 to / à 229
are withheld pursuant to sections
sont retenues en vertu des articles**

69(1)(e), 69(1)(g) re (a)

**of the Access to Information
de la Loi sur l'accès à l'information**

TAB B

**Pages 231 to / à 244
are withheld pursuant to sections
sont retenues en vertu des articles**

69(1)(e), 69(1)(g) re (a)

**of the Access to Information
de la Loi sur l'accès à l'information**

**Pages 245 to / à 253
are withheld pursuant to section
sont retenues en vertu de l'article**

69(1)(a)

**of the Access to Information
de la Loi sur l'accès à l'information**

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Tuesday, May 02, 2017 5:19 PM
To: Today's News / Actualités (PS/SP)
Subject: Toronto Star: MPs calling on federal government to boost protection of Canadian civil liberties

MPs calling on federal government to boost protection of Canadian civil liberties

Toronto Star
Tonda MacCharles
2017-05-02

An influential group of Liberal MPs is calling on the Liberal government to give greater protection to Canadian civil liberties in its coming national security overhaul than was promised in its election platform.

Liberal MPs on the Commons standing committee on public safety released a report Tuesday containing 41 recommendations. They urged Prime Minister Justin Trudeau to increase parliamentary, civilian and judicial oversight of national security agencies, to create a new watchdog agency for Canada's border agency, and to dial back extraordinary threat reduction powers given to CSIS by the Conservatives in controversial changes to Canada's anti-terror law under Bill C51.

They want the law to require ministerial approval and prior judicial warrants for any measures that could be perceived as potential violations of the Charter of Rights and Freedoms. But the Liberals would not move to repeal that CSIS power altogether.

Under prime minister Stephen Harper, the Conservatives boosted CSIS' ability to reduce threats even if its agents would breach an individual's rights — say, to free expression, to enter or leave Canada, or to be free of unreasonable search or seizure — with judicial authorization.

CSIS says it hasn't yet used those powers while it awaits the Liberal government's long-promised reforms.

It is not entirely clear how Liberal MPs — nor the Liberal government — want those powers to work.

The MPs say the law enforcement and intelligence gathering functions “have become blurred,” in the words of committee chair Rob Oliphant.

“They should never act in violation of the Charter, there should be no exceptions to that, especially by intelligence or police forces, that's our bottom line,” said Oliphant.

“That said,” he added, “Charter rights are always subject to judicial understanding of what Charter rights embody.”

Liberal MP Nicola Di Iorio said Liberals recognize there will be situations where a timely response would justify extraordinary disruptive measures, for example if CSIS learned a cyber-attack was imminent and “they have to turn off the power.”

“Yes, there are situations that clearly violate the Charter — but there is a grey zone and you need to be in front of a judge who will assess whether it's a violation of the Charter or not.”

Other recommendations say vague definitions in the Criminal Code, such as “terrorist propaganda,” must be clarified, and there must be an obligatory review of all appeals from persons who feel they are wrongly listed on the so-called “no fly” list for air travel.

The Liberals recommended the government not legislate greater “lawful access” for police and intelligence agencies who want to acquire telecom companies' customers' subscriber information, online activities, telephone conversations, and encrypted communications, without further study.

But the Liberals would make it easier to prosecute terror cases by allowing criminal trial judges to review secret information and decide on matters of confidentiality in national security cases, without requiring those questions be put before a separate Federal Court judge.

Oliphant said the message is there "need be no tradeoff between national security and the rights of Canadians. In fact, they both can only be fully realized if they are both fully respected."

The Liberal party holds a majority on the public safety committee, reflective of the government's majority position in Parliament. But if anything, the report had the flavour of an opposition urging the government to action.

Public Safety Minister Ralph Goodale said he wants to review the report, and still hopes to bring his proposals for change sometime in the next seven weeks.

Oliphant said the report is "rooted in our platform commitments" but he defended the decision to call for greater individual protections of privacy rights saying "our role as MPs is not to be stuck in the party platform."

The Conservatives issued a dissenting report that supported the previous government's approach to Bill C51. Public safety critic Tony Clement said he supported the Liberal majority report on matters such as increased oversight for the Canada Border Services Agency, and the creation an office with responsibility to oversee the information-sharing and national security activities of the roughly 17 departments and agencies that have some role in national security.

But Clement and the Conservatives say that the government should not repeal measures that make it easier for police to obtain peace bonds or to preventively arrest terror suspects. He said the Liberal government should leave Bill C51 in place.

He said the CSIS power to disrupt perceived terror threats – even if it violates Canadians' charter rights – is necessary. When it was pointed out those measures have not yet been used, Clement said "well, they haven't been overused either."

The NDP issued a separate report that supported the majority of the Liberal report but said the government should go further and completely repeal Bill C51.

NDP public safety critic Matthew Dubé (Beloeil – Chambly) backed the development of a community strategy to prevent radicalization and the limitation of preventive detention to exceptional circumstances, but said they are "only steps in the right direction."

The NDP wants an end to the current ministerial directive on torture, complete access to classified information for the future parliamentary national security surveillance committee, and an end to criminal code provisions that jeopardize freedom of speech and freedom of the press.

Elizabeth May, Green Party leader, agreed. "I urge the Government to take this report as a floor, not a ceiling, of what is possible in undoing the harms of C-51."

Josh Paterson, head of the BC Civil Liberties Association, supported the call for a dedicated, integrated agency to provide review of national security operations across the whole of the government.

Increased oversight has been recommended by two previous judicial commissions of inquiry – into the Maher Arar affair, and into the Air India bombing.

But Paterson supported the NDP'S call for a full repeal of Bill C-51, and the repeal of the ministerial directive on torture "to ensure that the government can never rely on information obtained through torture or share information that is likely to result in torture."

Sent to: !!INTERNAL; !!INTERNAL 2; RCMP Breaking News; CBSA Breaking News; CSIS Breaking News

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Tuesday, May 02, 2017 2:37 PM
To: Today's News / Actualités (PS/SP)
Subject: Transcript: Liberal members of House of Commons Standing Committee on Public Safety and National Security hold news conference to discuss report Protecting Canadians & Their Rights - A New Road Map for Canada's National Security - 2017-05-02 - 11h30 ET

DATE/DATE:
May 2, 2017 11:30 a.m. ET

LOCATION/ENDROIT:
NPT, OTTAWA, ON

PRINCIPAL(S)/PRINCIPAUX:

Rob Oliphant, Chair, House of Commons Standing Committee on Public Safety and National Security;
Michel Picard, Member, House of Commons Standing Committee on Public Safety and National Security;
Nicola Di Iorio, Member, House of Commons Standing Committee on Public Safety and National Security;
Pam Damoff, Member, House of Commons Standing Committee on Public Safety and National Security;
Sven Spengemann, House of Commons Standing Committee on Public Safety and National Security

SUBJECT/SUJET:

Liberal members of the House of Commons Standing Committee on Public Safety and National Security hold a news conference to discuss the report Protecting Canadians and Their Rights: A New Road Map for Canada's National Security.

Moderator: Hello. Bonjour. Good morning. Welcome to the National Press Theatre. I'm Kristy Kirkup from Canadian Press and I will be chairing this press conference.

Today, we're going to be hearing from Liberal members of the House of Commons Standing Committee on Public Safety and National Security. To start off, we'll be hearing from MP Rob Oliphant as well as from his colleague, Michel Picard. I'll let you guys begin.

Rob Oliphant: Thank you. Merci beaucoup et bienvenue tout le monde.

I want to thank you for joining us today. This morning, I had the honour to table in the House of Commons a report of the Standing Committee on Public Safety and National Security, which is entitled Protecting Canadians and Their Rights: A New Road Map to Canada's National Security. The report includes 41 recommendations, primarily in response to the anti-terrorism laws established by the former Bill C-51, but also in response to evidence and testimony that the committee heard during its study.

This study included the kind of broad coast to coast public consultations and expert witness testimony and solid respectful deliberation among Members of Parliament that we believe should have taken place in the last Parliament but did not when the former Conservative government enacted their Bill C-51.

This report clearly notes that there need be no trade-off between national security and the rights of Canadians. They both may be fully realized and in fact, can only be fully realized if they are both fully respected. Among the 41 recommendations, there are some key ones I want to draw our attention to today and that one of the first things we do is we require all warrants for the Canadian Security Intelligence Service, CSIS, to respect the Canadian Charter of Rights and Freedoms.

We'll be requi-, we are recommending the clarifying of overly vague definitions in the Criminal Code, such as terrorist propaganda to ensure that Canadians are not limited from doing lawful protest. Making changes to the passenger protect

program, or what is often called the no-fly list, making the program more responsive to complaints and more transparent for all Canadians to understand.

Developing a strategy based on, based in communities for the prevention of radicalization to violence, a national strategy but with local engagement, local priorities. And finally, clarifying definitions of the SCISA, the Security of Canada Information Sharing Act, to ensure that Canadians' privacy is always protected.

I want to mention with thanks committee members on both sides of the House, particularly my colleagues who are with me this morning for collegial thoughtful activity, but also for those in the opposition who engaged well in this process. It's obvious that the Conservative members of the committee did not agree with our report and have issued a dissenting opinion. However, we stand firm that there need be no trade-off between liberty and security. Rather, they are bound together, and we as Canadians value that and that is what we heard from Canadians from coast to coast.

The NDP have offered a supplementary opinion saying that they agree with our report, however would go further, which I think indicates that we have struck an important Canadian balance in the middle between those two extremes and are offering Canadians a chance to have the best security possible, as well as ensuring that their rights are protected.

M. Picard.

Michel Picard: Merci. Ce matin, le président du Comité permanent sur la Sécurité publique et la sécurité nationale a déposé en chambre un neuvième rapport intitulé Protéger les Canadiens et leurs droits: une nouvelle feuille de route pour la sécurité nationale du Canada.

L'étude qui a précédé le dépôt de ce rapport a été motivée par un engagement à revoir les dispositions de la loi anti-terroriste, mieux connue sous le numéro C-51. Le comité a tiré profit de nombreux témoignages d'experts, d'académiciens et de citoyens d'un océan à l'autre. Au surplus, les débats entre parlementaires auront aussi contribué à mieux circonscrire les recommandations que nous portons à l'attention du gouvernement. À trait indicatif, le rapport propose que tous les mandats du Service canadien de renseignements en sécurité respectent la charte canadienne des droits et libertés.

Qu'il faille clarifier un certain nombre de définitions apparaissant dans la loi sur les communications d'information ayant trait à la sécurité du Canada, de même que dans le Code criminel, par exemple, celle de la propagande terroriste afin d'éviter que les Canadiens ne soient restreints inutilement dans leur désir de manifester légalement. Que le programme de protection des passagers soit plus transparent, plus compréhensif, notamment en manière de gestion des plaintes, et que le développement d'une stratégie de prévention de la radicalisation menant à la violence tienne compte de la réalité des différentes communautés.

En fait, s'il y avait un seul message à retenir de l'ensemble des travaux du comité, c'est la primauté de la charte, l'importance, le caractère incontournable qu'il faille absolument garder l'assurance de la protection des droits en même temps que celle de la liberté de tous les Canadiens.

Merci.

Moderator: Okay, and we will now proceed with questions. So to start off, Hélène Buzzetti, Le Devoir.

Question: Mr. Oliphant, I've read most of the recommendations in the report, but some of them go quite far. I was wondering if you have any indication by your Liberal government that they're open to embrace those recommendations. Have you had any discussions?

Rob Oliphant: The government saw this report when you saw it. So what I would say is that the, the report and its recommendations are rooted firmly in platform commitments that were made during the election. The Minister obviously came to our committee and outlined the changes that he was making. We encouraged him. And I think that any recommendations that are beyond the platform requirements that we would see as part of what we wanted to do come out of what Canadians have asked for us to do.

And, and they push into areas like the, the no-fly list, Passenger Protect Program, or some information sharing and also some oversight that I think adds some depth to what the party has already said. And I think this is our role as MPs. Our role as MPs is to not be stuck in the party platform, use it as our base and then drive beyond it to reflect what Canadians have been asking us.

Question: So is it a case of, you know, going further in the hope of getting really what you want? Are you going further than what you think the government is prepared to accept or do you think that this will be entirely –?

Rob Oliphant: I think I would speak for all, all our members here today in saying that this isn't a bargaining position. What this is is a thoughtful and we believe Canadian and Liberal approach to the issues of security and freedom, and making sure that privacy rights are protected and to correct the imbalance that came out of Bill C-51, and to do that in a way that Canadians can have the best laws possible.

It's complex, it's 41 recommendations. It touches on many acts, it's a thorough study. We believe it's a study that should have been done in the last Parliament, but it's not a bargaining position. It is very much a thoughtful exercise. It's been done in parallel with the Minister's own public consultations and we haven't had a report yet on that public consultation. I suspect there will be differences, but I suspect there will be more similarities.

Moderator: Tonda MacCharles, Toronto Star.

Question: Hi. Can you clarify – so I've read this section on disruption warrants and the Liberal platform, you know, said what it seems to me to be much the same thing as you're saying, make sure that the warrants for this kind of activity comply with the Charter of Rights, but can you clarify exactly what you want to happen because many of the experts who examined that section and that power say that it's completely upended. It's backwards anyway, because a judge should not be authorizing a violation.

Rob Oliphant: Correct.

Question: So I don't understand what you want to see. How do you think that that power can be made tolerable?

Rob Oliphant: The first we would say, we heard this in, not unanimously, from testimony but overwhelmingly in testimony, was that the McDonald Commission, which actually was used to set up CSIS, made a clear distinction between enforcement and intelligence. Those functions used to be blended and over the years, and the Minister said this at committee as well, those have become blurred, those distinctions. And our first call is to, the government, to step back from that and clarify that the RCMP and other police forces in Canada are enforcers and we have a very important security function being done in the intelligence realm, and those two should not be blurred.

We recognize however that at times, our, CSIS has information that they need to act on in a time sensitive way. What we have said about that, first is they will never act, or should never act, in violation of the Charter. That is our primary goal, there should be no exceptions to that, especially by intelligence or police forces, not, you know, that's our bottom line.

In —

Question: So, so I'm, just so I can understand that, so you're saying that in fact, there shouldn't be judicial warrants allowed for disruptive measures that would violate Charter rights —

Rob Oliphant: Absolutely.

Question: — such, such as, if I could just finish my thought there, so anything like even crashing a website, disrupting someone's travel plans via, you know, their checking in or whatever, that all of that would violate either mobility rights or, or expressive rights. So you're saying that there actually shouldn't be those warrants. That power shouldn't exist in CSIS' hands?

Rob Oliphant: That's right, except Charter rights are always subject to judicial understanding of what Charter rights do have, do embody. What we have said is there are times when things may be against the law, such as break and entry, as some, you know, if anybody in the intelligence area or the police force want to do break and entry, then we're saying two things are required. You need to have a warrant and by judge prior to the activity and also ministerial approval.

So that, that's what we're saying, that there, there are times, we want to make sure that our police and our security forces have all the tools they need, absolutely, so they have that ability, but not to the point of Charter rights being infringed. I'm just going to turn to my colleague, Nicola, and see if you would like to add to that.

Nicola Di Iorio: Power to disrupt is an important power. It has been recognized by witnesses that appeared before the committee. And I'll give you an example: somebody's about to launch a cyber attack that will be extremely detrimental to this country. You obviously want your security forces to be able to disrupt that activity. If they have to turn off the power,

for example. You said something crucial in your question, though, because you said that, you were referring to another example, you said that obviously infringes on the Charter.

What we're advocating is that yes, there are situations that clearly violate the Charter, but what we're saying is that there are situations that are in the grey zone and therefore, you need to be in front of a judge who will assess whether it is a violation of the Charter or not. And if it is not a violation of the Charter, the judge will most likely allow the activity to go on. If the judge comes to the conclusion that it is a violation of the Charter, he puts an end to it. There's no further discussion.

Question: But there would not be judicial authorization for intelligence forces to violate the Charter, even if it means for example, crashing a website. This is the power they have now, right? So you're saying take that power away from them?

Nicola Di Iorio: Well, your question's important because you say even for example, crashing a site. Well, a judge would decide whether crashing a site violates the Charter. That's what we're saying. Instead of deciding ahead of time that everything is permissible regardless, we say we live in a country that is governed by the Charter. This is the principle that we advocate around the world, and this is what we want to serve as an example to the world.

So what we're saying is let's go in front of a judge who's trained to interpret and evaluate, knows how to assess the facts and then we'll determine whether it is permissible or not.

Moderator: Charelle Evelyn, The Wire Report.

Question: I wanted to ask about is recommendation 39, it says you know, it doesn't recommend any changes to the lawful access regime in terms of (inaudible) require subscriber data or, you know, accessing someone's mobile device. This is something that, you know, the Association of Police Chiefs has been asking for, saying it'll make their jobs easier. Why is it that you decided that this is not the way to go?

Pam Damoff: Thank you for that, and you're correct. We did hear from the police chiefs advocating for further powers, but we also heard from witnesses who referenced the Spencer Decision and said that they already have the power to do that. They just have to get a warrant. And so we're saying that it's important that they do get that warrant and we're not, we're not recommending that they, the power be expanded.

Rob Oliphant: I might just add to that that overwhelmingly, we recognize that we need to do a 21st century study on cyber security, that these are, you know, we have three recommendations around that area, however, that was not broadly the scope of this study. We heard testimony, we made some recommendations, but more work needs to be done in that area because it's, it is maybe perhaps one of the more constantly evolving issues that we need to take time on.

Question: If I could follow up, from my, maybe I understood it incorrectly, my understanding is that they were asking for, to be able to compel people to give, say, their passwords, for devices seized under a warrant. So you're saying even if, so they, as far as I understand, they don't currently have that, so they can get the devices under the warrant but they can't make you open it. So that, so that they don't currently have that power, so why, why wouldn't you want to give them?

Rob Oliphant: We are arguing that right now, they have sufficient power within the current law not to have more, open however to more study. We needed more time on that issue. But at this time, we're recommending no changes to the regime as it stands. The argument was made. It wasn't yet compelling, but we're also open to the fact that we learn every day. And so we do need to study that more further, further.

Moderator: Omar Sachedina, CTV.

Question: Hi. Some of the issues that you've highlighted in the report have, have already been talked about and addressed at length. I'm thinking of, you know, potential examples of overreach having to do with C-51 and beg definitions. Throughout these consultations, is there anything that, that surprised even you that had not been addressed in the public domain before, that you sort of sat back and said that's not something that has been discussed or not even something that we had thought of previously?

Unidentified Male: We thought —

Unidentified Male: I think, if I, if I (inaudible) —

Unidentified Male: Apart the no-fly list, one thing that I learned, I'm going to share with you, no-fly list, we always look at it as a Canadian problem. What we don't realize when we think about no-fly is that we border the United States and our

flights have to fly over that country. So if you go from Toronto to Vancouver, you will be flying over US territory. And therefore, the US has a legitimate right, a sovereign right to determine who's going to be flying over its territory.

So sometimes people are denied access to flying, not because they're on the Canadian no-fly list, it's cause they're on the American no-fly list. That's something that I discovered. I always believed that if they were denied on Canadian soil, it was because it was a Canadian no-fly list. I discovered that it could be because of the US no-fly list.

Michel Picard: Since it goes beyond what was the Liberal Party engagement and the platform, we went much further than just initial engagement and focus on (inaudible) went far. The only idea of reconsidering what is the real threat, the level of threat, so we can assess that correctly brought us to make sure that we asked the right question and get the right level and make proper recommendation, not based on what is already recommended by CSIS, other organization and they, they, it's not surprises as making sure that we were going to the limit of what we can ask and get to the, what can be covered in order to make sure that we go as far as we could.

So it's not rather surprises then make sure that the report brings to the attention of the government a much wider range of concerns that what it was engaged at the first time, in the first place.

Sven Spengemann: If I can just add, this is an excellent question. I think there's a, there were thought processes out there that were in the public realm, but this exercise really sharpened them and brought them to light. And one of them is the importance of public trust in government as being fundamental to specifically this undertaking to, to improve our security but also to uphold our Charter values. It's really the sense that we have to do both, that there aren't any trade-offs and also that we need to be inclusive of communities across our country.

In fact, Ihsaan Garde, who's the Executive Director of the National Council of Canadian Muslims, said that inclusion is a key component of public safety, the inclusiveness that everybody has to have a stake in these two ambitions, which is to safeguard our Charter values and to deliver the most effective possible security across the country. I think this, this really sharpened that view that we thought was out there, but witness after witness agreed with this proposition.

Pam Damoff: Just to say I think what surprised me was also around the Passenger Protect or no-fly list. I have a young man in my riding who's on, whose name is on that list and I think it's important to distinguish between whether it's the person or the name and it's his name that's on the list, that the previous government, for 10 years, didn't do anything to put in place a system that would – in the States, United States, they have the redress system.

We didn't have anything designed in Canada to allow people to get a redress number like they have in the States. And the fact that that went on for the last 10 years, and that's why we're recommending that we do put in place a redress system so that people like this young man can apply and get a number that does allow him to fly and have his, that individual have a much easier time flying, which is in place in the United States and nothing was done here for 10 years, to put in place a system that they can get redress if their name is on that list.

Rob Oliphant: I might add to my general feeling on this topic was that I believe this is a modest report and it's modest in that we start out very early saying what we don't know. And our response as the majority on the committee is to say when we don't know something, we want to learn more. And so the first couple of recommendations around getting that threat assessment report out there and to do more research and develop more capacity in these broad areas.

Our response is not knee-jerk to close down society because we don't know things. It's not to, to stop citizens' rights and privacy because of lack of knowledge. Instead, we reach out, we reach out to marginalized communities, reach out to those who may be excluded because of racism or sexism or other issues. We reach out to bring people in and study. And that's not a passive kind of activity. It's a real activity to say we don't know enough. We need more expertise, more money for research and more transparency around what the real threats are to Canada. And then through that, we'll be guarding rights, protecting them and making sure we have a safe country.

That, that actually felt good that I thought we, as a country, knew more, and we actually need to know more.

Moderator: (inaudible)

Question: What happens next? I mean, some of the issues, like C-51, it was a flashpoint during, during the campaign. A lot of Canadians, you know, if you bring it down, this report for the average Canadian, you know, who want, who want action on this, they've been waiting for action on some of these things, what do you tell them and who might just fear that this is just another report and now, it'll be up to the government to decide what to do?

Michel Picard: Such an easy question. Thank you. I'll start in French and I'll do it in English, because it's a very, that's the point of the whole thing.

Quarante-et-une recommandations sur un sujet que le gouvernement antérieur avait dit il y a rien à refaire sur ce qu'on a fait dans C-51. L'ancien gouvernement prétend que C-51 est correct, adéquat, parfait, il y a rien à refaire. Les gens ont démontré au-delà des engagements du parti Libéral en campagne, au-delà que quelque attente que ce soit, ont démontré la grande quantité de modifications, des points sur lesquels il fallait apporter une attention particulière pour justement améliorer ce qui vraisemblablement faisait défaut.

Alors, toute prétention à l'effet que le système d'avant était adéquat, nous on ne fait que rapporter ce que les gens ont conclu à l'effet que non, voici ce dont nous avons besoin.

It's an obvious, we have to realize that what has been done in the past is clearly not sufficient based on the fact that we ended up with 41 recommendations. If C-51 was right on, we wouldn't need those, that many recommendations. People have, have said, talked, explained, shared, exchanged their concern because we needed those modifications. We just put that together. As Sven said, we sharpened everyone's opinion to have a clear picture of what is needed for us, then to send it to the government's attention.

So any, anyone who pretends that what was in the past was fine maybe is missing some part of it.

Rob Oliphant: I might add on that that the government has an agenda on this issue. They're working, government moves slowly. We as parliamentarians are out there in our ridings. We're hearing this issue and so we did the study to, to push, to absolutely push on behalf of the people we represent. So that, that's a purpose of the study. We're, there is no lack of confidence in what the government is doing. What we're saying is more.

So we're strongly supportive of Bill C-22, and the oversight measure of putting in a committee of parliamentarians and we're also then saying that's a great start. We also want independent oversight of CBSA, the Canada Border Services Agency. We also want oversight of the 17 agencies that have some intelligence security aspects to them that don't have oversight. We're looking for that. And we're looking at a legislative gateway that looks at all the agencies and makes sure that they're able to do joint studies together and it's the appropriate amount of, of information sharing. And we're also encouraging government – this is a political part – to say you need to resource, fund, support those agencies commensurate with the expanded activities.

So if you have an RCMP, or a CSIS or a CBSA or a Security, Communications Security Establishment, if you have those bodies that have broader mandates and more people working there, you need to up the oversight and that relates, I think, to what Mr. Spengemann has said about confidence and trust. Oversight and review are good for the agencies. We're just asking for more.

Moderator: (off microphone) we're just going to go Hélène, and who has second round of questioning, so Hélène first and then (inaudible).

Question: Okay, I just want to go back to this oversight thing, because recommendation number 10, I believe, proposed the creation of a overseeing body of oversight, kind of thing, but where you also recommend to have more bridge between the oversight mechanism. So I just want to know is that, is that contra-, not contradictory but is that a duplication? How, why do you need both?

Rob Oliphant: We don't think so. We think that there's one thing that is a statutory gateway which requires and facilitates the conversation appropriately between oversight agencies so they don't duplicate work. So we don't end up having to have an O'Connor or a Iacobucci inquiry or commission. We don't want to do that. We think that it should be integrated into the system so that's a statutory function.

We're also suggesting that there be an office, a national security review office – I would have put it in capital letters – (laughter) that, that is responsible for the appropriate integration of that activity and also those other agencies which don't have as their principal mandate national security but have, Transport Canada has some security function. There's many parts of government, there are 17 bodies that have some aspect. You're not going to set up a whole body for them, but you set up an office that, that monitors them.

And, and we got into the difference between review and oversight. Most of what we're talking about is review, looking at past activities in that office; in the bigger agencies, we're looking for oversight that is real time.

Question: So as a supplementary, I just wanted to go back to Tonda's questions about the, voyons, perturbations, —

Michel Picard: Disruption?

Question: — disruption, thank you – the disruption powers, so correct me if I'm wrong, what you're saying is that because now currently, and correct me if I'm wrong, I believe you need a mandate from a judge only if what you're about to do is contrary to the Charter. Right? And now what you're saying is that you want to go in front of a judge for every case of disruption and if the disruption is contrary to the Charter, it will be refused. Did I get this right?

Michel Picard: Correct. But there is no other way. I mean, if we say that there can no longer be the power to disrupt, if there's a violation of the Charter, it does imply that you have to go in front of a judge every time because otherwise, you'd be judge and party. You would be deciding well, it doesn't violate the Charter, you know, we're just going to be, you know, doing this horrible thing, but we don't feel it's violating the Charter.

What I want to stress is that, you know, the fact that you put in legislation as it was in C-51, that you can violate the Charter, what you're basically doing is you're leaving your citizens at the mercy of individuals who have maybe other priorities on a given day, and you know, what we always have to be mindful and remind the Canadian people is that when you give a power like that, it's not necessarily used against the bad guys. It could be used against the good guys or mistakenly perceived as bad guys.

And then you wind up in a situation where you damage the Canadian brand because people look at this and list what kind of situations we have in those countries and then you have a mega investigation going on as to why this happened and why did we (inaudible) that situation? Well, we can see it with C-51.

Pam Damoff: Could I just add to that? I think it's important to remember that we take security very seriously. But there was an example that was given when we were hearing testimony of surveillance and how people want to make sure that they're protected, but the idea of having a camera in their house that would monitor their home 24/7 where someone was watching just in case there was ever a break-in is not something that people would be comfortable with.

So it was, it struck home with me that example of, of yes, we want to make sure that we're safe, but would I be prepared to have a camera in my home 24/7 monitoring me? No I wouldn't. So I think, you know, that was a very concrete example of where it would be going too far, in my opinion. So I think, you know, we need to be mindful that we do take security very seriously, but we need to be also cognizant of the privacy of individuals.

Unidentified Male: I think just to go back to your question about the range of 41 recommendations, some of them are complex or governance related, some of them are very simple. Like the Security Infrastructure Program, for example. It's an existing program, and we had faith leaders come up to us through this process and in our communities as well, to say we have congregations from, from a range of different communities who are now fearful to exercise their faith in their places of worship.

So this program was up and running, it was being used and the simple reflex for us was to say we should, we should do more. We should fund it more and we should make sure that communities are aware of the parameters of this program, which basically allows them to install perimeter security even inside the places of worship as well, cameras, fencing, and ID checks and those, those kinds of things, right? So some, some recommendations exist. They're part of the basket and we're simply saying we need to ratchet up and to respond to the rather fluid and changing security environment that we're in.

Moderator: Are there any other questions? This conclu-, oh.

Rob Oliphant: I was just going to say thank you for this and to publicly again thank my colleagues for their, their work. This is obviously a passionate issue for many Canadians and it's been borne out in the passionate work of the committee members.

Question: (off microphone) (laughter) minority dissenting report by the NDP —

Rob Oliphant: A supplementary report.

Question: A supplementary report, you're right, you said that you're somewhere between the two extremes, but I was, I was wondering why you use that word since the NDP maybe does not go as far to its extreme than the Conservatives do. So can you just (off microphone)?

Rob Oliphant: I think in their first recommendation in their supplementary opinion, they call for a repeal of all acts affected or touched by C-51, and we don't think that's a responsible way of approaching it. That would be the difference. I mean, they're in agreement and accord with our report except they would then repeal all of it, and we're saying no, the safety and security of Canadians is entrusted to, to parts of those acts and we want to make sure that their rights are also equally recognized in that process, no trade-off.

So we just don't believe that that's a responsible way of governing. We think the responsible way is to actually do the hard work of the 41 recommendations. They're not all easy to get into, but it is, yeah, in some ways it's simpler, you know, to just repeal. That's not what we're about, so we would not go to that extreme.

Michel Picard: La qualité des témoignages que nous avons reçus a démontré une approche relativement raisonnable de l'ensemble des témoins. Rien d'extrême. L'équilibre que Mme Damoff a parlé au niveau de la liberté des droits a été retrouvé dans la plupart des témoignages. Donc, si l'ensemble des Canadiens qui s'expriment pour emmener ce genre de rapport suggèrent une approche raisonnable équilibrée, mais probablement que ceux qui avaient des vues extrêmes, comme notamment le NPD a changé un peu son approche en réalisant que finalement, d'ailleurs quelques-unes de leurs recommandations font aussi partie du lot, finalement l'approche raisonnable plus équilibrée s'avère plus représentative de la volonté des Canadiens.

Rob Oliphant: And lastly and not only because I think they're watching, but to thank our Clerk, Jean-Marie and our analysts and our staff that did hard work. This was a long study and it was a demanding study, so I want to make sure that out there, they know that they are thanked.

Moderator: Thank you very much.

Michel Picard: Oui effectivement, nos pensées vont à toutes ces personnes qui nous ont soutenus tout au cours de cette démarche. C'est un travail très exigeant, très rigoureux qui demande une attention à une foule de détails, et ils étaient toujours présents, toujours disponibles, toujours attentionnés et certainement dévoués et très travaillants. Alors on les remercie pour tous ces beaux efforts.

Moderator: Thank you.

-30-

NOTE: TRANSCRIPTS CANNOT BE SHARED OR TRANSFERRED OUTSIDE OF YOUR DEPARTMENT WITHOUT THE CONSENT OF MEDIA Q INC.

*Questions? Please contact us at ps.pspmediacentre-centredesmediaspsp.sp@canada.ca
Questions ? Veuillez communiquer avec nous au ps.pspmediacentre-centredesmediaspsp.sp@canada.ca*

Sent to: !!INTERNAL; !!INTERNAL 2; CBSA Breaking News; RCMP Breaking News

Today's News / Actualités
May 4, 2017 / le 4 mai 2017
08:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 08h00 et 14h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / LES FEMMES ET LES FILLES
AUTOCHTONES DISPARUES ET ASSASSINEES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

RCMP eyes expanded media protections amid police surveillance concerns

Newly disclosed documents say the RCMP is eyeing a policy change for organized crime probes to better protect the rights of journalists. The possible move follows revelations in Quebec about surveillance of reporters by provincial and municipal police. Under a 2003 federal directive, the RCMP must take special care in national security investigations involving sensitive spheres such as the media, politics, academia, religion and unions. Internal RCMP notes say the Mounties are looking at applying the directive to all of the police force's federal investigations, including those involving organized crime. The Canadian Press recently obtained the November 2016 notes through the Access to Information Act. RCMP spokesman Harold Pfeleiderer says the force has nothing to add at this time, and a **spokesman for the public safety minister** says a review of the federal directive is ongoing. [Canadian Press](#) (CTV News)

est à 1 kilomètre de la rivière des Outaouais, et des organisations locales craignent non seulement pour la rivière, mais également pour le fleuve. [Le Devoir](#); [iPolitics](#)

Nanaimo Search and Rescue twice as busy in 2017

Nanaimo Search and Rescue volunteers have been twice as busy in 2017... Emergency Management B.C. covers most costs for vehicle fuel, repairs and other expenses incurred in searches, which are most often called for by the RCMP, B.C. Ambulance Service or B.C. Coroners Service. [Nanaimo News Bulletin](#)

[BACK TO TOP / HAUT DE LA PAGE](#)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

China condemns news about Chinese journalists spying in Canada

The Chinese Embassy in Canada has strongly condemned a report by a Montreal-based newspaper in which it claims that intelligence services has been tracking some Chinese journalists in Canada over suspicions of espionage. Yang Yundong, spokesperson for the Chinese Embassy, said that such fabricated news mislead Canadian people and undermine ties between China and Canada. La Presse, a French-language daily newspaper, published an article on May 1 titled "Des journalistes ou des espions chinois à Ottawa?" (Chinese journalists or spies in Ottawa?), in which it claims that the Canadian Security Intelligence Service has been keeping tabs on a certain number of Chinese correspondents from Xinhua news agency and People's Daily in Canada. The author, Joel-Denis Bellavance, argued that these journalists have been collecting information for the Chinese government, taking advantage of their privileged access to high-profile meetings in Canada. He backed his allegation with quotes from unnamed sources, which he claimed have worked with former Prime Minister Steven Harper or are in the higher ranks of the intelligence services in the country. "We have noticed a few days ago that La Presse reported about resident Chinese journalists in Canada committing espionage against Canada. We are shocked by and strongly condemn the despicable action of fabricating lies," Yang said. Yang stressed that Chinese journalists in recent years have positively reported stories about Canada's politics, economy, society and culture, enhancing Chinese people's understanding and knowledge of Canada and fostering friendly sentiments toward Canadian people. [Chinese News Service](#)

Don't change lawful access rules, Parliamentary committee recommends

Liberal-dominated parliamentary committee says the government shouldn't change the current lawful access regime that limits the ability of police to get at telecom subscriber information and encrypted data unless they have a warrant. The recommendation came this week from the House of Commons' public safety and national security committee as part of a broad review of the country's national security framework. Last year the Trudeau government launched a public consultation into federal national security policy, which included the parliamentary committee's work. The government hasn't given an indication yet of when a new policy will be issued. Today a spokesperson for the Canadian Wireless Telecommunications Association (CTWA) which represents most of the country's wireless carriers, said the group had no comment on the committee's recommendations because government policy hasn't changed. The parliamentary committee also made other national-security related recommendations including increasing the funding of all public safety and national security review bodies, limiting the powers of the Canadian Security and Intelligence Service (CSIS) and more oversight over federal national security bodies. [IT World Canada](#)

[BACK TO TOP / HAUT DE LA PAGE](#)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Niagara man arrested at the Rainbow Bridge

A Niagara man faces charges after U.S. Customs and Border Protection officers discovered more than 11 pounds of marijuana in a vehicle at the Rainbow Bridge. According to the CBP, a motorist crossed the bridge into the U.S. on Tuesday and was referred for a secondary inspection. Authorities searched the



SECRET / Confidence of the Queen's Privy Council (with attachments)

**Minister's Briefing
Breffage du ministre**

Friday, May 5, 2017 - 1:15 p.m. to 4:00 p.m. / Le vendredi 5 mai 2017 - 13h15 à 16h00

Minister's Boardroom / Salle de conférence du ministre

AGENDA / ORDRE DU JOUR

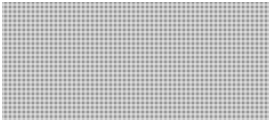
s.15(1) - Subv
s.23
s.24(1)
s.69(1)(g) re (a)
s.69(1)(g) re (e)

| ITEM / POINT | SUBJECT / SUJET | PARTICIPANTS | DURATION / DURÉE |
|--------------|---------------------------------------|--|-----------------------------------|
| | Flooding in Ontario and Quebec | <p><u>LEAD / RESPONSIBLE</u></p> <p>Stéphanie Durand <i>A/Assistant Deputy Minister, EMPB</i></p> <p>Mario Boily <i>A/Director General, Government Operations Centre, EMPB</i></p> | <p>1:15 1:30 (15 min)</p> |
| 1 | [REDACTED] | <p><u>LEAD / RESPONSIBLE</u></p> <p>Kathy Thompson <i>Assistant Deputy Minister, CSCCB</i></p> <p>Angela Connidis <i>Director General: Crime Prevention, Corrections and Criminal Justice Directorate, CSCCB</i></p> <p>Karl Hanson <i>Senior Research Scientist, CSCCB</i></p> <p><u>OTHERS / AUTRES</u></p> <p>Talal Dakalbab <i>Executive Director General, PBC</i></p> <p>Peter Henschel <i>Deputy Commissioner RCMP</i></p> <p>Jamie Tomlinson <i>Director General, Communications, PACB</i></p> | <p>1:30 2:00 (30 min)</p> |
| 2 | [REDACTED] | <p><u>LEAD / RESPONSIBLE</u></p> <p>Donald Piragoff <i>Senior Assistant Deputy Minister, Policy Sector, Justice</i></p> <p>Elisabeth Eid <i>Assistant Deputy Minister, Public, Defence and Immigration Portfolio, Justice</i></p> <p>Doug Breithaupt <i>Director and General Counsel, Criminal Law Policy Section, Justice</i></p> <p><u>OTHERS / AUTRES</u></p> <p>[REDACTED] <i>Director General, Policy and Foreign Relations, CSIS</i></p> <p>John Davies <i>Director General, National Security Policy Directorate, NCSB</i></p> <p>Sophie Beecher <i>Director, National Security Policy Directorate, NCSB</i></p> <p>Jamie Tomlinson <i>Director General, Communications, PACB</i></p> | <p>2:00 2:45 (45 min)</p> |

s.15(1) - Subv
s.24(1)

s.69(1)(g) re (a)
s.69(1)(g) re (e)

3a



LEAD / RESPONSABLE

Monik Beauregard
Senior Assistant Deputy Minister, NCSB

John Davies
Director General, National Security Policy Directorate, NCSB

Sophie Beecher
Director, National Security Policy Directorate, NCSB

OTHERS / AUTRES

Donald Piragoff
Senior Assistant Deputy Minister, Policy Sector, Justice

Elisabeth Eid
Assistant Deputy Minister, Public, Defence and Immigration Portfolio, Justice

Karen Audcent
Senior Counsel, Criminal Law Policy Section, Justice



Director General, Policy and Foreign Relations, CSIS

Peter Henschel
Deputy Commissioner, RCMP

Jamie Tomlinson
Director General, Communications, PACB

3b



LEAD / RESPONSABLE

Monik Beauregard
Senior Assistant Deputy Minister, NCSB

John Davies
Director General National Security Policy Directorate, NCSB

Sophie Beecher
Director, National Security Policy Directorate, NCSB

OTHERS / AUTRES

Jamie Tomlinson
Director General, Communications, PACB

2:45
3:30
(45 min)

3:30
4:00
(30 min)

UNCLASSIFIED



GOVERNMENT OPERATIONS CENTRE

CENTRE DES OPÉRATIONS DU GOUVERNEMENT

Senior Level Brief

2017 Quebec and Ontario Flooding (00693-17 and 00692-17)

As of 11:30 EDT on 05 May, 2017

DATE: 05 May, 2017
RDIMS No.: 2227165



Government
of Canada

Gouvernement
du Canada

Canada

Background

GOVERNMENT OPERATIONS CENTRE

UI CLASSIFIED

Areas of Concern: Eastern Canada, including Quebec, Ontario and New Brunswick

- Localized spring flooding has been occurring in Ontario, Quebec and New-Brunswick as a result of a wet spring.
- A weather system carrying high levels of moisture coming at a time where water levels are high and soils are saturated or close to saturation.
- In eastern Quebec, forecasted rain will add to the significant runoff resulting from the melting of the snowpack which is 2 to 3 times superior to the normal this year.



Government
of Canada

Gouvernement
du Canada

RIN/S No.:

Current Weather Situation

GOVERNMENT OPERATIONS CENTRE

UNCLASSIFIED

- A storm is moving from the southern United States toward eastern Ontario, southern Quebec and the Atlantic provinces.
- The storm will bring two bands of heavy rains and moderate to high winds.
- The first band of rain reached Ontario on May 4 and will reach Quebec on May 5. It will bring:
 - 40 to 80 mm of precipitation in southern Ontario and up to 100 mm locally (over a 72 hour period);
 - 30 mm to 60 mm of precipitation in Quebec.
- The second band of rain should reach the Maritimes and eastern Quebec (Gaspé Peninsula) on May 6 and bring 50 to 100 mm of precipitation.



Total Cumulative Precipitation – May 8, 2017

GOVERNMENT OPERATIONS CENTRE

UNCLASSIFIED

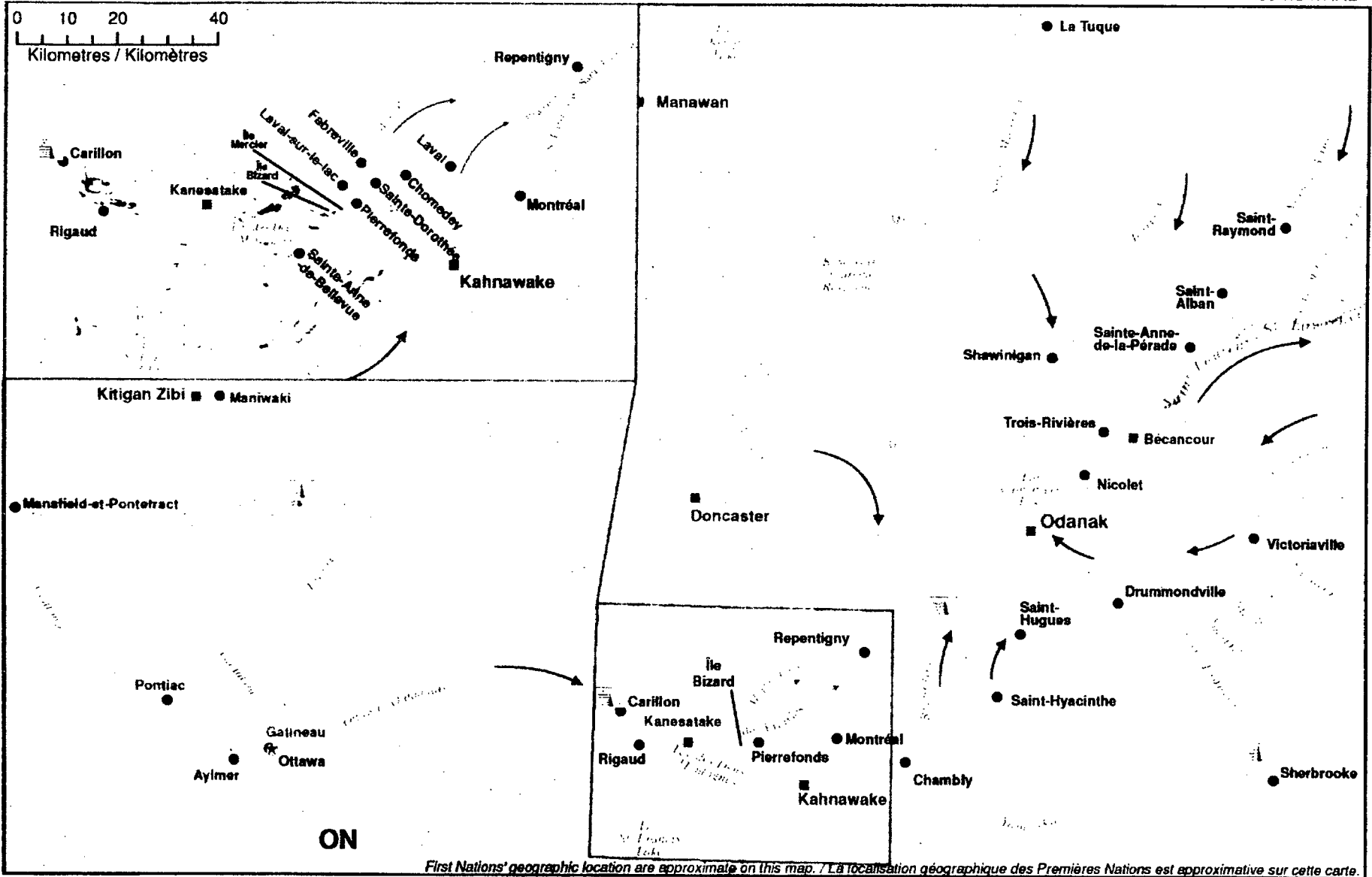


Government
of Canada

Gouvernement
du Canada

Flooding in Quebec / Inondations au Québec

Current as of / Mise à jour
05 May / mai 2017
11:00 EDT/HAÉ



- Town Affected / Ville affecté
- Town / Ville
- First Nations
Premières Nations

- ☞ Flood Extent / Étendue d'inondation
- Flood-control Dam / Barrage pour la protection contre les crues

- Highway / Autoroute
- River / Rivière
- River flow direction
Direction de l'écoulement



Canada

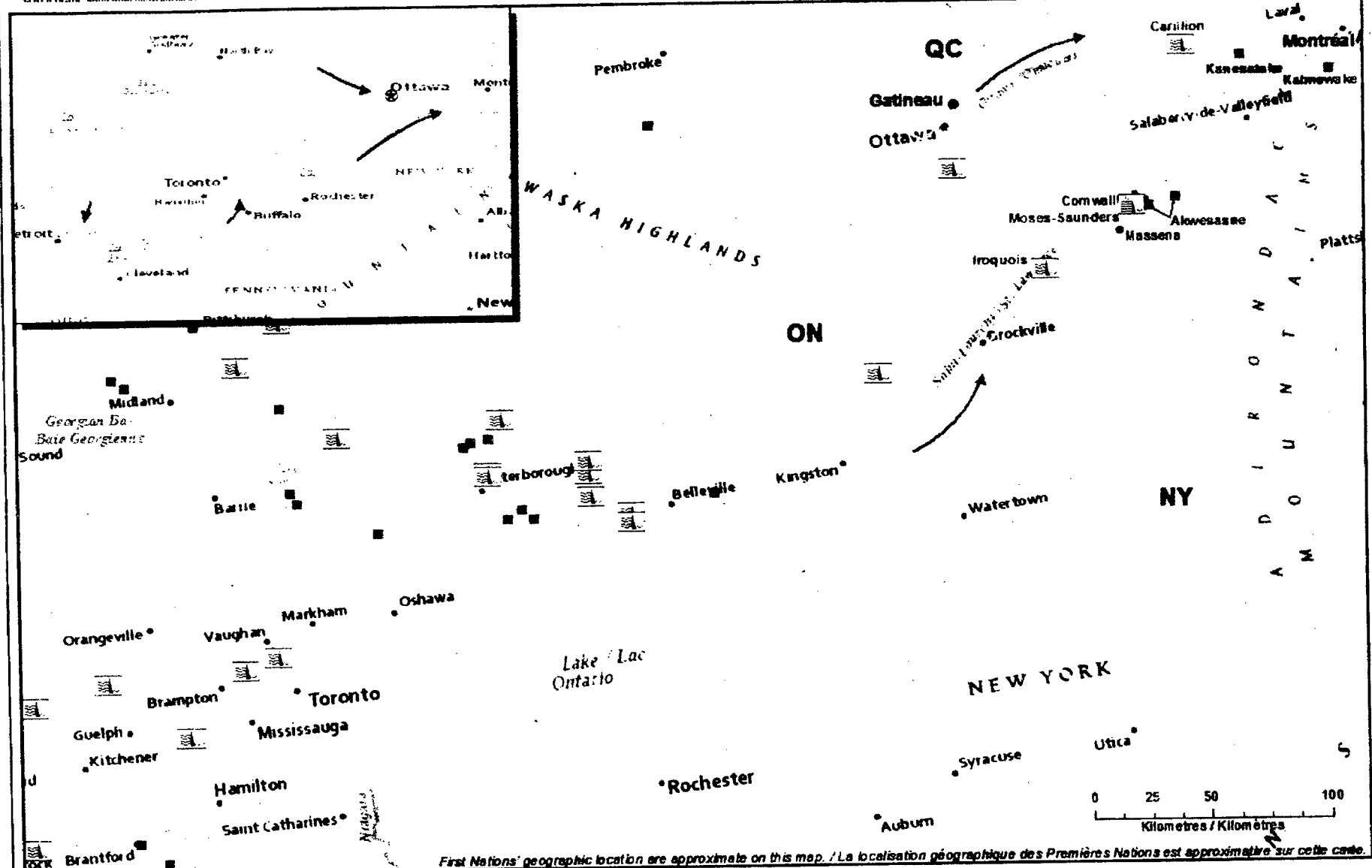
Map data sources / Sources des données:
GOC-COG, INAC / AANC, EGS / SGU,
NRCan / RNCan, DMTI Spatial

GOCC COG
 GOVERNMENT OPERATIONS CENTRE
 CENTRE D'OPÉRATIONS GOUVERNEMENTALES

00963-17

Current as of / Mise à jour
 05 May / mai 2017
 11 00 EDT/HAE

Water systems in Ontario / Réseau hydrographique en Ontario



First Nations' geographic location are approximate on this map. / La localisation géographique des Premières Nations est approximative sur cette carte.

Canada

Map data sources / Sources des données
 300-CDS / CAC AAND DIT 50114 ESR

RE

Assessment and Impacts – Quebec

GOVERNMENT OPERATIONS CENTRE

UNCLASSIFIED

- The municipalities downstream from the Carillon Dam are most at-risk from flooding (i.e. Rigaud, Pierrefond, Kanesatake) .
- Across the Province, the regions of Montréal, Outaouais, Laurentides, Lanaudière, Montérégie, Mauricie and the Gaspé Peninsula will be closely monitored for flooding on the following waterways: the St-Lawrence River, Saint-Louis lake, Deux-Montagnes lake, Saint-Pierre lake, as well as the Ottawa, Mille Îles, des Prairies and Saint-Maurice Rivers.
- It is expected that rainfall will occur over the weekend, from Friday to Monday.

Assessment and Impacts - Ontario

GOVERNMENT OPERATIONS CENTRE

- Impacts are expected for the following watersheds: Lake Huron, Lake Erie, Lake Ontario, Ottawa River and St. Lawrence River.
- High winds and high water levels may generate storm surges and wave generated erosion, on Lake Ontario and Lake Erie.
- There have been no reports of critical infrastructure sector damages to power, transportation, or telecommunications networks.
- The City of Toronto is preparing for a possible evacuation of Toronto Island due Lake Ontario's high water levels.
- This event will likely bring impacts to transportation in the Greater Toronto Area:
 - Toronto Pearson International Airport: consulting with its major customers to restrict the number of flights through the airport.
 - Billy Bishop Island Airport: no flooding has been reported in the terminal or tunnel. The water levels are being closely monitored and pumps and sweepers are on standby should the water levels rise.



Provincial Preparedness

GOVERNMENT OPERATIONS CENTRE

UI CLASSIFIÉ D

Quebec

- The Province's Centre des opérations gouvernementales is closely monitoring the situation.
- The Sécurité Civile du Québec's decision centre was relocated to Montreal.
- A press conference is expected in the afternoon of May 5 to provide a flooding update.
- A request for federal assistance is likely

Ontario

- Toronto is currently managing the event without any anticipated request for assistance to the Province.
- The Provincial Emergency Operations Centre is tracking the weather system and has been in contact with affected and potentially impacted communities.
- Municipalities continue to conduct assessments regarding actual and potential risks.
- Several communities have started to prepare, including the distribution of sandbags.



Federal Preparedness

GOVERNMENT OPERATIONS CENTRE

UNCLASSIFIED

Government Operations Centre (GOC)

- Event Team Stood up at Level 3 (Federal Coordination).
- Reached out and established initial communications with key Federal / Provincial partners in Ontario and Quebec.
- Deployment of Subject Matter Experts and Liaison Officers is being requested from key federal departments and the Canadian Red Cross.
- Requests for Information are being sent to federal partners in preparation for potential requests for federal assistance.

Public Safety Regional Offices

- Quebec and Nunavut Regional Office has activated its regional response plan.
- Ontario Regional Office has not yet been activated.

Federal Preparedness (Continued)

GOVERNMENT OPERATIONS CENTRE

UNCLASSIFIED

Innovation Science and Economic Development (ISED)

- On May 03, the Quebec Regional Office has activated le *Plan régional de télécommunications d'urgence* to level 1 (monitoring).

Environment and Climate Change Canada (ECCC)

- Providing engineering support to estimate releases at Moses-Saunders Dam in Cornwall, including forecasting Lake Ontario and St. Lawrence water levels.
- Overseeing the operation of the Ottawa River Regulation.
- Regional and national teams have been liaising and providing data and modeling information.
- Monitoring and providing information on water flows and engineering advice for both the Great Lakes-St Lawrence and the Ottawa River to decision makers.

Natural Resources Canada (NR Can)

- Will be providing emergency Geomatics services over the weekend and analyzing satellite imagery to extract flooding extents.



Weather Outlook and Assessment

GOVERNMENT OPERATIONS CENTRE

UNCLASSIFIED

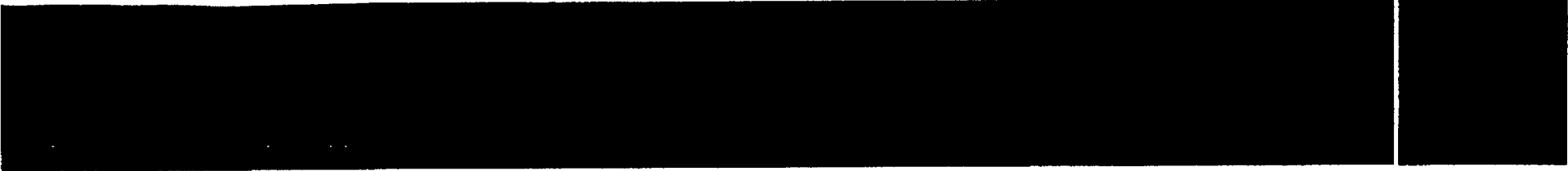
Next week

- Southern Ontario and western Quebec outlook:
 - Temperatures are expected to be below or around normal with scattered and intermittent showers.
- Starting May 7 and early the following week, there could be significant runoff around Manicouagan, Quebec.

Assessment

- Next week's weather system should lead to stabilizing or decreasing water levels, with the exception of the Manicouagan area.





GOVERNMENT OPERATIONS CENTRE

CLASSIFICATION



Government
of Canada

Gouvernement
du Canada

REF ID: A111111

TAB 1

**Pages 282 to / à 291
are withheld pursuant to sections
sont retenues en vertu des articles**

69(1)(e), 69(1)(g) re (a)

**of the Access to Information
de la Loi sur l'accès à l'information**

TAB 2

**Pages 293 to / à 309
are withheld pursuant to section
sont retenues en vertu de l'article**

23

**of the Access to Information
de la Loi sur l'accès à l'information**

TAB 3

Tab A

**Pages 312 to / à 330
are withheld pursuant to sections
sont retenues en vertu des articles**

69(1)(e), 69(1)(g) re (a)

**of the Access to Information
de la Loi sur l'accès à l'information**

Tab B

**Pages 332 to / à 342
are withheld pursuant to sections
sont retenues en vertu des articles**

69(1)(e), 69(1)(g) re (a)

**of the Access to Information
de la Loi sur l'accès à l'information**

Daily Media Summary / Revue de presse quotidienne
Canadian Security Intelligence Service / Service canadien du renseignement de sécurité
May 5, 2017 / le 5 mai 2017

CSIS IN THE NEWS / LE SCRS DANS LES NOUVELLES

MINISTER / MINISTRE

SECURITY AND LAW ENFORCEMENT / SÉCURITÉ ET EXÉCUTION DE LA LOI

BORDER ISSUES / ENJEUX FRONTALIERS

CYBER AND TECHNOLOGY / CYBER ET TECHNOLOGIE

MILITARY ISSUES / ENJEUX MILITAIRES

PUBLIC SERVICE / FONCTION PUBLIQUE

LEGISLATION AND POLICIES / LÉGISLATION ET POLITIQUES

OTHER / AUTRES

INTERNATIONAL / INTERNATIONAL

CSIS IN THE NEWS / LE SCRS DANS LES NOUVELLES

The Gargoyle: Spies, scribes and the French election

True to its budget promise to create jobs, the federal government is on a hiring spree – specifically for spooks, border cops and code-crackers. Recruiters will be hanging out Thursday at a job fair in the Toronto area looking for those interested in joining: The Canadian Security Intelligence Service (CSIS) Royal Canadian Mounted Police (RCMP); Canada Border Service Agency (CBSA); Correctional Service Canada (CSC); Communications Security Establishment (CSE); Canadian Armed Forces (CAF); Public Safety Canada (PSC). “Many job seekers are often surprised to learn about the variety of roles available,” notes a press release on the event. We can only imagine. Ottawa Citizen (Dylan C. Robertson) (2017-05-03)

Don't change lawful access rules, Parliamentary committee recommends

Liberal-dominated parliamentary committee says the government shouldn't change the current lawful access regime that limits the ability of police to get at telecom subscriber information and encrypted data unless they have a warrant. The recommendation came this week from the House of Commons' public safety and national security committee as part of a broad review of the country's national security framework. Last year the Trudeau government launched a public consultation into federal national security policy, which included the parliamentary committee's work. The government hasn't given an indication yet of when a new policy will be issued. A number of police departments have called for Ottawa to allow law enforcement to more easily get access to subscriber metadata – including names, street addresses, email addresses and IP addresses — for investigation as well as more tools to enable them to crack suspicious encrypted communications. The recommendations by the parliamentary committee – endorsed by the Liberals and the NDP – could be a sign of the way the government is leaning. But the committee's recommendation did leave police faint hope. The two recommendations involving communications are... –”That the Communications Security Establishment, [the federal electronic spy agency] in acting upon the requests of other national security agencies regarding the

surveillance of private communications and the gathering and retention of metadata, work only with appropriate warrants from the agencies making such requests." The parliamentary committee also made other national-security related recommendations including increasing the funding of all public safety and national security review bodies, limiting the powers of the Canadian Security and Intelligence Service (CSIS) and more oversight over federal national security bodies. [IT World Canada](#) (Howard Solomon) (2017-05-04)

Stop delaying on security fixes

An editorial states, "In opposition, the Liberals took a strange stand on the Harper government's draconian anti-terrorism legislation, formerly Bill C-51. They agreed to support the bill, with the proviso that, if they won the election, they would rein in its worst excesses. Well, they won - but nearly halfway through their first mandate, the reining-in has yet to begin. Instead, the Trudeau government, as it is wont to do, undertook a number of public consultations, which have now finished, and convened a parliamentary committee to review our security policy. This week, the Liberal-led committee delivered its welcome, partisanship-transcending conclusion: It's time for the government finally to act. C-51 ought to be repealed entirely. However, in the likely event that doesn't happen, the committee's recommendations provide a workable roadmap for accomplishing the next best thing: fixing the "most problematic" aspects of the law, as the Liberals promised. Deeply problematic, for instance, is a provision that allows the Canadian Security Intelligence Service to "take measures" to disrupt activities it believes pose a security threat, without defining what those measures are or creating mechanisms to ensure the agency doesn't trample Canadians' rights along the way." [Toronto Star](#), A12

[BACK TO TOP / HAUT DE LA PAGE](#)

MINISTER / MINISTRE

RCMP eyes expanded media protections

The RCMP is eyeing a policy change for organized crime investigations to better protect the rights of journalists, newly disclosed documents say. The possible move follows revelations in Quebec about surveillance of reporters by provincial and municipal police and growing concern about the ability of journalists to shield sources from authorities. Under a 2003 ministerial directive, the RCMP must take special care in national security investigations involving sensitive spheres such as the media, politics, academia, religion and unions. It means Mounties must seek high-level approvals before engaging in terrorism and espionage probes that touch these sectors. "Recognizing the sensitivity of investigations involving the media, we are currently discussing how to apply this national security related ministerial directive to all RCMP federal investigations, such as those involving organized crime," internal Mountie briefing notes say. The Canadian Press recently obtained the November 2016 notes through the Access to Information Act. RCMP spokesman Harold Pfeleiderer had no additional comment. Public Safety Minister Ralph Goodale, the cabinet member responsible for the RCMP, has previously said the government is reviewing the 2003 directive to ensure the language is sufficient to safeguard press freedoms. [Canadian Press](#) (Jim Bronskill) (Red Deer Advocate, A14, Times Colonist, Kitchener-Waterloo Record, Toronto Star, Kingston Whig-Standard, Edmonton Sun, Ottawa Sun); [La Presse Canadienne](#) (La Presse+, Le Devoir)

Copts have security concerns

An opinion piece states, "Last month, just a week before Easter, two Coptic Christian churches in Egypt were targeted by Islamic State suicide bombers, killing scores of churchgoers and injuring another 120 innocents. Tragically, the co-ordinated Palm Sunday strikes did not mark the first time that Copts have come under attack by Islamists. In February 2015, 21 Coptic Christian migrant workers in Libya were abducted by the Islamic State and beheaded in a gruesome propaganda video...Although "the Church in Egypt declared no festivities this Easter," Coptic Christians in Mississauga went ahead with Easter celebrations, albeit with "extra security measures," Tawfilis said. Are Coptic Christians elsewhere in Canada taking extra security precautions? "Yes," an Ottawa-area Coptic Christian said in a background interview. The Copt, who wishes to remain anonymous in order to protect loved ones in Egypt, said Coptic Christians in this country have "become vigilant, mindful of the evil around us, stand up to protect

GRC·RCMP



GENDARMERIE ROYALE DU CANADA / ROYAL CANADIAN MOUNTED POLICE

**Daily Media Summary / Revue de presse quotidienne
Royal Canadian Mounted Police / Gendarmerie royale du Canada
May 5, 2017 / le 5 mai 2017**

The Daily Media Summary can also be accessed through [Newsdesk](#) / La Revue de presse quotidienne peut également être accédée via [InfoMédia](#)

TOP STORIES / ACTUALITÉS

CONTRACT & ABORIGINAL POLICING / SERVICE DE POLICE CONTRACTUELS ET AUTOCHTONES

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

FEDERAL & INTERNATIONAL OPERATIONS / OPÉRATIONS FÉDÉRALES ET INTERNATIONALES

ORGANIZATIONAL ISSUES / ENJEUX ORGANISATIONNELS

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

EDITORIALS & OPINIONS / ÉDITORIAUX ET LETTRES D'OPINIONS

OTHER / AUTRES

TOP STORIES / ACTUALITÉS

La GRC envisage une mesure pour une meilleure protection - Droit des journalistes

La Gendarmerie royale du Canada (GRC) envisage une modification à une directive ministérielle afin de mieux protéger les droits des journalistes relativement aux enquêtes sur le crime organisé, indiquent des notes internes. La possible modification survient dans le contexte de révélations de surveillance de journalistes au Québec par la Sûreté du Québec et la police de Montréal et d'inquiétudes grandissantes sur la capacité des journalistes à protéger l'identité de leurs sources. En vertu d'une directive ministérielle de 2003, la GRC doit porter une « attention spéciale » au statut des médias, des politiciens, des universitaires, des leaders religieux et des syndicats dans le cadre d'enquêtes sur la sécurité nationale. Cela signifie que les policiers doivent obtenir des approbations de haut niveau avant de s'investir dans des enquêtes sur l'espionnage ou le terrorisme qui touchent ces secteurs. Des notes internes à la GRC indiquent que les autorités discutent de la manière d'élargir cette directive reliée à la sécurité nationale à toutes les enquêtes fédérales de la GRC, « comme celles impliquant le crime organisé ». [Presse canadienne](#) (La Presse, 14) (2017-05-05); [Canadian Press](#) (CTV News) (2017-05-04)

Arrests have been made in another Facebook Live murder, and this time two teenage girls are the culprits

Two unidentified, Canadian teenage girls, 16 and 17, have been arrested on second-degree murder charges after allegedly filming a Facebook Live video featuring them beating a fellow student to death. The girls, both students at Sagkeeng Anicinabe High School, shared the disturbing video on their

LEGISLATION & POLICIES / LÉGISLATION ET POLITIQUES

New law encourages reporting of drug ODs

A new federal law aims to reduce the number of people who die from opioid and other drug overdoses in Canada. The Good Samaritan Drug Overdose Act was introduced as a private member's bill last year by Liberal backbencher Ron McKinnon of B.C. and received royal assent on Thursday. The law provides immunity from simple possession charges for anyone calling 911 to report an overdose. McKinnon, the MP for Coquitlam-Port Coquitlam, said he was spurred to action by an epidemic of opioid overdoses in B.C. and the rising number of deaths in Alberta and other provinces. McKinnon said there have been cases where people have been afraid to call police or an ambulance for help when someone is having an overdose over fear they will be charged with drug possession. [Times-Colonist](#), A10; [Canadian Press](#) (CBC News) (2017-05-04)

La GRC envisage une mesure pour une meilleure protection - Droit des journalistes

La Gendarmerie royale du Canada (GRC) envisage une modification à une directive ministérielle afin de mieux protéger les droits des journalistes relativement aux enquêtes sur le crime organisé, indiquent des notes internes. La possible modification survient dans le contexte de révélations de surveillance de journalistes au Québec par la Sûreté du Québec et la police de Montréal et d'inquiétudes grandissantes sur la capacité des journalistes à protéger l'identité de leurs sources. En vertu d'une directive ministérielle de 2003, la GRC doit porter une « attention spéciale » au statut des médias, des politiciens, des universitaires, des leaders religieux et des syndicats dans le cadre d'enquêtes sur la sécurité nationale. Cela signifie que les policiers doivent obtenir des approbations de haut niveau avant de s'investir dans des enquêtes sur l'espionnage ou le terrorisme qui touchent ces secteurs. Des notes internes à la GRC indiquent que les autorités discutent de la manière d'élargir cette directive reliée à la sécurité nationale à toutes les enquêtes fédérales de la GRC, « comme celles impliquant le crime organisé ». [Presse canadienne](#) (La Presse, 14) (2017-05-05); [Canadian Press](#) (CTV News) (2017-05-04)

Don't change lawful access rules, Parliamentary committee recommends

Liberal-dominated parliamentary committee says the government shouldn't change the current lawful access regime that limits the ability of police to get at telecom subscriber information and encrypted data unless they have a warrant. The recommendation came this week from the House of Commons' public safety and national security committee as part of a broad review of the country's national security framework. Last year the Trudeau government launched a public consultation into federal national security policy, which included the parliamentary committee's work. The government hasn't given an indication yet of when a new policy will be issued. Today a spokesperson for the Canadian Wireless Telecommunications Association (CTWA) which represents most of the country's wireless carriers, said the group had no comment on the committee's recommendations because government policy hasn't changed. The parliamentary committee also made other national-security related recommendations including increasing the funding of all public safety and national security review bodies, limiting the powers of the Canadian Security and Intelligence Service (CSIS) and more oversight over federal national security bodies. [IT World Canada](#) (2017-05-04)

Loblaw keeping eye on marijuana legislation – MARIJUANA

The CEO and chairman of Loblaw Companies says he hasn't ruled out the possibility of selling recreational marijuana, a slight shift in position for Canada's largest grocery and drugstore chain. Galen G. Weston said his focus remains on dispensing medical cannabis. But when asked whether Loblaw has closed the book on entering the recreational marijuana market, Weston said, "You can never predict the future," adding that the company is closely watching for more details about the federal government's proposed legalization of the drug. "It's fair to say that at this point, based on everything we know today, medical is a place where we see an opportunity," Weston said at Loblaw's annual general meeting. "We believe there is a strong and growing medical case for marijuana and pharmacies should be an important distribution system for medical marijuana." [Canadian Press](#) (Red Deer Advocate, A27)

B.C. lawyer who challenged pot laws defends 3 Saint Johners after dispensary raids - Kirk Tousaw calls raids on 6 medical marijuana dispensaries 'complete overkill'

**Daily Media Summary / Revue de presse quotidienne
Canadian Security Intelligence Service / Service canadien du renseignement de sécurité
May 9, 2017 / le 9 mai 2017**

CSIS IN THE NEWS / LE SCRS DANS LES NOUVELLES

MINISTER / MINISTRE

SECURITY AND LAW ENFORCEMENT / SÉCURITÉ ET EXÉCUTION DE LA LOI

BORDER ISSUES / ENJEUX FRONTALIERS

CYBER AND TECHNOLOGY / CYBER ET TECHNOLOGIE

MILITARY ISSUES / ENJEUX MILITAIRES

PUBLIC SERVICE / FONCTION PUBLIQUE

LEGISLATION AND POLICIES / LÉGISLATION ET POLITIQUES

OTHER / AUTRES

INTERNATIONAL / INTERNATIONAL

CSIS IN THE NEWS / LE SCRS DANS LES NOUVELLES

RCMP created metadata-crunching tool to glean criminal intelligence

The RCMP created, then suddenly abandoned, a tool to crunch electronic message trails gathered during criminal investigations – a previously unknown foray into the controversial realm of big-data analysis. The Mounties' national intelligence co-ordination centre was operating the Telecommunications Analytical Platform, as the tool was known, as recently as mid-November, say internal RCMP notes obtained by The Canadian Press through the Access to Information Act. "The TAP is a platform that regroups copies of certain telecommunications metadata, which are lawfully collected by the RCMP and other Canadian police services in the course of criminal investigations," the RCMP notes say. Metadata is information associated with communications, but does not include the content of actual emails or phone calls. Still, privacy advocates say it can reveal much about a person and should be subject to strict handling procedures. The RCMP tool analyzes metadata from concluded investigations only, such as phone numbers, associated crime types, source links to police records management systems and the geographical region where the metadata was recorded, the notes add. The tool was a "proof of concept" that turned out to be unsuccessful and "therefore the project was ended," said Cpl. Annie Delisle, an RCMP spokeswoman. "No data was retained." News of the RCMP information-sifting tool's apparently brief existence follows a furor over the Canadian Security Intelligence Service's data analysis centre. In early November, Federal Court Justice Simon Noel said CSIS violated the law by keeping electronic data about people who were not actually under investigation. His sharply worded ruling said the spy service should not have retained the information because it was not directly related to threats to the security of Canada. [Canadian Press](#) (Jim Bronskill) (Global News)

What happened to Justin Trudeau's all-star Cabinet?

An opinion piece states, "A single episode, no matter how demoralizing, shouldn't be inflated into the story of a whole government. Still, the pummelling Defence Minister Harjit Sajjan took in question period and beyond—after he had to apologize for untruthful boasting about his role in a military operation more

PM offered zero help: Left defence minister to apologize repeatedly

An opinion piece states, "If Defence Minister Harjit Sajjan were still on the battlefields of Afghanistan, he'd be radioing for air cover as he continues to hunker down against a relentless assault trying to take him out. But he is not there, and when he was first being hammered in the Commons by opposition forces last week for intentionally exaggerating his architect's role in Operation Medusa, Prime Minister Justin Trudeau was all but absent, basically sitting back in mid-political firefight and providing little cover for Sajjan." [Winnipeg Sun](#), A6 (Edmonton Sun, Toronto Sun, Ottawa Sun)

[BACK TO TOP / HAUT DE LA PAGE](#)

PUBLIC SERVICE / FONCTION PUBLIQUE

Politics This Morning: Federal buildings in Gatineau, Que. closed for second day today due to devastating flooding

The significant flooding in Eastern Ontario continues today, with federal buildings in Gatineau, Que. - one of the hardest-hit regions - remaining closed for a second day today. As of Monday night, reports stated that the water levels have stabilized and should start falling, unless there is more significant rainfall. [The Hill Times](#) (2017-05-09); [Postmedia](#) (Ottawa Sun); [La Presse](#) (2017-05-08)

[BACK TO TOP / HAUT DE LA PAGE](#)

LEGISLATION AND POLICIES / LÉGISLATION ET POLITIQUES

LAWFUL ACCESS: Don't change police limits on access to carrier data, says parliamentary committee

Independent Internet providers are cautiously optimistic a parliamentary committee's recommendations this week not to change Ottawa's policies restricting police and intelligence agencies' lawful access to subscriber metadata and encrypted communications will be adopted by a new federal national security strategy. Christopher Hickey, director of industry affairs at the Canadian Network Operators Consortium, said in an interview Thursday he's hopeful the recommendations from the House of Commons public safety and national security committee will be part of the Trudeau government's new national security framework. They were commenting on two recommendations from the committee: First, that because of the 2014 Supreme Court of Canada's decision in *R. v. Spencer*, which said police need a warrant to get access to basic telco subscriber information, no changes to the lawful access regime or encrypted information be made under any new national security policy. However, police were given faint hope with the recommendation that the committee "continue to study such rapidly evolving technological issues related to cyber security." Second, that the Communications Security Establishment - the federal electronic spy agency—can only act on the requests of other national security agencies for surveillance of private communications and the gathering and retention of metadata only if those agencies get appropriate court authority. These were a small part of the report, which mainly deal with oversight of intelligence agencies. [Cartt.ca](#)

[BACK TO TOP / HAUT DE LA PAGE](#)

OTHER / AUTRES

Canadian officials make 1st visit to Tehran since embassy closed in 2012

Canadian government officials will be on the ground in Tehran this week for the first time since the Harper government closed the Canadian Embassy there nearly five years ago. The visit by Global Affairs officials comes just days ahead of a crucial presidential election in Iran, a country Canadian diplomats abandoned in 2012 partly due to security concerns. A government source confirmed to CBC News the officials are in Tehran advocating for Canadians entangled in Iran's legal system, as well as for the improvement of Iran's overall human rights record. [CBC News](#)

Today's News / Actualités
May 19, 2017 / le 19 mai 2017
08:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 08h00 et 14h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / LES FEMMES ET LES FILLES
AUTOCHTONES DISPARUES ET ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

Personal rights, privacy must trump new security powers, Canadians tell feds

Protecting personal rights should trump requests from law enforcement and national security agencies for extra powers, according to a long-awaited consultation report on what Canadians want to see in federal security policy. The summary report from recent national security consultations was released Friday and outlines the responses received from 17,000 emails and 58,000 submissions from Canadians delivered through an online portal. The government launched the consultations last fall to help guide it as it crafts its own national security policy. "Most participants in these consultations have opted to err on the side of protecting individual rights and freedoms rather than granting additional powers to national security agencies and law enforcement, even with enhanced transparency and independent oversight," the report reads. The consultations tackled a wide array of security policy zones: accountability, threat reduction, domestic national security information-sharing, preventing radicalization, amending existing Criminal

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

[BACK TO TOP / HAUT DE LA PAGE](#)

OTHER / AUTRES

NIL

[BACK TO TOP / HAUT DE LA PAGE](#)

INTERNATIONAL

NIL

[BACK TO TOP / HAUT DE LA PAGE](#)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

[Amanda Connolly](#)

Package of broad proposals stemming from the national security report should come within weeks: Goodale

[RalphGoodale](#)

Congrats to Jagger & Chloe on your retirement from [@CanBorder!](#) [@Safety_Canada](#) thanks you for your service!

[NewsroomGC](#)

Min Goodale announces release of the national security consultation summary report. <http://ow.ly/wYDX100G9tu>

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

[globeandmail](#)

Flooding threatens more than half of buildings on Toronto Islands <http://trib.al/TUnoYx5>. From [@GlobeToronto](#)

[mtlgazette](#)

Quebec floods: 2889 residences in 178 municipalities still affected on Friday <https://t.co/ZxnMelXkvt>

[Global Montreal](#)

[#Quebecfloods](#): Almost 2,890 [#Quebec](#) homes still affected <https://t.co/yqQWHQdcL4>

[CKNW](#)

[#UPDATE](#): another threat of [#flooding](#) in [#BC](#)'s Southern Interior due to anticipated heat, melting snow.

<https://t.co/GL6AmMCdgb>

[CTVNews](#)

Severe thunderstorm knocks out power for thousands of residents as lines knocked down in northern New Brunswick <http://ctv.news/gw0MdyB>

NATIONAL SECURITY / SÉCURITÉ NATIONALE

[cforcese](#)

Report <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2017-nsc-wwlr/index-en.aspx...> affirms impression: moving forward w/ both post C-51 fixes & lawful access reform at same time bad idea /1

cforcese

Lawful access/cyber-privacy issues are the most galvanizing in the public space, this report suggests. /2

cforcese

Any effort to bundle revamped lawful access to address "going dark" w/ other changes in same bill would hijack that bill. /3

cforcese

I hope government choses to reach for "low hanging fruit" & fix C-51 mess before attempting lawful access reform /4

cforcese

And incidentally, I am among those who think lawful access reform is necessary, b/c our lawful access laws are patchwork mess. /5

cforcese

Final point: Really hope fact that report supportive of nat'l security reform is being released Fri before a long weekend isn't a signal /6

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

GgNewsCA

Refugee claimant who walked across Manitoba border granted refugee status <https://t.co/8lef9cnzQ1>

CanBorder

Crossing the #BC border on #VictoriaDay long weekend? Check out our #traveltips!<http://ow.ly/4kP430bRMcl>

CYBER SECURITY / CYBERSÉCURITÉ

globeandmail

French researchers find last-ditch cure to unlock WannaCry files <http://trib.al/tx24o6R>. From @globetechnology

SkyNews

Hackers have been arrested across Europe over a spree of thefts from cash machines <https://t.co/f033amddf>

SCMagazine

'Combo list' database of previously breached accounts contains over 560M credentials <https://t.co/dblh36i4Qa>

SCMagazine

Joomla 3.7.1 patches critical SQL injection flaw <https://t.co/vydd8Wti9g>

SCMagazine

Exploit kits, Slammer worm top April's most wanted malware list, Check Point <https://t.co/CrAtBRBBd4>

LAW ENFORCEMENT / APPLICATION DE LA LOI

NewsroomGC

Government of Canada to Defer Firearms Marking Regulations until December 1, 2018 <http://ow.ly/QaB2100G9XM>

rcmpgrcpolice

For #NationalPoliceWeek, the RCMP features a new documentary about the May 2016 Fort McMurray fires. <http://rcmp-grc.ca/ZYi>

grcrcmppolice

#semainedelapolice : la GRC présente un nouveau documentaire sur les feux de forêts de mai 2016 à Fort McMurray. <http://rcmp-grc.ca/ZY5>

rcmpgc

The Musical Ride will be in Blainville on July 6 and in Pont-Rouge on July 8 and 9. An event not to be missed! <https://twitter.com/rcmpgrcpolice/status/865277124512493568>

Today's News / Actualités
May 24, 2017 / le 24 mai 2017
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via
[InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS |
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

Sort out RCMP governance before replacing Paulson, says union

Canada's national police force is at a "crossroads" and the federal government should sort out how the RCMP will be managed before appointing a new commissioner, says the association vying to be the force's first union. The National Police Federation (NPF) says it would be "premature" to immediately replace RCMP Commissioner Bob Paulson while the government is studying possible management and governance changes to deal with concerns raised by three stinging reports into the force's management of thorny workplace issues, ranging from harassment and bullying to mental health. Paulson is retiring from the force effective June 30. There is speculation already about possible candidates to fill the position

TheTorontoSun

From @anthonyfurey: Canada has dozens of jihadists walking free, yet authorities won't charge them.
<http://ow.ly/ntRl30c0TB9> #cdnpoli

OpenMediaOrg

Responses to govt's national security consultation reassure strong public opposition to lawful access:
<http://ow.ly/BoFE30c0P0f> via @mgeist

LAW ENFORCEMENT / APPLICATION DE LA LOI

ipoliticsca

Sort out RCMP governance before replacing Paulson, says union. @kathryn_may has more
<http://ipoli.ca/Je1J30c0l0d> #cdnpoli

KelownaRCMP

Mountie applies tourniquet to pedestrian struck by motorcycle on highway <http://bit.ly/2rVF7bC> #Kelowna

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Safety Canada

Crime prevention project in #Saskatoon will empower youth & help w/ smart decisions that benefit the community
<http://ow.ly/u7bo30c1km8>

Securite Canada

Le projet de prévention du crime à #Saskatoon aidera jeunes à prendre bonnes décisions pr eux et collectivités
<http://ow.ly/v2HL30c1koX>

OttawaCitizen

Provincial stats show fentanyl now Ottawa's deadliest drug <https://t.co/FIWWe24Twh>

**MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / FEMMES ET LES FILLES AUTOCHTONES
DISPARUES ET ASSASSINEES**

I_stone

'It just makes me sick:' Justice minister's father slams missing and murdered inquiry delays via @cattunneycbc
<https://t.co/onfVGduUoL>

PnPCBC

'It's become almost a farce' says Chief Bill Wilson, of lack of action from #MMIWG inquiry. #cdnpoli #pnpcbc

kkirkup

Justice minister's father calls missing, murdered women inquiry 'bloody farce'
<http://www.metronews.ca/news/canada/2017/05/24/national-public-inquiry-a-blood-farce-justice-minister-s-father.html> ... via @Cdnpress #cdnpoli

PUBLIC SERVICE / FONCTION PUBLIQUE

ipoliticsca

Liberals blame Conservatives for Phoenix, drop another \$142M to fix troubled pay system. @kathryn_may has more
<http://ipoli.ca/BNWF30c0x8f>

OTHER / AUTRE

theprovince

Canada 'poured thousands and thousands' into 'fruit machine' — a wildly unsuccessful attempt at gaydar
<http://bit.ly/2rBdjwJ>

Levert, Jean-Philippe (PS/SP)

From: Media Relations / Relations avec les médias (PS/SP)
Sent: Wednesday, May 31, 2017 10:38 AM
To: Brien, Dan (PS/SP); Media Relations / Relations avec les médias (PS/SP); Baker3, Ryan (PS/SP); Tomlinson, Jamie (PS/SP); MacLean, Megan (PS/SP); Levert, Jean-Philippe (PS/SP); Duval, Jean Paul (PS/SP); Martel, Karine (PS/SP); Bardsley, Scott (PS/SP)
Subject: RE: IMSI catcher background
Attachments: MDI Comms Strategy.docx; MDI Fact Sheet FINAL.DOCX; ML - MDI post ISED authorization_FINAL April 5 2017.docx

Hi Dan

Here is what the RCMP have:

Statement: <http://www.rcmp-grc.gc.ca/en/news/2017/5/rcmp-use-technology-identify-cellular-devices-law-enforcement-purposes>

Tech briefing transcript: <http://www.rcmp-grc.gc.ca/en/news/2017/7/cbc-transcript-april-5th-tech-briefing-teleconference>

Comms strategy, Media lines and Fact Sheet are attached.

Also, to close the loop from your request yesterday, CSEC does not have lines on this.

Thanks
-Andrew

From: Brien, Dan (PS/SP)
Sent: Wednesday, May 31, 2017 7:52 AM
To: Media Relations / Relations avec les médias (PS/SP); Baker3, Ryan (PS/SP); Tomlinson, Jamie (PS/SP); Gowing, Andrew (PS/SP); MacLean, Megan (PS/SP); Levert, Jean-Philippe (PS/SP); Duval, Jean Paul (PS/SP); Martel, Karine (PS/SP)
Cc: 'julie.gagnon'; Harold Pfleiderer; Bardsley, Scott (PS/SP)
Subject: IMSI catcher background

Did the RCMP's "lifting the veil" on IMSI catchers include any background material, decks, or handouts?

db mobile

2017/02/28 7:55 AM

Communications Plan

Use of cell-site simulators for law enforcement purposes

Issue:

The RCMP will publicly acknowledge its use of cell-site simulators (CSS) and provide details on the technology to correct misconceptions that have been reported in the media.

Background:

The RCMP uses CSS technology when necessary to assist in criminal investigations relating to national security, serious and organized crime, and other serious *Criminal Code* offences that impact the safety and security of Canadians. During these complex investigations, the RCMP will at times encounter criminals who use multiple disposable cellular devices to mask their illegal activities. The use of a CSS to identify a target's mobile device is often the only way investigators can gather valuable evidence and further an investigation.

In 2015, the RCMP only used CSS technology in connection with 24 priority criminal investigations, and only one of these cases involved exigent circumstances.

In addition to collecting limited information, a CSS may cause limited cellular interference for devices within range of the tool. This may include individuals and cellular devices who are not the target of the investigation but are within range of the CSS. In rare cases, the tool may cause limited cellular interference to 911 calls for some mobile devices with older cellular technology. While evolving technology has significantly minimized this risk, the RCMP always identifies this potential impact when seeking judicial authorization, and ensures that CSS deployment either mitigates or minimizes any potential negative effects.

Strategic Considerations

The RCMP's use of CSS technology has been the subject of recent misperception by the media and the public. To date the RCMP has refused to confirm or deny its use of this technology to protect the RCMP's operational use of the tool from potential exploitation by criminals. The use of this technology has been identified in court disclosures (e.g. Project Clemenza). The concern is why are we releasing this information now, when there doesn't seem to be a link to anything specific that would require us to release it.

While the public information will be general in nature, certain details and sensitive information won't be disclosed to protect the integrity of CSS technology for investigative purposes, and prevent criminals from evading law enforcement surveillance and detection.

s.19(1)

At present, Innovation, Science and Economic Development Canada (ISED) has not signed the final authorization for the RCMP's use of this device.

The Office of the Privacy Commissioner (OPC) is finalizing its investigation in response to a complaint that the RCMP was contravening the collection provision of the *Privacy Act* by collecting personal information using "StingRays" or International Mobile Subscriber Identity (IMSI) catchers. The investigative results will be presented to the complainant – a media outlet – who will undoubtedly release the results publicly. This is expected to be released mid-March.

Communications Objective:

- To position the RCMP and government as being more open and transparent with its investigative tactics.
- To demonstrate that the RCMP has used this technology within given parameters and with judicial authorization.
- Reassure the public that the RCMP is not collecting private information on innocent citizens.

Communications Approach:

Reactive:

- Media lines and Qs and As
- Additional information on the OPC report and/or recommendations (if any) to be added to media lines and communications products featured on the external website

Proactive:

- Teleconference briefing with specified media
 - Media Relations to invite [REDACTED] - CBC, [REDACTED] – Toronto Star, [REDACTED] – Globe and Mail, and one or two French reporters (e.g. [REDACTED] – Radio Canada) to participate in a teleconference briefing to discuss the RCMP's use of CSS technology.
- External website
 - Fact Sheet to be posted before the OPC report is published, and just prior to the teleconference briefing

It is not recommended to use social media to promote the use of CSS technology.

Jeff Adam will act as media spokesperson and identify a French speaking spokesperson for this issue, responding to media inquiries as they come in.

Key Messages:

- The RCMP wants to publicly confirm the use of technology to identify and locate cellular devices in certain investigations and clarify how they are used in the interest of being transparent and improving the public's understanding of the RCMP's use of this technology.
- The RCMP uses a variety of investigative techniques to assist in criminal investigations relating to national security, serious and organized crime, and other serious *Criminal Code* offences that impact the safety and security of Canadians.
- This particular technology helps with criminal investigations related to national security, serious and organized crime and other *Criminal Code* offences that impact the safety and security of Canadians.
- The RCMP uses this technology in full compliance with Canadian laws, including the Charter, and proper judicial processes. Except in extreme cases (e.g. to prevent death or imminent harm), the RCMP must get a judge's authorization before using the technology.
- There are a limited number of authorized and trained police officers who can use this technology and its use is subject to very strict rules, senior management approval and judicial authorization prior to deployment.

Evaluation

As the information is going public, we will monitor media coverage and social media pick up of the information following the teleconference briefing. Should media calls become un-manageable after the story goes public, we may want to consider holding a more broad technical briefing.

We will monitor the traffic on the RCMP web page.

Written by: Michelle Rose (27 Jan 2017)

Reviewed by: Melanie Roush

Approved by:

RCMP Fact Sheet

RCMP use of technology to identify cellular devices for law enforcement purposes

Technology used to identify and locate cellular devices, commonly referred to as Mobile Device Identifiers (MDI), has been the subject of recent media coverage.

In the interest of transparency, the RCMP confirms the use of MDI technology to identify and locate a suspect's mobile device. This capability can be used to further criminal investigations relating to national security, serious and organized crime, and other serious *Criminal Code* offences that impact the safety and security of Canadians.

The RCMP uses MDI technology in full compliance with Canadian laws, including the Charter of Rights, and proper judicial processes. Except in extremely urgent cases (i.e., to prevent death or imminent harm), the RCMP must get a judge's authorization before using the technology.

There are a limited number of authorized and trained RCMP operators who can use MDI technology and its use is subject to very strict rules, senior management approval, and judicial authorization prior to deployment.

What does it do?

RCMP MDI technology is an important investigative tool used to identify a suspect's cellular device, such as a mobile phone. It helps the RCMP identify an unknown cellular device used by a target (suspect) under investigation by collecting limited signaling information, or for other policing matters, such as identifying the location of a known cellular device linked to a missing person.

In very simple terms, when a trained officer deploys MDI technology, it attracts and momentarily connects cell phones in the immediate proximity, before returning them to their own networks. The technology collects International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) data associated with the phones, allowing the operator to identify the phone used by the suspect. The IMSI and IMEI are internationally standardized unique numbers to identify a mobile subscriber and device, respectively.

What doesn't it do?

RCMP MDI technology does not collect private communication. In other words, it does not collect:

- voice and audio communications
- email messages
- text messages
- contact lists
- images
- encryption keys
- basic subscriber information

Information that is not relevant to the investigation is immediately destroyed after court proceedings, appeal periods, and any specific orders from a judge.

How does it help investigations?

MDI technology provides valuable assistance to criminal investigations and other policing duties. It may be used to help identify an unknown cellular device associated with an individual under investigation by collecting limited information from devices within range of the technology. It may also be used to locate cellular devices which are already known to police.

How is it deployed?

After getting authorization from a judge, the MDI is deployed for a short period of time to attract and collect limited information (IMSI and IMEI data) from cellular devices in close proximity. This data can be used to help identify a cellular device used by a suspect under investigation.

How often is this technology deployed?

There are a limited number of authorized and trained RCMP operators who can use this technology. Further, its use is limited to only the most serious cases, and only when there are grounds to believe that a suspect is using an unknown cell-phone to conduct criminal activities. Its use requires a judge's authorization, as well as authorization at very senior levels of the RCMP. There are also strict reporting requirements for each use.

In 2016, the RCMP used MDI technology in only 19 investigations.

Who makes the decision to deploy the technology and what oversight is there of their use?

Before this technology is deployed, senior officer approval and a valid judicial authorization are required. Prior judicial authorization is not required, in extremely urgent cases where the police reasonably believe there is a need to deploy the technology to prevent imminent harm or death.

Those authorized to use the technology have received specialized training and each use is reported and recorded by the operator.

What happens to the data the MDI technology collects?

The limited data collected by MDI technology (IMSI and IMEI data) is stored in an isolated system that is only accessible by those managing the technology.

To further a criminal investigation beyond this limited data, the RCMP must get a production order from a judge to obtain basic subscriber details associated with the IMSI or IMEI data from a Telecommunications Service Provider (e.g., the telephone number, name and address of the subscriber).

Information that is not relevant to the investigation is immediately sequestered by the operator and not shared with investigators. It is destroyed after court proceedings, appeal periods, and any specific orders from a judge.

Does this impact other cell phone users in the area?

MDI technology can cause limited cellular interference for devices within range of the tool. The RCMP makes every effort to deploy the technology in a way that causes the least disruptions to service and public safety.

12/06/2018 11:29 AM

RCMP Media Lines

-APPROVED -

Date: April 5, 2017

Issue/Title: The RCMP use of Mobile Device Identifier (MDI) technology for law enforcement purposes

Background:

The RCMP's use of Mobile Device Identifier (MDI) technology has been the subject of recent misperception and confusion by the Canadian public and the media. The RCMP wants to publicly confirm their use in certain investigations and clarify how they are used in the interest of being transparent and improving the public's understanding of the RCMP's use of this technology.

Media Lines - General:

- As Canada's national police force, the RCMP uses various technical investigative tools and methods to lawfully obtain evidence in order to protect Canadians and advance serious criminal investigations.
- The RCMP uses technology to identify and locate cellular devices to assist in criminal investigations relating to national security, serious and organized crime, and other serious *Criminal Code* offences that impact the safety and security of Canadians.
- The technology is an important law enforcement tool that works by collecting limited information from an unknown cellular device used by a suspect, such as a mobile phone.
- Being able to identify a suspect's mobile device allows investigators to pursue other lawful avenues to gather valuable evidence and further an investigation.
- If the particulars of a mobile device are known, the use of the technology allows the RCMP to search for the device, such as when trying to locate missing persons.
- The RCMP's technology is not capable of collecting the contents of any form of private communication. It cannot collect the content of voice and audio communications, email messages, text messages, contact lists, images, encryption keys, or any other content and basic subscriber information.

Authority to Use the Technology

- The RCMP uses investigative tools and techniques in full compliance with the laws of Canada, including the Charter, and appropriate judicial processes.
- With the exception of exigent circumstances (i.e. to prevent imminent bodily harm), the RCMP seeks prior judicial authorization to use the technology, and only uses this technique with the approval of a senior officer when required to further an investigation.

The RCMP and Innovation, Science and Economic Development Canada:

- The RCMP has worked closely with Innovation, Science and Economic Development Canada (ISED) to analyze the *Radiocommunication Act* and determine the appropriate legal framework for the use of the technology by the RCMP.

Office of the Privacy Commissioner of Canada Investigation

- In April 2016, the RCMP received notification from the Office of the Privacy Commissioner of Canada that an investigation was being launched in response to a complaint that the RCMP was contravening the collection provision of the *Privacy Act* by collecting personal information using devices known as International Mobile Subscriber Identity (IMSI) catchers.
- The RCMP has fully cooperated with the Office of the Privacy Commissioner of Canada in this matter, and has provided a detailed explanation of its operations and policies.

Q&As

Q: How does a cell-site simulator work?

A: During complex national security or organized crime investigations, the RCMP may need to identify an unknown cellular device used by criminals. Under judicial authority, the technology is used for a short duration to attract and collect limited information from cellular devices, such as mobile phones in close proximity, including International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) data. This data can be used to help identify a cellular device used by a suspect under investigation.

In rare but urgent situations, the RCMP may be required to locate a specific mobile device, such as in the case of missing persons. If the IMSI or IMEI numbers are known, the technology can be utilized to locate a specific mobile device in a limited geographical area.

Q. Are these also referred to as "IMSI Catchers?"

A. Yes, this technology is sometimes referred to in public forums as "IMSI catchers" or incorrectly "Stingrays."

Q: Will the use of this technology impact other cell phones in the area?

A: It may cause limited cellular interference for devices within range of the tool. The RCMP makes every effort to deploy the technology in a way that causes the least disruptions to service. This includes deploying the technology for short duration periods and frequently changing cellular frequencies. In rare instances, the deployment of the tool may cause limited cellular interference to 911 calls for some mobile devices with older cellular technology. While evolving technology has significantly minimized this risk, the RCMP always identifies this potential impact when seeking judicial authorization, and ensures that the deployment either mitigates or minimizes any potential negative effects.

Q. If my information is collected through this technology, what happens to it?

A: The RCMP destroys any collected data from non-targets (third parties) immediately following court proceedings, including appeal periods, and any specific orders from a judge.

Q: How often does the RCMP use CSS technology?

A: In 2016, the RCMP used the technology in connection with 19 criminal investigations. In 2015, the RCMP used the technology in connection with 24 investigations.

Q. What type of judicial authorization is required prior to the use of this technology?

A. Prior to deploying the technology, unless there are exigent circumstances, (such as threat to life), the RCMP obtains a Transmission Data Recorder Warrant (Section 492.2 of the Criminal Code). The RCMP's use of the technology is always guided by legislation, court decisions, consultation with Crown and the National Wiretap Experts Committee (NVEC). The NVEC is comprised of criminal justice personnel, including Federal and Provincial Crown prosecutors and law enforcement from across Canada. The NVEC provides guidance to law enforcement and prosecutors on the application of legal tools (procedural powers) in the *Criminal Code*.

Q. Does the RCMP now have an authorization under the *Radiocommunication Act* to use this technology a ?

ISED has authorized the RCMP to use radio devices, referred to as mobile device identifiers or more commonly, "IMSI catchers" or Stingrays, designed to capture device identifier data on commercial mobile networks. Further, Section 54 of the *Radiocommunication Regulations* permits the interception and use of radio signals for public safety and law enforcement purposes.

This authorization does not exempt the RCMP from the requirement to obtain judicial warrants when using these devices in criminal investigations.

Q. Why is the RCMP only now confirming use of this technology when it's been in the public domain for a while?

A. The RCMP wants to strike a balance between public transparency on the use of the technology, and continuing to protect this important tool for public safety and law enforcement purposes.

IF PRESSED ONLY

Q Does the RCMP deploy the technology in aircraft?

A. To prevent criminals from learning of ways to defeat or avoid surveillance, the RCMP does not discuss specifics on how it deploys any type of surveillance technology. The RCMP only deploys surveillance technology when it is lawful to do so and with the appropriate judicial authorization.

Contact: Media Relations, National Communication Services NCS,
(613) 843-5999

Prepared by: Michelle Rose, National Communications Services (613) 843-5492

Reviewed by: **Melanie Roush, NCS**
Jeffrey Morris, Strategic Policy and Integration, SPS
Kimberley Pearce, Legal Services

Approved by: **Chris Lynam, Strategic Policy and Integration, SPS**
Kelly Bradshaw, Tactical Operations, Technical Investigation Services
John Robin, Technical Investigation Services
Jolene Bradley, Director Operations, NCS
Joe Oliver, Technical Operations



SECRET / Confidence of the Queen's Privy Council (with attachments)

s.69(1)(g) re (a)

s.69(1)(g) re (e)

Minister's Briefing Breffage du ministre

Monday, June 5, 2017 – 4:30 p.m. to 5:30 p.m. / Le lundi 5 juin 2017 – 16h30 à 17h30

Room 501-S, Centre Block / Salle 501-S, Édifice du centre

AGENDA / ORDRE DU JOUR

| ITEM / POINT | SUBJECT / SUJET | PARTICIPANTS | DURATION / DURÉE |
|-----------------|-----------------|--|--------------------------|
| 1 | | <p><u>LEAD / RESPONSABLE</u></p> <p>Monik Beauregard <i>Senior Assistant Deputy Minister, NCSB</i></p> <p>Sophie Beecher <i>Director, National Security Policy Directorate, NCSB</i></p> <p><u>OTHERS / AUTRES</u></p> <p>Jeff Yaworski <i>Interim Director, CSIS</i></p> | 4:30 5:30 (60 min) |

TAB 1

**Pages 368 to / à 387
are withheld pursuant to sections
sont retenues en vertu des articles**

69(1)(d), 69(1)(e), 69(1)(g) re (a), 69(1)(g) re (e)

**of the Access to Information
de la Loi sur l'accès à l'information**

Tomlinson, Jamie (PS/SP)

From: Brown, Malcolm (PS/SP)
Sent: June-20-17 5:11 PM
To: Tomlinson, Jamie (PS/SP)
Subject: RE: Transcript - Not for attribution technical briefing prior to a national security-related announcement - 2017-06-20 - 11:30 ET

thanks

From: Tomlinson, Jamie (PS/SP)
Sent: Tuesday, June 20, 2017 5:11 PM
To: Brown, Malcolm (PS/SP)
Cc: Beauguard, Monik (PS/SP); Wherrett, Jill (PS/SP); De Santis, Heather (PS/SP)
Subject: FW: Transcript - Not for attribution technical briefing prior to a national security-related announcement - 2017-06-20 - 11:30 ET

fyi

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: June-20-17 4:08 PM
To: Today's News / Actualités (PS/SP)
Subject: Transcript - Not for attribution technical briefing prior to a national security-related announcement - 2017-06-20 - 11:30 ET

DATE/DATE:
June 20, 2017 11:30 a.m. ET

LOCATION/ENDROIT:
National Press Theatre, Parliament Hill, Ottawa, Ontario

PRINCIPAL(S)/PRINCIPAUX:
Senior Officials

SUBJECT/SUJET:
Not for attribution technical briefing prior to a national security-related announcement.

Moderator: Good morning and welcome to this technical briefing on the National Security Act 2017. My name is Moderator. I am joined today by the following officials: Senior Official 1, Senior Official 2, Senior Official 3, Senior Official 4 and Senior Official 5.

The purpose for today's session is to provide you with an overview of the National Security Act 2017 which was tabled in the House of Commons earlier today. As you will see in our media advisories, Ministers will be here shortly after this session to provide statements and to take your questions. We are then offering a series of more detailed briefings to discuss elements of the bill in greater detail.

As this briefing is on background I would remind you that cameras are not permitted nor is any recording for broadcast. I would ask that attribution be made to Senior Officials. Bonjour et bienvenue à cette séance technique sur la loi de 2017 sur la sécurité nationale. Je m'appelle Moderator. Je suis accompagné par les représentants suivants : Senior Official 1, Senior Official 2, Senior Official 3, Senior Official 4 and Senior Official 5.

La séance aujourd'hui a pour but de vous donner des renseignements liés à la loi de 2017 sur la sécurité nationale déposée devant la Chambre des Communes plus tôt aujourd'hui. Comme l'indiquent les avis aux médias les Ministres

seront ici peu de temps après la séance pour faire des déclarations et répondre à vos questions. Ensuite nous tiendrons une série de séances plus détaillées pour discuter d'une façon plus approfondie des éléments continus dans la loi.

Puisque cette séance d'information vise des renseignements généraux je vous rappelle que les caméras sont interdites et qu'il n'y a pas d'enregistrement aux fins de diffusion. Je demande que toute attribution renvoie à de hauts fonctionnaires. To begin the briefing I will ask Senior Official 1 to make opening remarks. Following her presentation we will open it up for your questions.

Senior Official 1: Bonjour. Je suis ravi d'être ici aujourd'hui en vue de vous expliquer des éléments dont la loi de 2017 sur la sécurité nationale est composée. Abroger des éléments problématiques de l'ancien projet de loi C51 et instaurer de nouvelles dispositions législatives qui renforcent la responsabilisation en matière de sécurité nationale représentaient un engagement clé du mandat du Ministre de la Sécurité Publique et de la Ministre de la Justice.

Le projet de loi qui a été déposé ce matin à la Chambre des Communes remplit cet engagement et même le dépasse afin d'aborder un nombre d'enjeux essentiels dans le domaine de la sécurité nationale. Le projet de loi réalise un double objectif de renforcer notre capacité à assurer la sécurité des Canadiens et en même temps à protéger nos valeurs, droits et libertés. Ensemble ces mesures proposées représentent des améliorations approfondies et grandement nécessaires au cadre de sécurité nationale du Canada.

Last fall the government engaged Canadians in an unprecedented conversation on national security through a broad public consultation. Canadians, academics, subject matter experts and key stakeholders all provided their views and ideas online and through a number of consultation events such as public town halls and ministerial town halls at Parliamentary Secretary level and ministerial level and various digital events. Finally two parliamentary committees concluded reviews and released reports with recommendations.

De plus comme vous le savez sans doute toutes les présentations publiques ont été rendues accessibles au moyen de portail des données ouvertes et un rapport indépendant sur les résultats des consultations a été publié. The National Security Act 2017 reflects the views and expectations the government heard during consultations while strengthening Canada's ability to address threats. It consists of ten parts. In addition the government is committing to other non-legislative measures to complement the bill.

I will go through the proposals thematically rather than sequentially and three themes are introduced in the next slide. Comme je l'ai mentionné au début le double objectif est de protéger les Canadiens tout en préservant nos valeurs, droits et libertés. Par la législation proposée le gouvernement fait ce qui suit : premièrement améliorer la responsabilité et la transparence en remaniant notre architecture d'examen de la sécurité nationale, en créant des mécanismes de surveillance plus solides et en mettant en marche un changement de culture relativement à la transparence.

Deuxièmement, s'acquitter de ses engagements en abordant les éléments problématiques du projet de loi C51 et en faisant même davantage afin d'apporter des modifications législatives supplémentaires. Finalement proposer des mises à jour législatives afin de garder le rythme avec les menaces en évolution et de préciser les pouvoirs de nos organismes de sécurité et du renseignement.

Looking at the first theme, the results of the consultations demonstrated a concern about the need for increase accountability and more transparency on national security. The government is proposing three key initiatives to meet this demand. First, enhancing review through a consolidated national security review body, the National Security and Intelligence Review Agency. The new review agency would replace the Security Intelligence Review Committee, SIRC, and the Office of the Communications Security Establishment Commissioner, OCSEC and would also take on a review of the RCMP's national security activities currently done by the Civilian Review and Complaints Commissioner.

This new body would have complete access to all information, be able to follow the thread wherever it may go to undertake reviews and cover all Canadian departments and agencies that have national security responsibilities. Approximately 14 additional departments and agencies will be for the first time accountable to a review body. The new review agency will be an important complement to the National Security and Intelligence Committee of Parliamentarians created by this government in Bill C22 and currently before Parliament.

Deuxièmement, améliorer la surveillance par la création d'un nouvel organisme de surveillance, le Commissaire aux Renseignements qui autorisera certaines activités liées aux renseignements avant leur exécution. Le Commissaire aurait comme mandat d'approuver les autorisations accordées et des déterminations effectuées par les Ministres pour certaines activités du Service Canadien des renseignements de sécurité et du Centre de la Sécurité des Télécommunications.

Il ou elle serait entièrement indépendant du gouvernement et des organismes de renseignement qu'il ou elle supervise. Le gouvernement va aussi réviser et étudier les instructions du Ministre concernant le partage d'information à des entités étrangères et de plus une nouvelle instruction du Ministre établira des attentes relatives à la manière dont les organismes de sécurité interagissent avec les journalistes.

Third and final initiative in the first theme is increasing transparency by setting in motion a new approach to transparency and national security backed by a series of principles and an implementation plan. Moving to the second theme, en plus d'accroître la responsabilisation et la transparence le gouvernement respecte son engagement de modifier les éléments problématiques de l'ancien projet de loi C51.

Le projet de loi comprend donc premièrement le remaniement de l'actuel processus ouvert d'obtention d'un mandat pour la réduction des menaces et son remplacement par une liste de pouvoirs spéciaux et l'introduction de nouvelles protections. Second, clarifying the information sharing process between federal institutions for national security purposes under the new Security of Canada Information Disclosure Act, formerly the Security of Canada Information Sharing Act, namely that SCIDA, the Disclosure Act authorities are only about disclosure to an agency with existing collection powers.

Enhancing the threshold for disclosure by prescribing specific conditions that need to be met prior to information being disclosed including accuracy and reliability and adding mandatory record keeping obligations. Ensuite modifier la loi sur la sureté des déplacements aériens afin d'améliorer le processus de recours en vue de retirer un demandeur de la liste à moins que le Ministre ne répond dans les 120 jours et de permettre au Ministre d'informer des parents que leur enfant ne figure pas sur la liste sans restrictions relatives à la divulgation.

The bill also proposes amending elements of the Criminal Code that were part of former Bill C51. The measures respond to concerns of vagueness and overbreadth of the advocacy or promotion of terrorism offence by revising it to more clearly resemble counseling. Since the definition of terrorist propaganda in the terrorist propaganda warrant scheme relies in the advocacy offence for meaning, corresponding changes are proposed to that definition to reflect the new counseling of terrorism offence.

The proposal would increase the threshold to obtain recognizance with conditions and no specific changes are being proposed on terrorism peace bonds but the legislation creates a requirement for the Attorney General of Canada to report annually to Parliament on the number of terrorism peace bonds that have been entered into. De plus un examen statutaire de la loi aura lieu après cinq ans afin de tenter de l'harmoniser avec l'examen statutaire du comité Parlementaire de sécurité nationale et du renseignement.

Finally under this second theme with respect to CSC the new intelligence commissioner would approve authorizations issued by the Minister of National Defence for certain intelligence and cyber security activities prior to their conduct. Maintenant sur le troisième thème, Premièrement la modernisation de la loi sur le SCRS. Le projet de loi établit un régime d'autorisation pour des activités qui seraient autrement illégales.

La proposition établit une justification limitée qui permettrait au service canadien du renseignement de sécurité d'exécuter des activités au cours d'une enquête qui seraient autrement illégales en vertu de la loi canadienne afin de s'assurer que le service puisse effectivement s'acquitter de son mandat face aux menaces complexes. Ce point est fondé sur une disposition sur l'application de la loi du Code Criminel mais adaptée au contexte de la sécurité nationale.

The legislation would exempt CSIS officers and sources from certain offence provisions that affect covert identity protection. The proposed legislation also creates a robust framework in the CSIS Act for the collection, retention and use of data sets. Data analytics can provide insight into subjects of investigation and identify new leads and intelligence gaps. It can also provide context and understanding to operations.

When it was written the CSIS Act could not have anticipated the technological changes of the last 30 years. This was acknowledged by the federal court which noted the value of data analytics but concluded the CSIS Act did not fully accommodate these programs. As such legislative amendments are being advanced to modernize the CSIS Act and address these gaps.

Deuxièmement, proposition d'une loi sur le CST. Le cyber environnement évolue rapidement. Pour empêcher que le CST ne se laisse devancer et lui permettre d'utiliser en toute légalité les outils à sa disposition il faut une loi qui l'aidera à protéger les Canadiens au pays et à l'étranger. La loi sur le CST proposé constitue une loi claire qui dissipera les ambiguïtés sur le travail du CST. Grâce à la loi sur le CST proposé, le CST pourra continuer à fournir les renseignements électromagnétiques étrangers pour protéger le Canada et les Canadiens contre les menaces et pourra continuer à protéger et à défendre les systèmes de gouvernement et à mieux protéger l'information la plus sensible et les

cyber-réseaux importants contre les compromissions. Finalement le CST pourra collaborer avec les propriétaires des réseaux importants afin de renforcer leur défense contre les cyber-menaces.

The proposed CSE Act would also permit CSE to support the Department of National Defence and the Canadian Armed Forces in their missions and outline the new proposed authorities for CSE to engage in cyber operations that will disrupt the capabilities and activities of adversaries that aim to cause serious harm. The CSE Act will clearly outline that privacy protection is fundamental to CSE activities.

The act will explicitly prohibit CSE from directing its activities at Canadians or anyone in Canada. It will also require that CSE have measures in place to protect the privacy of Canadians. The act also proposes to introduce important new transparency and accountability measures including advanced certification of CSE's foreign intelligence and cyber security ministerial authorizations by the independent intelligence commissioner.

These measures also include more and more specific privacy protection measures that are enshrined in legislation. They include strong and independent review of CSE's activities by the new national security and intelligence review agency as well as the additional oversight provided by the national security and intelligence committee of Parliamentarians. The role of the commissioner would be filled by a retired judge of a superior court as is the case with the current CSE commissioner.

The commissioner would assess and approve the reasonableness of ministerial conclusions authorizing foreign intelligence and cyber security activities to ensure they are reasonable, necessary and proportionate and that appropriate privacy protections are in place. The commissioner would be reviewing CSE's ministerial authorizations before CSE could conduct collection activities under those authorizations.

The approval of the commissioner would be binding meaning that CSE must have the commissioner's approval to proceed with those activities. Other proposed legislative changes captured in the third theme include amending the Criminal Code measures dealing with witness protection to create a general power of the court to make any order to protect witnesses testifying in recognizance with conditions of peace bond hearings, amending the Criminal Code terrorist entity listing regime to enhance procedural efficiency.

Apporter des modifications à la loi sur le système de justice pénal pour les adolescents, ce qui implique de veiller à ce que tous les jeunes qui ont des démêlés avec le système de justice pénal pour des comportements liés au terrorisme bénéficient des mesures procédurales supplémentaires et des autres protections prévues dans la loi sur le système de justice pénal pour les adolescents.

(Cross talk)

On a aussi des briefings techniques qui suivent cet après-midi donc on a beaucoup d'opportunités de pouvoir se parler. En résumé l'objectif est de protéger les Canadiens tout en préservant nos valeurs, droits et libertés et pour se faire il faut améliorer la responsabilisation et la transparence, s'acquitter de nos engagements prévus au mandat et mettre à jour et améliorer la loi sur la sécurité nationale. Voilà.

Moderator: Thank you very much. We'll now move to our questions and answers. Nous passerons maintenant à la séance des questions et réponses. We will begin with questions here in the room.

Question : À la page 101 dans le projet de loi vous modifiez paragraphe 21.1 en ajoutant des mesures qui expliquent un peu plus le rôle de CRS. Est-ce qu'au cours des dernières années les CRS faisaient autre chose que ça, que ce qu'on définit ou bien encadrer ce que le CRS peuvent faire, page 110.

Senior Official 1 : Les mesures – les amendements proposent vraiment de remplir les engagements envers la révision des éléments problématiques du projet de loi C51 et en fait ce qu'on propose ici vous verrez qu'on propose de supprimer l'ancien paragraphe qui existait dans la loi et de le remplacer par celui-ci. Peut-être qu'à ce moment-là je peux passer la parole à Senior Official 4.

Senior Official 4 : Essentiellement ça définit effectivement les mesures qu'on peut prendre, une limite à ces mesures-là.

Question : Est-ce que les CRS faisaient autre chose avant ?

Senior Official 4 : Non, nettement non. C'est le genre d'activité qu'on faisait avant.

Question : Est-ce que le CST, le CRS ou d'autres agences peuvent collecter des métadonnées des Canadiens avec cette ouverture de la loi ?

Senior Official 1 : Une des nouvelles provisions proposées dans la loi concerne les ensembles de données et il y a tout un cadre qui est proposé dans la loi autour de la collection d'ensembles de données mais aussi du maintien et du query, c'est-à-dire de garder l'information. Il y a plusieurs étapes. Le processus qui est décrit envisage que le commissaire va déjà donner des autorisations d'obtenir des ensembles de données canadiennes.

Ensuite le service aura une période de temps pour évaluer s'il y a une valeur ajoutée. Si effectivement le service détermine qu'il y a une valeur ajoutée le service devra aller à la cour fédérale pour obtenir la permission de garder des ensembles de données et ensuite de pouvoir procéder aux data analytics.

Question : Des Canadiens ?

Senior Official 1 : Oui.

Question: There's an adaptive warrant for national security. In Criminal Code cases there's usually the release of the information after the return of the warrant. People can see what was seized by the police after the investigation is concluded, after the warrant has been executed. There's a post facto accountability there. Will there be that in the case of these intelligence warrants? Will we know after they've been executed what was done, what was seized, what activities were performed?

Senior Official 1 : That's one of the elements that I raised in the talking points was that we did model the justification regime that we are now proposing to adopt on 25.1 of the Criminal Code. It was adopted for national security purposes. There are different dynamics at play of course and what we're proposing to do is add on top of that some fairly robust accountability and review measures around that.

Question: What happens after the warrant's executed? Does it become available to the parties? In the case of a Criminal Code warrant you can see afterwards what was obtained or what was done under the warrant. You can't necessarily I would presume in the case of an intelligence warrant. Is that correct?

Senior Official 4: That's correct. We don't release the information publicly. That being said, there is tremendous review and this new legislation adds that review with the creation of the new bodies that are being created. There will be plenty of opportunities for the intelligence commissioner, for the review committee and for the federal court themselves, if we renew warrants we have to go back in front of the federal court. Generally speaking unless we release information to law enforcement the information remains classified.

Question: Is there any change in the way you've constructed CSE's powers and limited them and they're not to be directed at a Canadian? CSE can still though work with any domestic law enforcement agency if that agency has a warrant, right? So they can assist and target and direct their operations at Canadians. That doesn't change. That can still happen. Is that correct?

Senior Official 2 : Correct, yes.

Question: In the context of – there's so much to ask.

Senior Official 2: If I can just specify, in that assistance we would be operating under the authorities of the requesting agency. A law enforcement or security agency such as CSIS or RCMP if they want to leverage us they have to demonstrate they have the lawful authority to target a Canadian.

For example they would need an actual warrant. They would have to show us the warrant and then we would be operating under their authority and bound by the parameters of that.

Question: (Off microphone) targeting Canadians under those warrants unless somehow they –

Senior Official 2: We would be operating as CSIS so it would be CSIS activities but they would be leveraging our capabilities.

Question: Just on page 74, in terms of the disclosure, you're authorizing CSE to disclose the information it collects in its foreign intel ops or other ops including presumably in those cases about Canadians to certain designated people. In other words are you going to – so CSE will still be able to disclose or has full authority to disclose to other foreign state

agencies, intel agencies, other foreign state actors even where for example there may be human rights concerns or torture practices. Right?

In other words the names of Canadians are still going to be able to be handed off. Is that correct?

Senior Official 2:No. In practice we collect foreign agency intelligence, we write reports. We obviously have agreements in place for example with the Five Eyes. Those agreements still require us to protect privacy. We have measures in place to protect privacy. We also have a ministerial directive that causes us to do a mistreatment risk assessment so that even if those agencies then want us to disclose that information further, identities of someone, for example we write a report.

We mask the identity of a potential Canadian that might want to be doing something wrong in the United States and the United States says, we have an interest in the identity of that Canadian. We still do a mistreatment risk assessment on any disclosure depending on what that disclosure looks like.

Question:On page 92 about the data set collection, it says that data sets publicly available can be retained by CSIS and CSE. Is there any limit on publicly available? For instance, the information that finds its way onto the internet cannot be processed and retained by the services?

Senior Official 4:We define publicly available as an example a phone book, a referential data set that the public could access. That's how we define it. Any data set that we want to retain, I mean we would need the authority of for the Canadian data sets the Minister and the intelligence commissioner would also look at those authorities and approve them. That's a third party review if you will.

Anything we retain needs to be relevant to our mandate, needs to be relevant to the duties and functions of CSIS. It needs to be strictly necessary. All of that examination goes into place when we're looking at the data sets.

Question: In terms of the retention of the data, there's nothing in here that would allow CSIS to go back to what it was doing with the ODAC in terms of keeping data forever in case it might be useful? There are still time limits on any data set that the service collects.

Senior Official 4: There are time limits. We can both I believe it's two years for Canadians and five years for foreign but we can go back to court to get extensions if we need to. But in order to extend that for the data sets we have to have federal court approval.

I do want to differentiate though if you're referring to the October 2016 decision by the federal court, that is a separate issue. That's to do with associated data on third parties non-threat related. It's a separate issue which we're still managing right now in terms of addressing that concern of the federal court. This has to do with data sets which the court also found in their judgment, recognizing the benefits of data analytics but expressing a concern that there be a better regime around the management of that which is what this addresses.

Question: Je ne comprends toujours pas exactement le changement qui est apporté aux mesures de réduction d'une menace. Si je comprends l'ancien projet de loi, le SCRS avait le pouvoir de commettre des gestes pour prédire une menace, la perturbation qu'on l'appelait et devait s'adresser aux tribunaux seulement s'il pensait que le geste qu'il allait poser était contraire aux lois ou à la Charte.

Je ne vois pas vraiment quel changement ici vous aménagez. Surtout vous avez reconnu à mon collègue toute à l'heure que la liste fournie dans le projet de loi d'activités est essentiellement la même chose que ce qui se faisait déjà par le CRS. Vous pouvez peut-être clarifier.

Senior Official 4 : (Off microphone) Voici ce que fait le service mais aussi ça nous limite à ce qui est inscrit dans la loi. Donc avant je pense qu'il y avait une préoccupation que c'était un peu vague. Les Canadiens ne savaient peut-être pas ce qu'on faisait. Maintenant on décrit ce qu'on peut faire, ce qu'on a le droit de faire et aussi ça indique clairement qu'il faut aller chercher un mandat si jamais cela enfreigne la Charte.

Question : Ce mandat-là c'est la même chose qu'avant. Avant si c'était contraire à la loi on devait s'adresser (cross talk) et là c'est la même chose. Avant c'était si c'était contraire à la loi on devait (cross talk) et là c'est la même chose. On n'a pas limité la Charte. Est-ce que le seuil pour obliger l'obtention d'un mandat est abaissé ou c'est le même ?

Senior Official 4 : Pas du tout, pas du tout. Je ne sais pas si Justice peut vous répondre mais non, pas du tout. C'est vraiment un effort de transparence pour dire voici les mesures parce qu'avant ce n'était pas inscrit dans la loi. Donc je pense qu'il y avait une préoccupation. Qu'est-ce qu'ils font au juste ?

Question : (Off microphone) C'est juste que maintenant il est écrit sur papier.

Senior Official 4 : On décrit les mesures.

Senior Official 1 : On ajoute une liste de restrictions aussi. C'est-à-dire, je n'ai pas la page mais on décrit exactement ce que le service ne peut jamais faire.

Question : In terms of the practical application of this new super SERC is how the Minister described it this morning, how would that work because it sounds like the SERC, the OCSEC, the SRCC, those functions are rolling into one overarching new agency or whatever you want to call it.

What happens to the staff, the apparatus from the other places? Do they get folded into this new one? How long after this legislation is passed do those other operations cease to exist? Is there a time limit?

Senior Official 1: You're right. SERC, the current SERC and the current portion of OCSEC, the portion that was currently doing review of CSE will be subsumed into this new review agency. There's growth also foreseen for the agency and in terms of how soon it will be delivered, it will also depend on how quickly we can get this bill passed.

Question: Those stats from the other areas, they just roll over to this one. Okay. You also mentioned there are 14 departments or agencies that are not currently under scrutiny or accountable which will now be accountable to this super agency. Is there a list of those 14 that's available?

Senior Official 1: You can probably just use the schedule 3 of the SCISA Act. Sorry, I can't list them all off the top of my head. DND, GAC, CBSA the border agency, Transport, FINTRAC, IRCC, all those other government departments, fourteen. We can make the list available if that helps so you don't have to go and search schedule 3 of SCISA.

Question: I wanted to get some clarification. In the past CSIS was only allowed to collect the data. Under C51 they were allowed to disrupt terrorist plots. Does that maintain? This is not changing. It's not going back to the original.

Senior Official 1: Not at all.

Question: I need clarification on judicial investigative hearings. Why did you decide to get rid of that other than it had been used once? Why wouldn't you maintain the tool?

Senior Official 3: It had been invoked once but never used. It didn't form part of the consultations but the consultations were unprecedented and took place throughout the fall and as a result of which Ministers and the government took an overall examination of the national security framework as a whole and the measures that are available to law enforcement and came to the view that the investigative hearing was unnecessary given the broad range of anti-terrorism measures and investigative tools available for law enforcement.

Question: Why is it proving so hard to find a long term solution for kids whose names are on the no-fly list?

Senior Official 5: On that one it is a very complex IT situation that we're continuing to look at. One of the key elements that's required is one of the amendments we're bringing to the SEDA (ph) in that we are introducing measures to enable centralized screening against SEDA which means essentially we're going to be allowing Public Safety to electronically screen air passengers against the SEDA list. This is a fundamental first step that we're taking in SEDA.

Question: Why the kids? Why is it so difficult with kids? You say it's an IT problem. What do you mean?

Senior Official 5: To implement or redress a system requires a wide variety of technological steps that need to be entered into. For the children what we are proposing to do is the amendment that the Minister can divulge the information to the parents of the children.

Question: I just wonder why you couldn't have if you're under ten you can't possibly be on the list.

Senior Official 5: It wouldn't solve the close name matches.

Question: Do you not have the birth dates in the system?

Senior Official 5: Those are issues we need to work out with air carriers. Those are part of the technological complex issues.

Question: Amanda Connelly with I Politics. General Vance said two weeks ago the defence policy review came out and the Forces got their new cyber operations mandate that the Forces would not be the ones using cyber to attack a foreign government. That was a direct quote from him.

The active cyber operations component in the CSE Act specifically says that CSE will be able to degrade, disrupt, influence, respond to or interfere with the capabilities of a foreign individual or a state as well. If you're going to be working with them as it says here on cyber operations, is CSE being essentially keyed up into a combat capability against states to work with the military?

Senior Official 2: Two parts to the answer to your question. If you look at what the (unintelligible) is proposing with regard to cyber operations there are two pieces to the puzzle. On the one hand we have an assistance mandate. We've always had an assistance mandate when it comes to law enforcement agencies.

What this act is doing is it's adding the Canadian Armed Forces to that assistance mandate. What that means is commensurate with the defence policy review that was released and the references to cyber operations in that, for military missions under the governance of those military missions, now the Canadian Armed Forces can leverage CSE meaning we have sophisticated tools and capabilities.

They can now leverage us to do cyber operations again similar to when we're assisting law enforcement agencies, we would be doing that under their authority. They would have to get the authority for a military mission. They would look into doing things in cyber space and they can look to leverage us. That's piece number one.

Piece number two the act is also stating that giving CSE the authority to engage in cyber operations that don't have a military nexus or don't start with a military mission, aren't under the purview of a military mission. That is a very serious responsibility and what the act stipulates is that there are very strict legal parameters and a very significant senior government level structure in order to engage in that.

What we would have to do in those circumstances would be to get a ministerial authorization approved by both the Minister of Defence and the Minister of Global Affairs and from there we could then engage in those activities provided they are under the auspices of that ministerial authorization which would then be reviewed by the new review body and benefit from all of the governance, transparency and accountability that comes with it.

Question: I'm having trouble understanding this. The military doesn't even have the mandate to attack a foreign government with cyber operations. Why should CSE?

Senior Official 2: The question of the mandate is blurred. Here I'll give you an example in terms of our mandate as it's being directed in the CSE Act. Let's say a foreign threat actor is attacking Canadian interests in cyber space. Right now under the National Defence Act in our current authorities we would be able to set up a defence against that and block against that.

What that foreign actor could do or threat actor could do is turn around and attack us at a different vector. Then we would set up a shield on that and then we would continue setting up a shield. What the new authorities would allow us to do is to go to the source and shut down the attack where it's happening. We're conscious of the fact that's a very serious responsibility so before we would be able to engage in that activity we would have to get a ministerial authorization approved by two Ministers. Does that answer your question?

Question: Brigitte Bureau de Radio Canada. La GRC et la SRS ont reconnu récemment qu'elles déployaient des IMSI catchers, une technologie très envahissante parce qu'elle est capable de capter non seulement les téléphones mobiles de la personne ciblée mais tous les téléphones mobiles d'une région particulière. Est-ce qu'on prévoit un meilleur encadrement de ce genre de technologie dans le projet de loi qu'on a déposé aujourd'hui ?

Senior Official 1 : Ce n'est pas adressé dans le projet de loi aujourd'hui non.

Question : Pas du tout ? Pourtant quand on a fait la consultation la majorité c'était l'accès aux données numériques ça a été cité comme une des préoccupations, la plus grande préoccupation des gens consultés qui craignaient que des agences puissent avoir accès à leurs données numériques. Il n'y a rien là-dedans qui parle de ça ?

Senior Official 1 :Non, vous avez raison. C'est un sujet qui continue à être une préoccupation principale des Canadiens. Pour l'instant le comité de la Chambre sur la sécurité nationale continue à étudier la situation.

Senior Official 4 :Juste pour le service, l'utilisation de cette technique est présentement suspendue et on fait une révision vu les préoccupations qui ont été soulevées. On continue la révision mais ça ne fait pas partie du projet de loi en tant que tel.

Question:If we had to explain to Canadians what is the biggest single change in this legislation that protects their Charter rights, what would it be?

Senior Official 1:I would say it is the multi layered approach to oversight, accountability, review and transparency.

Question:Once that puts them to sleep, is there an easier way to explain how their rights are protected?

(Laughter)

Senior Official 1:I'm going to try not to put you to sleep. The oversight will be conducted by the commissioner that will pre-approve classes of activities for both CSIS and CSE. Then you will have this new review agency that will now extend to government departments that were previously not being reviewed. You have of course the national security and intelligence committee of Parliamentarians that adds on top of that, so a multi-layered approach of independent oversight, expert review, parliamentary review and you add transparency on top of that where the government intends on making a transparency commitment where –

Question:This is all after the fact, right?

Senior Official 1:Not the commissioner part. The commissioner is before the fact.

Question:What would be the single biggest change that enhances security because a lot of Canadians are concerned about terrorist attacks? We see them every single day. Is there a single biggest change that enhances security?

Senior Official 1:Everything that I mentioned towards the end in the third theme about modernization of both the CSIS Act and introducing a new CSE Act goes exactly to that point.

Question:I wanted to know if the new multi-pronged approach as you described it to oversight will represent a budgetary increase over what existed before and if so how much.

Senior Official 1:The government will make a total investment of approximately \$97.3 million over five years to ensure that the initiatives around accountability, oversight, the review, transparency do have the adequate resources.

Question: How much more does that represent than they're spending now?

Senior Official 1: I would have to get back to you. It does include the current existing funding for SERC and OCSEC. I would have to get back to you on the details this afternoon in terms of the additional portion that represents.

Question: Back to the no-fly list, when you say that the IT problems around a redress system are prohibitive, is it the cost of actually producing that system that's prohibitive or is it the complicated nature of it?

Senior Official 1: The complicated nature, the costs, there are a lot of variables that need to be taken into consideration.

Question:Have you seen an estimate for that cost?

Senior Official 1: I don't think I'm at liberty to answer that one.

Question: D'abord avez-vous – je veux m'assurer qu'est-ce que vous distribuez, vous donnez des informations des données sur les Canadiens aux pays alliés? Je ne suis pas certaine dans votre réponse d'avoir saisi.

Senior Official 2 : On a des mesures en place pour protéger l'information des Canadiens. Ceci dit il va y avoir des cas exceptionnels où il sera nécessaire possiblement de partager une information à propos d'un Canadien et donc la loi explique clairement ce genre de situation et quand le CST a le droit de partager ce genre d'information.

Question : Je voulais vérifier avec vous sur le pouvoir de suspension de perturbation des activités terroristes. Est-ce que vous êtes en mesure de nous dire combien de fois vous l'avez utilisé et est-ce que par le passé vous avez dû obtenir des mandats des tribunaux pour pouvoir le faire parce que cela enfreignait les droits ?

Senior Official 4 : Nous l'avons utilisé à peu près 30 fois plus ou moins, jamais sous mandat. Nous n'avons jamais appliqué pour une demande de mandat.

Question : Donc ce n'était pas nécessaire.

Senior Official 4 : Ce n'est pas pour cette raison-là, pas du tout. C'est parce que nous étions tout de même conscients qu'il y avait des préoccupations au niveau de la façon que la loi était écrite. Donc nous avons décidé d'agir par la prudence. C'était aussi un nouveau type de service. Alors on voulait s'assurer d'avoir une bonne gouvernance en place avant de l'utiliser. Donc c'est pour ces raisons-là que nous avons choisi de prendre une approche plus prudente.

Question : Toutes les limites sont maintenant, les restrictions sont maintenant dans la loi. C'est toutes les façons de faire que vous avez essayées depuis que la loi –

Senior Official 4 : Non, pas nécessairement. Il y en a qu'on a déjà fait oui mais il y en a d'autres qu'on pourrait faire.

Question: In terms of data sets are there new powers here to collect data sets or is it just a balise on the way that data sets are collected, queried, analysed and shared with other countries?

Senior Official 4: No new powers to collect, no. It is as you highlighted a better system to ensure transparency and to ensure our ability to retain the data sets. When it comes to Canadian data sets and we want to retain those data sets we require additional authorization to do that.

Question: Can we expect, given these new rules, that data sets would be CSIS or CSE would be or does CSE do data sets or is it only CSIS?

Senior Official 2: I'm not sure. I think data sets has a very specific connotation when it comes to CSIS, not so much for me. Obviously we're not focused on Canadians. We're focused on foreign. We collect foreign signals intelligence.

Question: In terms of Canadian data sets, can we expect with these new limits for them to be increased or for CSIS to see this as a tool that's now more readily available to do so?

Senior Official 4: I should specify my earlier answer. What is new in terms of the collection of them is the requirement that the Minister must pre-approve the classes of Canadian data sets and the intelligence commissioner needs to validate that authorization as well as approve the retention of foreign data sets.

It obliges that distinction to be made beforehand. We can't retain a data set unless the Minister has agreed that you can retain that specific data set. We always collect because until we collect and analyze we don't always know what we have. I hope that clarifies it.

Question: Under these new rules, can we expect more data sets or CSIS to go a bit more into that field of collecting information on Canadians?

Senior Official 4: I think it's an acknowledgment that technology has evolved and the volume of information has evolved. The threat is global. We have to be in a position to be able to conduct analysis from various informations. I can give you an example.

If we have a foreign data set that could be let's say a voter list in country X and we have information that there is a foreign national in contact with a terrorist suspect in Canada, while our ability to query a foreign data set may help us identify that individual, that requirement in today's mobile world to be able to look at the various data to help us in terms of our investigation of the threat.

Question: Peut-être que cela m'a échappé. Vous avez expliqué mais je voudrais comprendre d'abord il y a la question des propagandes. Vous dites que maintenant ça va être plus resserré. C'est une grande préoccupation avec C51, l'échange d'information entre les ministères, les conditions. Je voudrais savoir s'il y a des dispositions qui viennent resserrer ça.

Lorsque vous parlez de l'organisme de surveillance, je veux bien comprendre il ne remplace pas le comité des plaintes de la GRC. Par contre il va couvrir toutes les instances. Est-ce que c'est une mise en œuvre du rapport Arar ?

Senior Official 1: En ce qui a trait à la loi sur le partage de l'information qui est maintenant la loi sur la communication d'information, les préoccupations ont été apportées par le commissaire à la vie privée auprès du comité de la Chambre des Communes. La manière qu'on propose d'adresser les préoccupations dans le projet de loi c'est de deux manières.

La première c'est d'apporter beaucoup plus de clarté autour de la définition de ce qui représente des activités qui sont menaçantes envers la sécurité du Canada. Donc on ajoute une liste précise de ce genre d'activités qui effectivement sont des menaces à la sécurité du Canada. On rajoute un test autour de ça. Quand un ministère ou une agence possède de l'information que ce ministère ou agence voudrait partager avec une autre entité canadienne, le propriétaire de l'information devrait se poser la question en ce qui a trait à l'utilité de cette information pour le destinataire, l'intégrité de cette information.

En d'autres termes est-ce que l'information est crédible, pertinente ? Troisièmement le test de la vie privée. Donc ce sont les clarifications qu'on apporte à la loi. En ce qui a trait à la GRC, oui, effectivement le comité qui existe actuellement va continuer pour les plaintes mais les plaintes qui ont un lien avec la sécurité nationale vont être travaillées en collaboration avec la nouvelle agence qui va faire les révisions.

Question : Est-ce que ça reflète (off microphone).

Senior Official 1 : Ce qu'on propose c'est que les plaintes en matière de sécurité nationale soient sous le mandat de la nouvelle agence.

Senior Official 5 : Pour ce qui est de votre question cela me fait plaisir de répondre au niveau de la propagande terroriste. La définition en effet se retrouve à être plus étroite. Elle maintenant va englober plutôt une référence. Elle faisait auparavant référence à préconiser ou fomenter la perpétration d'une infraction de terrorisme et maintenant elle va plutôt faire référence à l'infraction de conseiller une infraction de terrorisme.

Elle va de pair avec les modifications qu'on fait à cette infraction de préconiser ou fomenter la perpétration d'une infraction de terrorisme qui elle aussi va maintenant englober plutôt l'infraction plus connue de conseiller. Donc on se débarrasse un peu du terme plus obscur qui était de fomenter et de promouvoir pour le remplacer par le fait de conseiller. J'espère que c'est assez clair.

Moderator: We'll take a question from those joining us by teleconference. Operator, do you have a question on the phone?

Operator: We have a question from Justin Lane from Vice News. Please go ahead.

Question: Just a point of clarification on something that was mentioned before. When we're talking about collecting publicly available data sets for CSIS, you said that would be subject to ministerial oversight by the courts. Obviously that's true but under the act and correct me if I'm wrong, the only qualification for CSIS to retain that information is that it was publicly available when CSIS obtained it.

Are there other qualifications that are missing? I don't see a qualification that needs to pertain to CSIS mandate. Can you be more specific about exactly what sort of steps CSIS has to go through to prove that they're allowed to retain that?

Senior Official 2: Let me clarify that. Anything that the service collects has to be in relation to its mandate. It needs to be strictly necessary to its mandate as defined in the CSIS Act. That's from the get go. What the legislation tries to do or the attempt is to try to address to clarify the authorizations for the various types of data sets.

We will have a technical briefing this afternoon that we can get into it a bit more but in essence it's defining it between foreign, Canadian and publicly available. For Canadian data sets the Minister will authorize the classes of Canadian data sets approved by the intelligence commissioner and if the service wants to retain Canadian data sets it will require a judicial authorization to do so.

It would be restricted to designated employees and any use of that information must be strictly necessary and relevant and pertinent to the duties and functions of CSIS. Foreign data sets, the retention needs to be approved by the new intelligence commissioner, all of this subject to review of course by the new review body. Publicly available data sets are available but again are available to the public but again the service can only utilize them if it is strictly necessary to accomplish our mandate.

Question: Just as a follow up, can you get more specific about CSE's use of publicly available intelligence? They now have that power to collect publicly available intelligence even if it relates to Canadians and also a bit more about the ability for CSE to get into the infrastructure, telecommunications infrastructure if it relates to foreign intelligence.

Senior Official 1: I'm not sure I understand fully. You touched upon three or four different areas of the new act. At the end of the day we continue to have a foreign signals intelligence mandate. We're allowed to collect foreign signals intelligence which is directed at foreigners outside of Canada.

We have to have ministerial authorizations in place to do that. We don't just collect things willy nilly. We collect things based on intelligence priorities set by Cabinet. The ministerial authorizations outline retention periods, outline exactly the classes of activities we engage in to collect that information.

The Minister checks that for reasonableness, necessity, proportionality. Following that now we have the new rule of an intelligence commissioner that will review the Minister's decision for reasonableness before we engage in those activities and then following that those activities will be reviewed for compliance with the law and compliance with the ministerial authorizations. That will be done by the new national security and intelligence review agency and of course we also have the role of the national security intelligence committee of Parliamentarians that will also have a similar role.

That's with regard to foreign signals intelligence collection. The act is a lot more clear in terms of the types of activities we can engage in and how that works. With regard to publicly available data sets we don't use that. I think section 24 states we can look at public information. That's more in line with research, developing tools, testing for vulnerabilities. It falls more under our cyber security and information assurance mandate in terms of looking at public information.

There's obviously public information is something that is already made public. There is no expectation of privacy attached to it. It's not like we're collecting that for the purposes of foreign intelligence. That doesn't fall under our mandate.

Moderator: Before we take our last question in the room, I would remind you that to consult our media advisories for the schedule of more detailed briefings where we'll focus on the particular themes. If you don't have those advisories with you, my media relations colleague can help you with the details of time and how to dial in.

Question: Je voudrais savoir dans la documentation que le CRS croit suffisant aujourd'hui, pouvez-vous donner des exemples concrets des pouvoirs supplémentaires qui vont être lui accordés qui vont faciliter son travail ?

Senior Official 4 : Aucun pouvoir supplémentaire. C'est plutôt une précision dans la loi et des meilleures protections des services. Donc si je prends par exemple le régime d'autorisation, cela identifie dans le nouveau projet de loi que le Ministre pourrait approuver certaines activités qui pourraient être illégales.

Donc je vais vous donner un exemple. Je crois que les Canadiens s'attendent que le service de renseignement puisse enquêter sur des projets d'attentats terroristes avant évidemment qu'ils arrivent. Donc semblable à ce qui existe déjà pour les corps policiers on met en place un régime d'autorisation pour nous permettre de faire quelques activités.

Le simple fait de recruter un individu dans un groupe terroriste pourrait être illégal quand on regarde le Code Criminel et les accusations potentielles sous le terrorisme. Donc c'est une meilleure protection dans la loi avec un régime d'autorisation très détaillé pour nous permettre à continuer à faire ce genre d'activités.

Donc ce que je dirais ce n'est pas les nouveaux pouvoirs mais c'est vraiment plus de transparence, plus de rigueur mais aussi une meilleure précision sur ce que nous faisons.

Question : Je reviens sur la question de ma collègue Julie. Qu'est-ce que ça change pour les Canadiens en termes de la protection de leur vie privée ?

Senior Official 1 : Il y a beaucoup d'éléments dans le projet de loi qui adressent la vie privée des Canadiens. On commence déjà avec les deux premiers nouveaux actes qui créent l'agence de revue, the review agency, la création également du commissaire et ensuite si vous regardez aussi pour le service on rajoute une préambule à la loi sur le service qui reconnaît que le service et en fait toute autre agence de renseignement et de sécurité du Canada doit s'acquiescer de ses tâches dans le respect des lois et de la Charte.

On regarde aussi du côté du changement à la loi du partage d'information, donc au niveau des communications d'information, là encore il y a un seuil à respecter au niveau de la vie privée. On a des changements aussi au the youth criminal protection act, et ainsi de suite. Il y a plusieurs mesures à travers le projet de loi qui continuellement rappellent la nécessité de respecter les droits et libertés des Canadiens ainsi que la Charte.

Moderator: Juste pour dire encore dans quelques instants les Ministres Goodale, Raybould-Wilson, Sajjan et Lebouthillier seront ici pour présenter leurs observations et répondre à vos questions. Thank you so much for your time and attention. We wish you a good afternoon.

-30-

NOTE: TRANSCRIPTS CANNOT BE SHARED OR TRANSFERRED OUTSIDE OF YOUR DEPARTMENT WITHOUT THE CONSENT OF MEDIA Q INC.

Questions? Please contact us at ps.pspmediacentre-centredesmediaspsp.sp@canada.ca
Questions ? Veuillez communiquer avec nous au ps.pspmediacentre-centredesmediaspsp.sp@canada.ca

Sent to: !!INTERNAL; !!INTERNAL 2; CBSA Breaking News; CSIS Breaking News; RCMP Breaking News



PS-017056

Doc date: 22-Juin-2017

File # 18-1370

s.69(1)(g) re (a)

s.69(1)(g) ré (e)

SECRET / Confidence of the Queen's Privy Council (with attachments)

Minister's Briefing Brefpage du ministre

Thursday, June 22, 2017 - 2:00 p.m. to 3:30 p.m. / Le jeudi 22 juin 2017 - 14h00 à 13h30

Minister's Boardroom / Salle de conférence du ministre

AGENDA / ORDRE DU JOUR

| ITEM / POINT | SUBJECT / SUJET | PARTICIPANTS | DURATION / DURÉE | |
|---|----------------------------------|---|------------------|---------------------------|
| 1 | Five Country Ministerial meeting | LEAD / RESPONSABLE | 2:00 | |
| | | Monik Beauregard <i>Senior Assistant Deputy Minister, NCSB</i> | 2:30 (30 min) | |
| | | Adam Green <i>Manager, Policy Development, NCSB</i> | | |
| | | OTHERS / AUTRES | | |
| | | Jill Wherrett <i>A/Assistant Deputy Minister, PACB</i> | | |
| | | Ritu Banerjee <i>Senior Director, Countering Radicalization to Violence, PACB</i> | | |
| | | Peter Hill <i>Associate Vice-President, Programs Branch, CBSA</i> | | |
| | | Jamie Tomlinson <i>Director General, Communications, PACB</i> | | |
| | | <hr/> | | |
| | | 2 | | LEAD / RESPONSABLE |
| Monik Beauregard <i>Senior Assistant Deputy Minister, NCSB</i> | 3:00 (30 min) | | | |
| Colleen Merchant <i>Director General, National Cyber Security Directorate, NCSB</i> | | | | |
| OTHERS / AUTRES | | | | |
| Jamie Tomlinson <i>Director General, Communications, PACB</i> | | | | |
| 3 | First Nations Policing Program | LEAD / RESPONSABLE | 3:00 | |
| | | Kathy Thompson <i>Assistant Deputy Minister, CSCCB</i> | 3:30 (30 min) | |
| | | Annie LeBlanc <i>Director General, Policing Policy Directorate, CSCCB</i> | | |
| | | Kristin Solvason <i>Director, Aboriginal Policing Policy Division, CSCCB</i> | | |
| | | OTHERS / AUTRES | | |
| | | Lori MacDonald <i>Assistant Deputy Minister, EMPB</i> | | |
| | | Bobby Matheson <i>Director General, Programs Directorate, EMPB</i> | | |
| | | Byron Boucher <i>Assistant Commissioner, RCMP</i> | | |
| | | Jamie Tomlinson <i>Director General, Communications, PACB</i> | | |
| | | <hr/> | | |

TAB 1

FIVE COUNTRY MINISTERIAL



Ottawa, Canada
June 26-27, 2017



Unclassified

FIVE COUNTRY MINISTERIAL/ JOINT QUINTET MEETINGS

June 26-27, 2017

Minister of Public Safety Event Binder

Table of Contents

| | |
|---|--------------|
| MASTER SCENARIO NOTE | TAB 1 |
| FCM/Joint Meeting Agenda | Tab 1A |
| Canadian Summary of Session Expected Outcomes | Tab 1B |
| Ministerial Biographies | Tab 1C |
| BILATERAL MEETINGS | TAB 2 |
| Scenario Note: Bilateral Meeting with Christopher Finlayson, N.Z | Tab 2A |
| Scenario Note: Bilateral Meeting with George Brandis, AUS | Tab 2B |
| Scenario Note: Bilateral Meeting with Jeff Sessions, U.S. | Tab 2C |
| Scenario Note: Bilateral Meeting with Peter Dutton, AUS | Tab 2D |
| Scenario Note: Bilateral Meeting with Amber Rudd, U.K. | Tab 2E |
| Scenario Note: Bilateral Meeting with John Kelly, U.S. | Tab 2F |
| SESSION 1: THREAT BRIEFING & COUNTERTERRORISM | TAB 3 |
| Canadian Scenario Note | Tab 3A |
| SESSION 2: COUNTERING VIOLENT EXTREMISM [CAN LEAD] | TAB 4 |
| Canadian CVE background note | Tab 4A |
| Canadian Detailed Scenario Note | Tab 4B |
| FCM Discussion Paper: CVE (CAN) | Tab 4C |
| FCM Annex 1: CVE Action plan overview (CAN) | Tab 4D |
| FCM Annex 2: CVE Action plan (CAN) | Tab 4E |
| FCM Annex 3:  | Tab 4F |
| FCM Annex 4:  | Tab 4G |

SESSION 3: MIGRATION AND REFUGEES **TAB 5**
[UK LEAD]

| | |
|---|--------|
| Canadian Scenario Note | Tab 5A |
| FCM Discussion Paper: [REDACTED] | Tab 5B |
| FCM Annex 1: Canadian Syrian Refugee Resettlement Project (CAN) | Tab 5C |
| FCM Annex 2: Innovation and Border Technology (CAN) | Tab 5D |
| FCM Annex 3: SRTP Dashboard – Migration 5 (formerly FCC) update | Tab 5E |
| FCM Annex 4: [REDACTED] | Tab 5F |

FCM/QUINTET LUNCH **TAB 6**

| | |
|--|--------|
| Canadian Scenario Note | Tab 6A |
| Canadian Lunch Speech | Tab 6B |
| FCM Discussion Paper: National Security Transparency (CAN) | Tab 6C |

SESSION 4 (JOINT): SECURITY COOPERATION & LAW ENFORCEMENT **TAB 7**
[US AND UK LEAD]

| | |
|----------------------------------|--------|
| Canadian Scenario Note | Tab 7A |
| FCM Discussion Paper: [REDACTED] | Tab 7B |
| FCM ANNEX 1: [REDACTED] | Tab 7C |

SESSION 5 (JOINT): CYBER SECURITY & ENCRYPTION **TAB 8**
[AUS LEAD]

| | |
|---|--------|
| Canadian Scenario Note | Tab 8A |
| FCM Discussion Paper: [REDACTED] | Tab 8B |
| FCM ANNEX 1: Quintet Experts Working Group on Cybercrime – Encryption [REDACTED] | Tab 8C |
| FCM Discussion Paper: Cyber Security (CAN) | Tab 8D |

| | |
|--|---------------|
| DRAFT JOINT COMMUNIQUÉ | TAB 9 |
| CLOSING REMARKS | TAB 10 |
| JOINT RECEPTION/DINNER | TAB 11 |
| Schedule and Participants | Tab 11A |
| Diplomats Biographies | Tab 11B |
| Floor Plan | Tab 11C |
| Canadian Toast | Tab 11D |
| | |
| ANNEX A: FINAL OUTCOMES 2016 & PROGRESS CHART FCM 2017 | TAB 12 |
| ANNEX B: FIVE EYES FORUMS CHART | TAB 13 |
| ANNEX C: COMMUNICATIONS PLAN SUMMARY | TAB 14 |
| ANNEX D: LETTERS FROM MIGRATION 5 AND AUSTRALIA ON FCM 2017 | TAB 15 |
| ANNEX E: FCM AGENDA & SUMMARY OF SESSIONS PAGEMARK | TAB 16 |

Tab 1



Public Safety Sécurité publique
Canada Canada

Deputy Minister Sous-ministre

Ottawa, Canada
K1A 0P8

For your meeting with:
SUBJECT: Five Country Ministerial
DATE: June 26-27, 2017
LOCATION: Ottawa

UNCLASSIFIED

DATE: Friday, June 9, 2017

RDIMS No.: 2260008

MASTER SCENARIO NOTE

**HOSTING INTERNATIONAL MINISTERS IN OTTAWA
FIVE COUNTRY MINISTERIAL**

(Information only)

SUMMARY

You will be hosting the Five Country Ministerial (FCM) in Ottawa on June 26-27, 2017. At the Ministerial, your Canadian counterparts will be:

- Honourable Jody Wilson-Raybould, Minister of Justice and Attorney General of Canada (**co-host**);
- Honourable Ahmed Hussen, Minister of Immigration, Refugees and Citizenship.

The other international Ministers in attendance will be:

- Honourable George Brandis, Attorney-General, Australia;
- Honourable Peter Dutton, Minister for Immigration, Australia;
- Honourable Christopher Finlayson, Attorney-General, New Zealand;
- Honourable Michael Woodhouse, Minister of Immigration, New Zealand;
- Right Honourable Amber Rudd, Home Secretary, UK;
- John Kelly, Secretary of Homeland Security, U.S.;
- Jeff Sessions, Attorney General, U.S.

You will also be accompanied and supported by:

- Marci Surkes, Office of the Minister
- David Herle, Office of the Minister
- Malcolm Brown, Deputy Minister
- John Ossowski, CBSA President
- Monik Beauregard, Senior Assistant Deputy Minister
- Jill Wherrett, Assistant Deputy Minister

UNCLASSIFIED

- 2 -

The full agenda for the FCM/Joint session is attached (**TAB 1A**), as are a summary of the discussions on June 26th (**TAB 1B**), and the Ministerial Biographies (**Tab 1C**).

SUNDAY, JUNE 25

On the day before the official conference proceedings, there will be opportunities to meet bilaterally with your international counterparts as they arrive in Ottawa. You will meet with New Zealand Attorney-General Christopher Finlayson (Scenario Note at **TAB 2A**) in the afternoon at the Fairmont Chateau Laurier. Your complete bilateral meeting schedule is included in **TAB 2**.

MONDAY, JUNE 26

The Five Eyes (FVEY) community, consisting of Canada, Australia, New Zealand, the United Kingdom and the United States, is one of the most established intelligence-sharing groups in the world. The Five Country Ministerial (FCM) was created as the ministerial forum to discuss policies, operational approaches and legal measures on a range of public safety and security issues. The first meeting took place in Monterey, California, in 2013; subsequent meetings took place in London (2015) and Washington, D.C. (2016). Your participation in the FCM marks the fourth time Canada participates in this forum, and the first time it will be hosted in Canada. The FCM will coincide with the Quintet of FVEY Attorneys General, hosted by your colleague, the Honourable Jody Wilson-Raybould. While the morning of the first day of the ministerial (June 26) is specific to the FCM Ministers, a joint session with the Quintet will be held in the afternoon.

In the morning, you will proceed to the headquarters of the Canadian Security Intelligence Service (CSIS), where you will meet your FCM counterparts for the formal conference proceedings.

The briefing material in this binder covers the following:

- **Session I:** A scenario note for the opening forum (**TAB 3A**), which will include a threat briefing and a discussion about counterterrorism and national security issues that will help frame the rest of the day. You will open the session by delivering opening remarks and introducing your ministerial counterparts.

For each of the following sessions, you are provided with a Canadian Scenario note containing sequencing, and talking points; an FCM Discussion paper, which all five countries have approved as the basis of conversation for this session and; additional annexes providing background papers relevant to each session.

- **Session II:** Countering Violent Extremism (**TAB 4**): you are leading the discussion on this topic. A background note (**TAB 4A**) as well as a detailed scenario note (**TAB 4B**) including all your talking points are provided.

UNCLASSIFIED

- 3 -

- **Session III:** Refugees and Migration (**TAB 5**) will be led by the UK. Your colleague, Minister Hussen will lead the majority of Canadian response, and you will be expected to lead the sub-discussion concerning border technology.
- **FCM/Joint Lunch session:** Scenario note (**TAB 6A**) and scripted speech (**TAB 6B**) are provided for you to lead an informal discussion on transparency and accountability in national security (**TAB 6**).
- **Session IV:** Security and Cooperation (Joint session with Quintet) (**TAB 7**) will be led by the U.S. You will lead the Canadian response.

In the break between these sessions, Ministers will be asked to join in taking a "family photo".

- **Session V:** Cyber Security and Encryption (Joint session with Quintet) will be led by Australia for the Encryption topic, and by Canada on cyber security. (**TAB 8**) Your colleague Minister Wilson-Raybould will lead the Canadian response to Encryption, and you will lead the discussion on Cyber security.
- **Joint Communiqué (TAB 9):** You will chair a short discussion on satisfaction with the proposed joint communiqué.
- **Closing Remarks:** You will deliver remarks to close the conference (**TAB 10**).

Following the conclusion of the day's meetings, you are scheduled to remain at CSIS to meet bilaterally with Australian Attorney-General George Brandis (Scenario Note at **TAB 2B**). You are subsequently scheduled to meet bilaterally with United States Attorney General Jeff Sessions (Scenario Note at **TAB 2C**).

You are then scheduled to travel to the FCM/Quintet reception and dinner at the Sir John A Macdonald building in the parliamentary precinct. The Ministers and their delegations will be at this event; the Heads of Diplomatic Mission of the four FVEY partners will also attend. Further information about the dinner is included (**TAB 11**).

TUESDAY, JUNE 27

This day is reserved for the meeting of the Quintet of Attorneys General, hosted by the Honourable Jody Wilson-Raybould. In the morning, you are scheduled to meet bilaterally with the Australian Minister of Immigration Peter Dutton (**TAB 2D**), UK Home Secretary Amber Rudd (**TAB 2E**), and United States Secretary of Homeland Security John Kelly (Scenario Note at **TAB 2F**).

COMMUNICATIONS

The Communications Branch of Public Safety Canada will issue a joint news release with counterparts from the Departments of Justice and Immigration, Refugees, and Citizenship, on June 27. A summary of the communications plan is included (**TAB 14**).

UNCLASSIFIED

- 4 -

A policy-led joint communiqué will also be released by Public Safety Canada at the conclusion of the conference. **(TAB 9)**

REFERENCE

On the final page of this binder, you will find a reference agenda and session outcomes summary, which you can use as a pagemark throughout the day.

Should you require additional information, please do not hesitate to contact me or Ms. Monik Beauregard, Senior Assistant Deputy Minister, National and Cyber Security Branch, at 613-990-4967.

Malcolm Brown
Deputy Minister of Public Safety

Tab 1A

FOR OFFICIAL USE ONLY
FIVE COUNTRY
MINISTERIAL

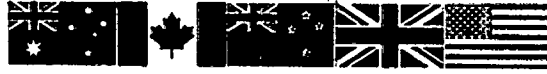


FCM 2017 & FCM/Quintet Joint meeting: Detailed Schedule

| TIMING | | MINISTERS ARRIVAL : June 25 |
|---|--|--|
| Afternoon | | <i>Bilateral Meetings (Fairmont Château Laurier)</i> |
| CONFERENCE DAY 1: June 26 (CSIS HQ, Ottawa) | | |
| FCM Plenary | | |
| 8:00 – 9:30 | SESSION 1: Intelligence Briefing / Counterterrorism (CAN) <ul style="list-style-type: none"> - Ministerial Introductions (CAN - ALL) - Threat briefing (CAN - Intelligence assessors) - [REDACTED] | |
| 9:30 – 10:45 | SESSION 2: Countering Violent Extremism (CAN) <ul style="list-style-type: none"> - Action plan (CAN) - [REDACTED] - [REDACTED] | |
| 10:45-11:00 | <i>Health break</i> | |
| 11:00 – 12:00 | SESSION 3: Refugees & Migration (UK) <ul style="list-style-type: none"> - [REDACTED] - Refugees/Screening (CAN-AUS) - Border Technology (CAN) | |
| 12:15 – 13:30 | FCM Lunch <ul style="list-style-type: none"> - <i>Served lunch for Ministers and Attorneys General in Director Boardroom</i> <li style="padding-left: 40px;"><i>Discussion on Transparency/Accountability (CAN)</i> - <i>Buffet-style lunch for other members of delegation in Lounge area</i> | |
| FCM/QUINTET JOINT MEETING | | |
| 13:45-15:00 | SESSION 4: Security Cooperation & Law Enforcement (US) <ul style="list-style-type: none"> - [REDACTED] - [REDACTED] | |
| 15:00 – 15:15 | <i>Health break – Family Photo</i> | |

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



| | |
|---------------|---|
| 15:15 – 16:30 | SESSION 5: Encryption & Cyber Security (AUS) <ul style="list-style-type: none"> - [REDACTED] - Cyber security / Response to Critical Cyber Incident (CAN) |
| 16:30 – 17:00 | Conclusion <ul style="list-style-type: none"> - Communique Agreement (ALL) - Closing Remarks (CAN) |
| 17:00 – 18:30 | <i>Bilateral Meetings (CSIS HQ or Fairmont)</i> |
| 19:30 – 22:00 | Reception and Dinner (Sir John A. Macdonald Building) |
| TIMING | CONFERENCE DAY 2: June 27 (Fairmont Chateau Laurier Hotel) |
| 8:30 – 12:00 | <i>Bilateral Meetings (Fairmont Château Laurier)</i> |
| 9:00 – 17:00 | Quintet Plenary <i>(see Quintet Draft Agenda)</i> |

Tab 1B

FOR OFFICE USE ONLY

FINAL VERSION

FIVE COUNTRY
MINISTERIAL



FCM/JOINT 2017: SESSION OUTCOME SUMMARY

FCM PLENARY SESSIONS

SESSION 1: Intelligence Briefing / Counterterrorism (CAN)

Intelligence assessors led by CSIS are currently working on Top Secret briefing.

SESSION 2: Countering Violent Extremism (CAN)

The FCM will discuss

- 1) [REDACTED] Introduce Canada's efforts at CVE.
- 2) Engagement with communications service providers to enhance efforts to counter online radicalization: [REDACTED]
- 3) Returning foreign fighters and their families: Consider how to mitigate potential threats from foreign terrorist fighters; strengthen research partnerships to study radicalization. [REDACTED]
- 4) [REDACTED]

SESSION 3: Refugees & Migration (UK)

The FCM will support international negotiations on immigration enforcement and increase cooperation between FVEY partners on border technology and migrant screening.

- 4) Canada's Lessons Learned: Ministers to take note of Canada's Lessons Learned Paper on Operation Syrian Refugees.

FCM/QUINTET JOINT SESSIONS

SESSION 4: Security Cooperation & Law Enforcement (US)

The FCM and Quintet will consider ways to improve information sharing for national security and law enforcement.

- 1) [REDACTED]
- 2) [REDACTED]
- 3) [REDACTED]
- 4) [REDACTED]

FIVE COUNTRY

SESSION 5: Encryption & Cyber Security (AUS)

The FCM and Quintet will develop a common approach (pursued individually) for engaging with communications service providers in the context of encryption and law enforcement.

Encryption:

[Redacted]

Cyber Security:

[Redacted]

Other potential topics of discussion:

Transparency/Accountability:

[Redacted]

Tab 1C



BIOGRAPHY

Senator the Hon George Brandis QC
Attorney General of Australia

Senator the Hon George Brandis QC was born in Sydney, Australia and grew up in Brisbane. He was educated at the University of Queensland (from which he graduated with first class honours in Arts and Law) and Magdalen College, Oxford, where he obtained a Bachelor of Civil Law.

On his return from the United Kingdom, Senator Brandis worked as a lawyer at Minter Ellison before going to the Bar in 1985. He established a successful commercial practice specializing in equity and trade practices law. He “took silk” (was appointed as Queen’s Counsel) in 2006. He was for several years a part-time lecturer in Jurisprudence at the University of Queensland Law School.

Senator Brandis was selected to fill a casual Senate vacancy in May 2000, representing the state of Queensland. He was re-elected in 2004 and 2010 and 2016. He is a member of the Liberal Party of Australia.

Senator Brandis has served as a Minister in the Howard, Abbott and Turnbull governments. He has held the portfolios of Attorney General and Vice-President of the Executive Council since September 2013.

A member of the Liberal Party’s Leadership Group since May 2010, Senator Brandis was appointed Leader of the Government in the Senate in September 2015.



BIOGRAPHY

Peter Dutton

**Australian Minister for
Immigration and Border
Protection**

Peter was elected as the Federal Member for Dickson in Queensland in November 2001 when, at the age of 30 he defeated Cheryl Kernot.

Peter was re-elected with an increased majority in 2004 and appointed Minister for Workforce Participation, with responsibility for the Job Network, Disability Employment Services, Work for the Dole and improving transition to work opportunities for all unemployed Australians.

At the time of his appointment Peter was one of the youngest Minister's since Federation.

In January 2006 Peter was promoted to Minister for Revenue and Assistant Treasurer. He worked closely with Peter Costello in areas including budget preparation, taxation, superannuation, prudential regulation, and competition and consumer policy.

Following his re-election in November 2007, and with the change of Government, Peter was promoted to Shadow Cabinet as Minister for Finance, Competition Policy and Deregulation. In September 2008 he was promoted to the position of Shadow Minister for Health and Ageing.

On the 18th of September 2013, Peter was sworn in as the Minister for Health and Minister for Sport in the newly elected Abbott Government. On the 21st of December 2014, it was announced that Peter would be appointed as the new Minister for Immigration and Border Protection. He was sworn in on the 23rd of December 2014.

Prior to being elected to Parliament, Peter owned businesses and employed over 40 staff. He started his working life at 12 - delivering newspapers, mowing lawns and working after school as a butcher's boy - a job he continued until starting university. He purchased his first property at 18.

Peter went on to complete a Bachelors degree in Business and was a police officer for 9 years, working in the Sex Offenders Squad, Drug Squad, and the then National Crime Authority. He left the police in 1999 to manage his business interests full time.

Peter's mother grew up at Albany Creek, where the Leitch family was a pioneering family first settling and establishing a dairy farm in the 1860s. Peter is married to Kirilly and is the proud father of three young children: Rebecca, Harry and Tom.



BIOGRAPHY

Ahmed D. Hussen

**Minister of Immigration,
Refugees and Citizenship**

Ahmed Hussen is the Member of Parliament for the riding of York South-Weston. A lawyer and social activist, he has a proven track record of leadership and community empowerment.

Born and raised in Somalia, Ahmed immigrated to Canada in 1993 where he settled in Regent Park and quickly gravitated towards public service. In 2002, he co-founded the Regent Park Community Council and was able to secure a \$500 million revitalization project for Regent Park, all while ensuring the interests of the area's nearly 15,000 residents were protected. Ahmed also served as the National President of the Canadian Somali Congress – a Somali community organization that works with national and regional authorities to advocate on issues of importance to Canadians of Somali heritage and strengthen civic engagement and integration. His results-driven reputation led to an invitation to join the task force for modernizing income security for adults in the Toronto City Summit Alliance.

Ahmed is fluent in English, Somali, and Swahili, and earned his Bachelor of Arts (History) from York University and his Law Degree from the University of Ottawa. In 2004, the Toronto Star recognized him as one of ten individuals in Toronto to have made substantial contributions to his community.



BIOGRAPHY

Jody Wilson-Raybould

**Minister of Justice and Attorney
General of Canada**

Jody Wilson-Raybould is a lawyer, advocate, and leader among British Columbia's First Nations. As a former Regional Chief of the BC Assembly of First Nations, Jody brings extensive experience in law, public service, and First Nations governance to Cabinet.

After being called to the Bar in 2000, Jody began her legal career working as a provincial crown prosecutor in Vancouver. She later served as an advisor at the BC Treaty Commission, a body established to oversee treaty negotiations between First Nations and the Crown. In 2004, Jody was elected as Commissioner by the Chiefs of the First Nations Summit.

Since being elected Regional Chief of the BC Assembly of First Nations in 2009, Jody has devoted herself to the advancement of First Nations governance, fair access to land and resources, as well as improved education and health care services. She was re-elected as Regional Chief in 2012 and held responsibilities for governance and nation building on the Assembly of First Nations Executive. She has previously been involved with the Chiefs Committee on Claims and chaired the Comprehensive Claims joint working group.

An active volunteer in her community, Jody has served as a Director for Capilano College, the Minerva Foundation for BC Women, the Nuyumbalees Cultural Centre, and the National Centre for First Nations Governance. She was also a director on the First Nations Lands Advisory Board and Chair of the First Nations Finance Authority. She is the recipient of the alumni award from the Minerva Foundation and the University of Victoria.

Jody is a descendant of the Musgamagw Tsawataineuk and Laich-Kwil-Tach peoples, which are part of the Kwakwaka'wakw and also known as the Kwak'wala speaking peoples. She is a member of the We Wai Kai Nation and is married to Dr. Tim Raybould.

BIOGRAPHY

Christopher Finlayson

Attorney General of New Zealand



The Honourable Christopher Finlayson is Attorney-General for New Zealand. He is also the Minister for Arts, Culture and Heritage and Minister for Treaty of Waitangi Negotiations.

He is also the Minister in Charge of the New Zealand Security Intelligence Service, the Minister Responsible for the Government Communications Security Bureau (GCSB) and the Associate Minister of Māori Development.

Chris was born in Wellington in 1956 and attended Victoria University, graduating with a Bachelor of Arts in French and Latin and a Masters of Law. He practised law in Wellington for 25 years, where he was a partner at Bell Gully from 1990 – 2002 and thereafter a barrister sole.

He entered Parliament in 2005 as a National Party Member of Parliament.

Before entering Parliament, Chris represented clients in all of New Zealand's Courts and Tribunals, including nine appearances in the Privy Council. For many years he maintained his links to academic life through part-time teaching at Victoria University's Law Faculty. He continues to sit on the Rules Committee of the High Court, which regulates court procedures in New Zealand.

Chris served on the board of Creative New Zealand for six years and chaired the Arts Board from 1998 - 2001. He was also a Trustee of the New Zealand Symphony Orchestra Foundation and a number of other arts organisations. He is well-known for his sponsorship of the arts. He previously served as the Minister for Arts, Culture and Heritage from 2008 to 2011.



BIOGRAPHY

Michael Woodhouse

New Zealand Minister of Immigration

Michael was first elected to Parliament in 2008 as a National List MP based in Dunedin. During his first term in Parliament, he was a member of the Transport and Industrial Relations select committee, the Health select committee and the Finance and Expenditure select committee. Following the 2011 General Election, Michael was made the Senior Government Whip – a position he held until his appointment as Minister of Immigration, Minister of Veterans' Affairs and Associate Minister of Transport in January 2013. In May 2014, Michael was also appointed Minister for Land Information.

After the 2014 General Election, Michael was reappointed Minister of Immigration and appointed Minister of Police and Workplace Relations and Safety. In December 2015, he gained the Revenue portfolio in place of Police. In December 2016, Michael gained the ACC portfolio in place of Revenue. Minister Woodhouse was appointed Deputy Leader of the House in May 2017.

Before being elected to Parliament in 2008, Michael was the Chief Executive Officer of Mercy Hospital Dunedin, a position he held for 7 ½ years. Prior to that Michael held senior management positions with ACC, where he was instrumental in implementing ACC's Elective Services Contracting framework and at Dunedin Hospital in change management, revenue and planning roles.

Michael was educated at St Pauls High School (now Kavanagh College) in Dunedin and graduated from the University of Otago with a Bachelor of Commerce degree. He is a Chartered Accountant and also has a Master of Health Administration from the University of New South Wales.

Michael is a former President of the NZ Private Surgical Hospitals Association and has also been the Vice President of the NZ Private Hospitals Association, a larger organisation which included the private aged care sector. He is also a Fellow of the New Zealand Institute of Management.

Michael is an honorary Rotarian and is active in community and voluntary work in the Otago region. He is an avid rugby fan, having played age group representative rugby for Otago and South Island teams and a premier grade referee, as well as a "fair weather" runner. Michael is married and has three daughters.



BIOGRAPHY

Amber Rudd

**Secretary of State for the UK
Home Department**

Amber Rudd was appointed Home Secretary on 13 July 2016, and re-appointed on June 11, 2016. She was elected Conservative MP for Hastings and Rye in 2010.

From 2010 to 2012 she was a member of the Environment, Food and Rural Affairs Select Committee. She then served as Parliamentary Private Secretary to the Chancellor of the Exchequer from 2012 to 2013, and as Assistant Whip from October 2013.

Amber was the Parliamentary Under Secretary of State at the Department of Energy and Climate Change from July 2014 until May 2015. She was then Secretary of State for Energy and Climate Change from May 2015 until July 2016.

Graduating from the University of Edinburgh with a degree in history, Amber worked in investment banking in the City of London and New York, before moving into venture capital. She then set up a freelance recruitment business and wrote for financial publications, before being elected to Parliament in May 2010.



BIOGRAPHY

John F. Kelly

**US Secretary of Homeland
Security**

Secretary Kelly was born and raised in Boston, Massachusetts. He enlisted in the Marine Corps in 1970, and was discharged as a sergeant in 1972, after serving in an infantry company with the 2nd Marine Division, Camp Lejeune, North Carolina. Following graduation from the University of Massachusetts in 1976, he was commissioned an Officer of Marines.

As an officer, Secretary Kelly served in a number of command, staff and school. He also served as the Special Assistant to the Supreme Allied Commander, Europe, in Mons, Belgium.

He returned to the United States in 2001, and was assigned duty as the Assistant Chief of Staff G-3 with the 2nd Marine Division. In 2002, selected to the rank of Brigadier General, Secretary Kelly again served with the 1st Marine Division, this time as the Assistant Division Commander. Much of the next two years was spent deployed fighting in Iraq. He then returned to Headquarters Marine Corps as the Legislative Assistant to the Commandant from 2004 to 2007. Promoted to Major General, he returned to Camp Pendleton as the Commanding General, I Marine Expeditionary Force (Forward). The command deployed to Iraq in early 2008 for a year-long mission as Multinational Force-West in Al Anbar and western Ninewa provinces. After rotating home and being confirmed as a Lieutenant General he commanded Marine Forces Reserve and Marine Forces North from October 2009 to March 2011. He then served as the Senior Military Assistant to two Secretaries of Defense, Messrs. Gates and Panetta, from March 2011 to October 2012 before being nominated for a fourth star and command of the United States Southern Command (SOUTHCOM), a position he held until January 2016.

During his 39 months in command of SOUTHCOM he worked closely with the remarkable men and women of U.S. law enforcement, particularly the FBI and DEA. He also worked intimately with Secretary of Homeland Security Jeh Johnson and the staff of the Department of Homeland Security, particularly in deterring threats against the U.S. homeland that flow along the trans-national criminal networks into the U.S. from the south. This relationship was a model of interagency cooperation and effectiveness.

After less than a year in retirement Secretary Kelly was offered the opportunity to serve the nation and its people again, now as the Secretary of Homeland Security. The U.S. Senate gave him and his family the great honor of confirming him on January 20, 2017 and he was immediately sworn in as the fifth Secretary of Homeland Security.



BIOGRAPHY

Jeff Sessions

**Attorney General of the
United States**

Jeff Sessions was sworn in as the 84th Attorney General of the United States on February 9, 2017 by Michael R. Pence. President Donald J. Trump announced his intention to nominate Mr. Sessions on November 18, 2016.

Prior to becoming Attorney General, Mr. Sessions served as a United States Senator for Alabama since 1996. As a United States Senator, he focused his energies on maintaining a strong military, upholding the rule of law, limiting the role of government, and providing tax relief to stimulate economic growth and to empower Americans to keep more of their hard-earned money.

Mr. Sessions was born in Selma, Alabama on December 24, 1946, and grew up in Hybart, the son of a country store owner. Growing up in the country, Sessions was instilled with certain core values – honesty, hard work, belief in God and parental respect – that define him today. In 1964, he became an Eagle Scout and thereafter received the Distinguished Eagle Scout Award. After attending school in nearby Camden, Sessions attended Huntingdon College in Montgomery, graduating with a Bachelor of Arts degree in 1969. He received a Juris Doctorate degree from the University of Alabama in 1973. Sessions served in the United States Army Reserve from 1973 to 1986, ultimately attaining the rank of Captain. He still considers that period to be one of the most rewarding chapters of his life.

Sessions' interest in the law led to a distinguished legal career, first as a practicing attorney in Russellville, Alabama, and then in Mobile. Following a two-year stint as Assistant United States Attorney for the Southern District of Alabama (1975-1977), Sessions was nominated by President Reagan in 1981 and confirmed by the Senate to serve as the United States Attorney for the Southern District of Alabama, a position he held for 12 years. Sessions was elected Alabama Attorney General in 1995, serving as the State's chief legal officer until 1996, when he entered the United States Senate.

Sessions and his wife, Mary Blackshear Sessions, originally of Gadsden, Alabama, have three children, Mary Abigail Reinhardt, Ruth Sessions Walk, and Sam. They have seven granddaughters, Jane Ritchie, Alexa, Gracie, Sophia, Hannah, Joanna, and Phoebe, and three grandsons, Jim Beau, Lewis, and Nicholas.

Tab 2

FOR OFFICIAL USE ONLY

Five Country Ministerial Bilateral Meetings Schedule

| Date | Time | Bilateral Meetings | Location |
|------------------------|--------------------------|---|--|
| Sunday, June 25, 2017 | 2:00 p.m. to 2:30 p.m. | Christopher Finlayson, Attorney General, New Zealand | MacDonald Room, Fairmont Château Laurier |
| Monday June 26, 2017 | 5:00 p.m. to 5:30 p.m. | George Brandis, Attorney General, Australia | CSIS, Room 1 |
| Monday June 26, 2017 | 5:30 p.m. to 6:00 p.m. | Jeff Sessions, Attorney General, United States of America | CSIS, Room 3 |
| Tuesday, June 27, 2017 | 8:00 a.m. to 8:30 a.m. | Peter Dutton, Minister for Immigration and Border Protection, Australia | L'Orangerie Room, Fairmont Château Laurier |
| Tuesday, June 27, 2017 | 8:30 a.m. to 9:00 a.m. | Amber Rudd, Secretary of State for the Home office, United Kingdom | Burgundy Room, Fairmont Château Laurier |
| Tuesday, June 27, 2017 | 11:00 a.m. to 11:30 a.m. | John F. Kelly, Secretary of Homeland Security, United States | L'Orangerie Room, Fairmont Château Laurier |

Tab 2A



UNCLASSIFIED

SCENARIO NOTE FOR THE MINISTER

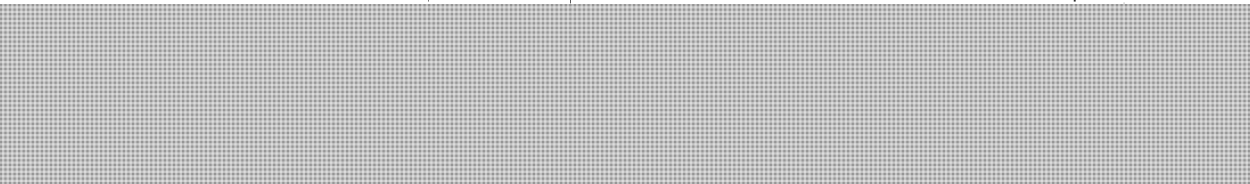
BILATERAL MEETING WITH CHRISTOPHER FINLAYSON (NEW ZEALAND)

Issue

You are scheduled for a 30-minute bilateral meeting with Christopher Finlayson, New Zealand Attorney General, Minister in Charge of the New Zealand Secret Intelligence Service (NZSIS) and Minister Responsible for the Government Communications Security Bureau (GCSB).

You previously met Attorney-General Finlayson during the last FCM. This meeting will be an opportunity to discuss national security and national oversight, given notable interest from New Zealand in Canada's newly-tabled legislation, as well as to preview issues of mutual interest during tomorrow's sessions. This note is intended to supplement detailed briefings that you will receive for your participation in the Five Country Ministerial plenary sessions.

National Security Oversight and Legislative Framework



Attorney-General Finlayson will be eager to understand the changes to Canada's accountability framework, including transparency, information sharing and oversight, as well as timing of when the legislation could be enacted.

The New Zealand Intelligence Community consists of three agencies: the New Zealand Secret Intelligence Service (NZSIS); the Government Communications Security Bureau (GCSB); and the National Assessments Bureau (NAB). The NZIS is CSIS' counterpart.



Review of New Zealand's intelligence community is performed, in part, by its Intelligence and Security Committee, a parliamentary committee that examines, among other things, the policy, administration, and expenditure of each of New Zealand's intelligence agencies.

New Zealand recently completed a reform of its intelligence and security legislation. New Zealand's legislation, however, explicitly precludes this committee from reviewing the operations of intelligence agencies, and the committee does not have authority to review sensitive information, unless explicitly authorized by the Prime Minister. You may wish to ask how the new legislation was received by the public.



UNCLASSIFIED

Cyber security

New Zealand adopted a new Cyber Security Strategy in 2015 that centres on four goals; cyber resilience; cyber capability; addressing cybercrime; and international cooperation. In April 2017, New Zealand's national computer emergency response team officially opened with the mandate to monitor, track and advise on cyber incidents.

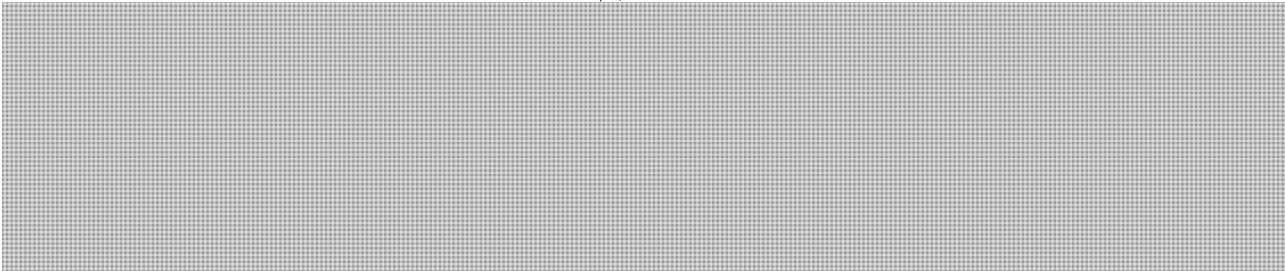
Canada has undertaken a Cyber Review to take stock of the evolving threats in cyberspace, to understand and explore the ways that cyber security is becoming a driver of economic prosperity, and to determine the appropriate federal role in this digital age.



discussions around cyber cooperation will take place under the cyber session of the joint FCM/Quintet.

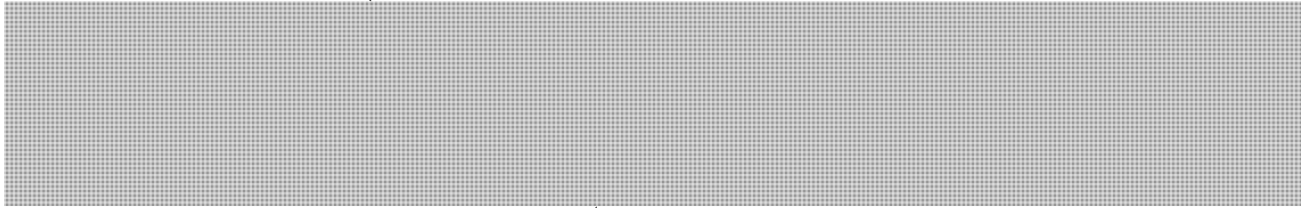
At the June 2017 meeting of the Ottawa 5 in Australia, Principals discussed domestic legislative and policy frameworks and examined responses to real world examples. Current Ottawa 5 priorities include: improving the collective understanding of the activities of key cyber actors; sharing information on collective cyber incident responses (including through joint exercises); and improving and collective understanding of cyber aspects of export control issues.

Emergency Management



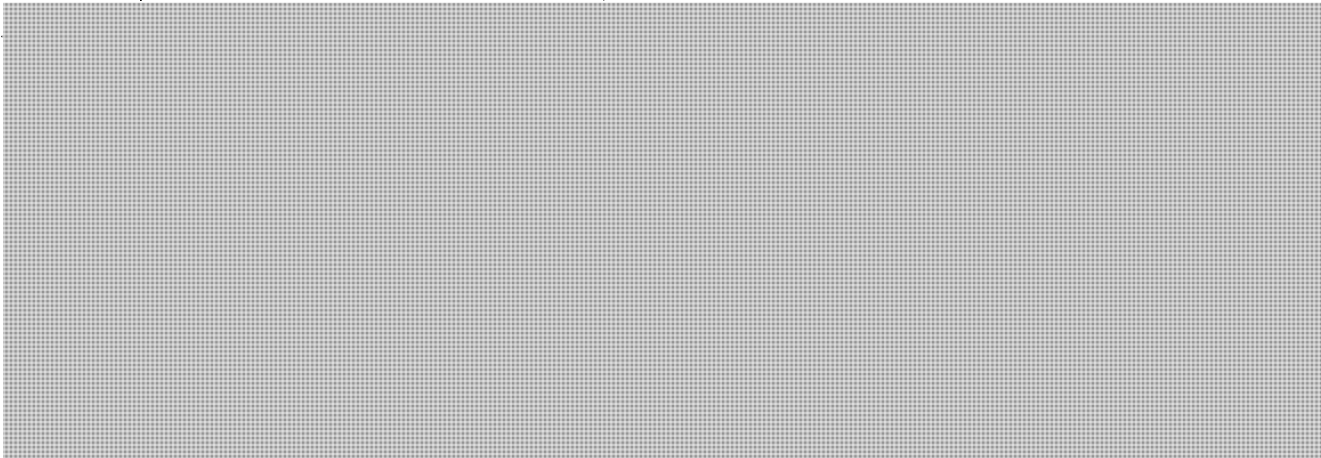
Law Enforcement Information Sharing

Enhanced law enforcement information sharing will be part of a joint FCM session. Should Attorney-General Finlayson wish to discuss this issue, you may wish to highlight the need to consider privacy and data protection requirements.





UNCLASSIFIED



Tab 2B



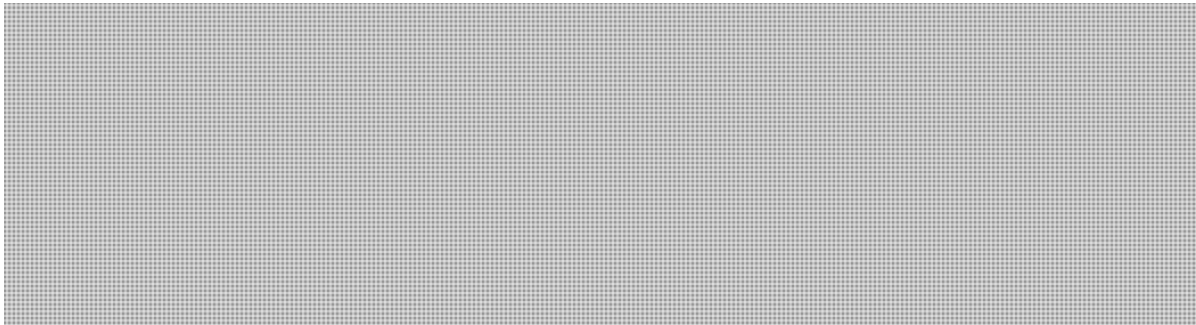
UNCLASSIFIED

SCENARIO NOTE FOR THE MINISTER

BILATERAL MEETING WITH GEORGE BRANDIS (AUSTRALIA)

Issue

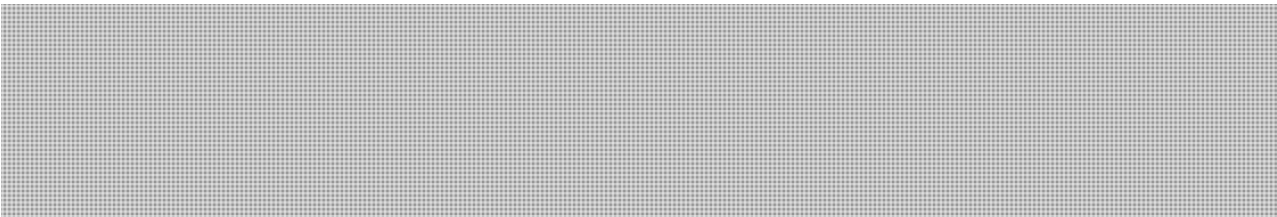
You are scheduled for a 30 minute bilateral meeting with Australia's Attorney General (AG), Senator George Brandis.



Australia has experienced a spate of attacks by radicalized individuals with the most recent being a Daesh-claimed attack in Melbourne on June 5, 2017, which left one person dead. More than 110 Australians are believed to have travelled to Iraq and Syria to fight alongside violent extremist organizations, specifically Daesh. There are roughly 40 Australians who have returned to the country after participating in hostilities in Iraq and Syria, with only two prosecuted.

Potential Discussion Topics

Encryption



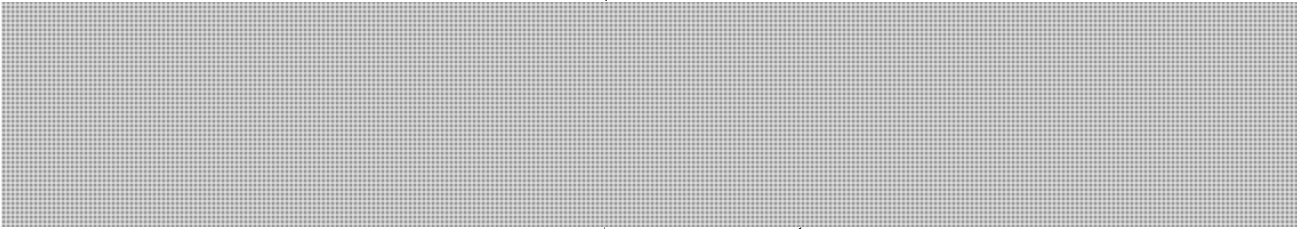
Key Message

In Canada's view, while encryption poses challenges for Canadian law enforcement investigators, it also safeguards our cybersecurity and our fundamental rights and freedoms. Canada has no intention of undermining the security of the internet by impeding the use of encryption.



UNCLASSIFIED

Overview of the new national security legislation



Key Messages

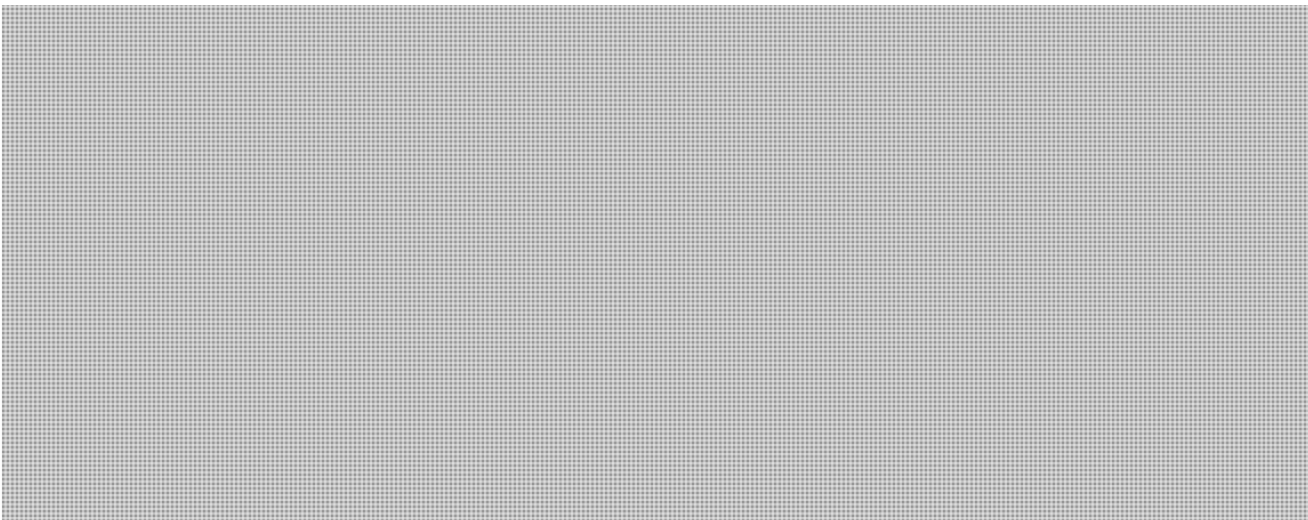
Canada will continue to work closely on national security issues with Australian counterparts so that we can both keep our citizens safe in a manner that safeguards their rights and freedoms.

Transparency and accountability in the context of this legislation means building a better relationship with citizens and raising awareness of the intelligence community's work in enhancing security.

Cyber security

Australia released its renewed cyber security strategy in April 2016, with priorities including developing a national cyber partnership, creating strong cyber defences, enhancing global responsibility and influence, stimulating growth and innovation, and creating a cyber-smart nation.

Australia will lead discussions on cybersecurity and encryption, including encryption and engaging with computer service providers at Monday's Five Country Ministerial plenary session.



s.15(1) - Int'l

s.21(1)(a)



Public Safety
Canada

Sécurité publique
Canada

UNCLASSIFIED

Key Messages

Canada is committed to increasing its own domestic cyber security and technical skills and those of its allies. Collaboration amongst Five Eyes allies is crucial to the development of the capabilities and skills necessary to enhance safety and prosperity.

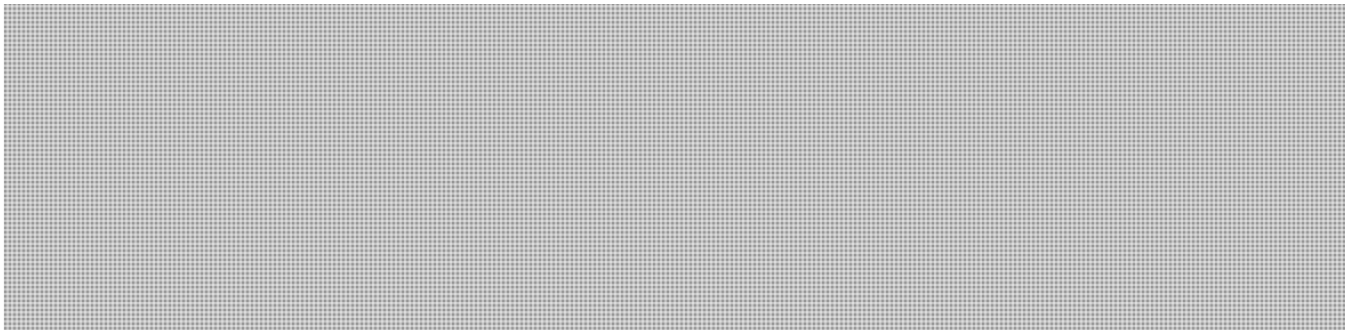


Other Potential Topic for Discussion

Emergency Management

Disaster and emergency management in Australia is led by Emergency Management Australia (EMA) a division within the Attorney-General's Department.

Like Canada, EMA works closely with state and territorial governments and the international emergency management community to deliver critical programs, policies and services that strengthen and maintain Australia's national security and emergency management capability.



Tab 2C

UNCLASSIFIED

SCENARIO NOTE FOR THE MINISTER

BILATERAL MEETING WITH ATTORNEY GENERAL JEFFERSON SESSIONS (U.S.)

Issue

You are scheduled for a bilateral meeting with U.S. Attorney General, Jefferson Sessions. Background information and key messages follow.

Given the short duration of the meeting and that this is your first time meeting in person, this will act primarily as a courtesy call, with the opportunity to begin discussions a couple of items of common interest notably:

- overview of proposed changes to Canada's national security framework;
- information sharing and privacy issues;
- opioids; and
- cannabis (responsive).

General overview

You last spoke to Attorney General Sessions on April 7, 2017.

This first in-person meeting will be an opportunity to reiterate these messages and to highlight the wide ranging areas of cooperation between your portfolios.

As the U.S. Cabinet member responsible for federal law enforcement, the Attorney General's portfolio overlaps with yours and includes: the Federal Bureau of Investigation and its Terrorism Screening Center; the Drug Enforcement Administration; the Bureau of Alcohol, Tobacco, Firearms and Explosives; United States Marshals Service, and the Bureau of Prisons. There is successful operational cooperation across the Portfolio with these organisations to ensure border integrity, cooperating on law enforcement investigations, and identify threats early.

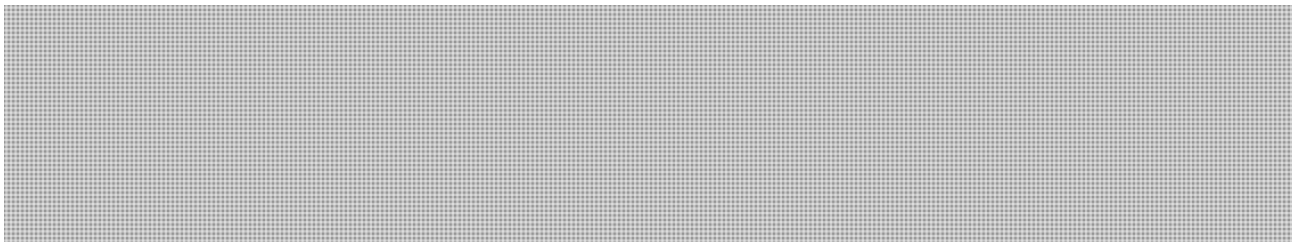
On June 21, 2017, Attorney General Sessions announce the creation of the National Public Safety Partnership to Combat Violent Crime, fulfilling part of President Trump's executive order on public safety. The partnership will provide funding to cities in the U.S. with a view to reducing gun crime, drug trafficking and gang violence. The program comprises two distinct levels of engagement: Diagnostic (supporting analysis) and Operations (supporting capacity building). These two complementary levels of engagement are offered based on the needs of the jurisdiction. The program enables the U.S. DOJ to provide cities with data-driven, evidence-based strategies tailored to the unique local needs of participating cities to address serious violent crime challenges tailored to their unique local needs. This meeting is an opportunity show interest in the initiative, and continue knowledge exchange on approaches.

s.13(1)(a)

s.15(1) - Int'l

s.21(1)(a)

Topic: Overview of the new national security legislation

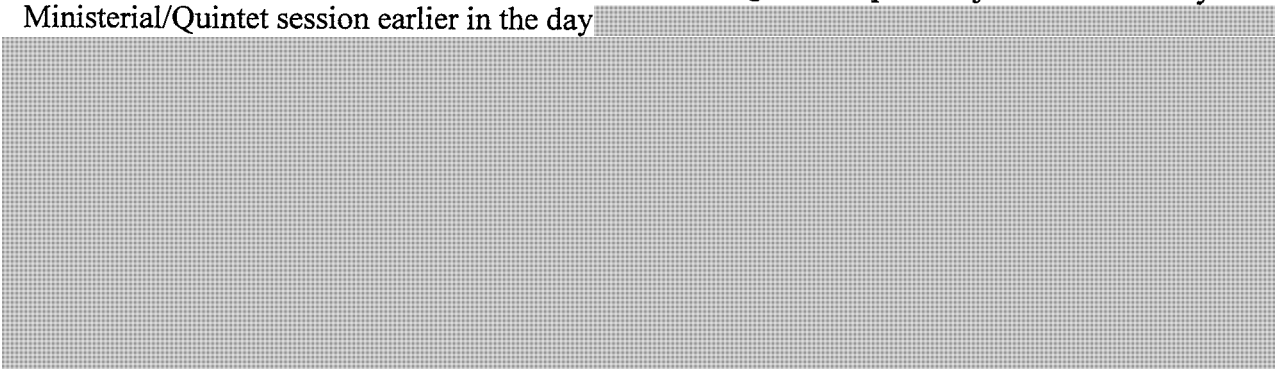


Key Messages:

- **Note that Canadians strongly support taking additional measures to improve accountability and transparency with respect to our national security. An example of this interest are the over 79,000 responses received during the online consultation process alone.**
- **Canada remains committed to working with US and to intelligence cooperation through the Five Eyes. Transparency and accountability in the context of this legislation means building a better relationship with citizens and raising awareness as to the value of the work the intelligence community does in enhancing security.**
- **Provide assurance that we will continue to work closely on national security issues with U.S. counterparts so that we can both keep our citizens safe in a manner that safeguards their rights and freedoms.**

Topic: Information sharing and privacy issues



Enhanced, real-time law enforcement information sharing is the topic of a joint Five Country Ministerial/Quintet session earlier in the day



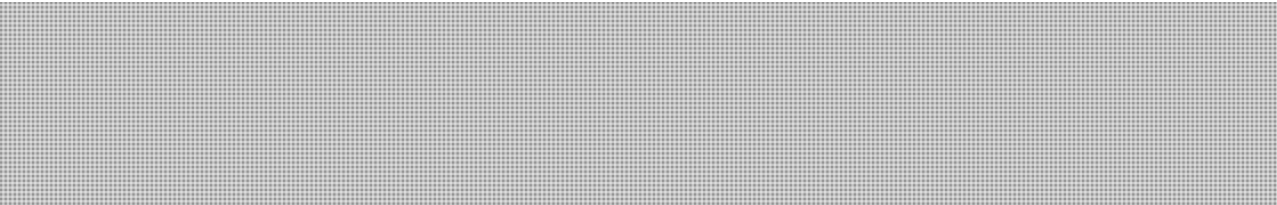
The Executive Order on public safety which dealt with removals included language that sought to have federal agency privacy policies exclude persons who are not United States citizens or lawful permanent residents. The issues of protection of Canadians' personally identifiable information that is shared with the U.S. is gaining increasing public awareness, including in: the context of media coverage of the experiences of individuals being refused entry to the U.S; the debate on the Preclearance legislation; and the House of Commons Standing Committee on Access to Information, Privacy and Ethics study "Privacy of Canadians at Airports, Borders and Travelling in the United States." The Privacy Commissioner wrote to a letter in March, jointly addressed to you and the Ministers of Justice and Defence. Officials continue to pursue written assurances from U.S. counterpart organisations that this will not change the way that information provided by Canada is handled, used and protected.


Key Messages:

- **Note the importance of being able to assure citizens on both sides of the border that their information and rights are safeguarded.**
- **Note that law enforcement-to-law enforcement information sharing for the purposes of criminal investigations is already well-established and working well. Underscore that Canada's approach is to do this on a case-by-case basis, to ensure that appropriate safeguards are in place to protect individuals' *Charter* rights and the integrity of criminal investigations.**


Topic: Opioids


The opioid crisis, driven primarily by a rapid increase in the use of fentanyl and other powerful illegal opioid drugs, has led to an unprecedented number of overdose deaths. The crisis is particularly acute in western Canada, but trends indicate that the situation is moving eastward. Affected individuals and families cross all demographics and this situation is impacting all Canadians:

- In 2016, almost 2,500 Canadians died from opioid-related overdoses.
 - In 2016, the death toll for illicit drug overdoses in British Columbia – the hardest-hit province – reached a record 914, up almost 80% from 2015. 374 illicit drug overdose deaths with fentanyl were detected; this is a 194% increase over the number of deaths (127) occurring during the same period in 2015.
 - In Alberta, there were 343 overdose deaths in 2016 in which fentanyl was detected, including 22 cases where carfentanil was involved.
 - In Ontario, preliminary data indicates 707 opioid-related deaths in 2015, 203 (29%) of which involved fentanyl. Opioid overdose deaths increased 463% between 2000 and 2013.
- 

Established under the 2016 North American Leaders Summit (NALS), senior officials from Canada, Mexico and the U.S. cooperate on the issue of illicit fentanyl and other opiates under the North American Drug Dialogue (NADD). Canadian participation in this forum has included

s.15(1) - Int'l

s.21(1)(a)

Public Safety, Justice Canada, Health Canada, CBSA, RCMP, FINTRAC and Global Affairs. U.S. participation has included the Drug Enforcement Agency, Homeland Security, the Office of National Drug Control Policy, Financial Crimes Enforcement Network (FinCEN) (a bureau of the Department of Treasury), Health and Human Services, Department of State, Department of Defence, and the Federal Bureau of Investigation.

Key Messages:

- **Note that the Government is taking a comprehensive approach to respond to the opioid crisis, focusing on several aspects of the problem including interdiction, demand reduction, treatment and harm reduction.**
- **Highlight that Bill C-37, which received Royal Assent on May 18, proposed new actions to reduce the supply of illicit opioids and other drugs by amending relevant legislation to better equip law enforcement and health officials to reduce harms linked to drug and substance use in Canada. Notably, Bill C-37:**
 - **Prohibits the unregistered importation of designated devices, such as pill presses and encapsulators that may be used in the illicit production of controlled substances;**
 - **Provides the authority to border officers to open mail weighing 30 grams or less, in order to stop fentanyl and other drugs, from entering Canada illicitly through the mail system; and**

Grants temporary accelerated scheduling to control new and dangerous psychoactive substances by allowing the Minister of Health to temporarily add a dangerous new substance to a schedule of the *Controlled Drugs and Substances Act*, pending a comprehensive review. The temporary scheduling would last for up to two years and would establish criminal offences and penalties for the production, trafficking, import and export of those substances that are added to the temporary schedule.
- **Mention that Public Safety, the RCMP and CBSA are working closely with the United States Drug Enforcement Administration and other U.S. agencies, to build the necessary intelligence, information sharing and operational measures to halt the flow of fentanyl into the continent.**

Responsive Issues

Topic: Cannabis

On April 13, 2017, the Government introduced legislation (Bill C-45) to legalize and strictly regulate cannabis. The proposed *Cannabis Act* would create a legal framework for controlling the production, distribution, sale and possession of cannabis in Canada. Following Royal Assent, the proposed legislation would allow adults to legally possess (30 grams in public) and use cannabis. The Bill would also, for the first time, make it a specific criminal offence to sell cannabis to a minor and create significant penalties for those who engage young Canadians in cannabis-related offences.

Attorney General Sessions is a vocal opponent of marijuana (medical and recreational), and has asked the U.S. DOJ to review its related policies on enforcement. In the spirit of increased U.S. DOJ action on this issue, he wrote to Congress seeking a lift of the prohibition of the use of U.S. DOJ funding to “prevent certain states from implementing their own State laws” related to the legalization of medical marijuana. He has expressed that this is partially based on concerns that organised crime has infiltrated the legal marijuana business, and it would therefore be “unwise for Congress to restrict the discretion of the Department of Justice to fund particular prosecutions.” You may want to signal that public education, including implications for cross-border travel, is a key part of the proposed legislation.

Key Messages:

- **Note the Government’s intentions to bring the proposed Cannabis Act into force no later than July 2018. Highlight that this will be done alongside a robust public awareness and education campaign to inform Canadian travelers, as well as international visitors, of the rules around cannabis possession.**
- **Underscore that the movement of cannabis and cannabis products across international borders would remain a serious criminal offence.**
- **Emphasize that Canada takes its international obligations very seriously and will continue to engage in constructive dialogue with the U.S. and other international partners throughout the legislative process.**

Tab 2D

**UNCLASSIFIED****SCENARIO NOTE FOR THE MINISTER****BILATERAL MEETING WITH PETER DUTTON (AUSTRALIA)****Issue**

You are scheduled for a 30 minute bilateral meeting with Australia's Minister for Immigration and Border Protection Peter Dutton.

Minister Dutton was sworn in as the Minister for Immigration and Border Protection on December 23, 2014. This will be your first face-to-face meeting. His department has not identified any specific items for discussion, so it will serve as an opportunity to follow up on discussions from the Five Country Ministerial (5CM), and better understand Australia's border challenges. If time permits, you could also enquire about Australia's work towards ratifying the Optional Protocol to the Convention against Torture (OP-CAT).

Border Agency Cooperation

The Canada Border Services Agency (CBSA) engages with the Australia Border Force (ABF) and the Department of Immigration and Border Protection (DIBP) on customs, border management and intelligence issues.

The CBSA and its Australian counterparts communicate regularly to share information and best practices and to reaffirm support for challenges within the border management environment. This relationship is strengthened by the presence of a CBSA Liaison Officer and Intelligence officer in at Canada's High Commission in Canberra, Australia, an ABF Counsellor in Washington, D.C. who is accredited to Canada, and a DIBP Counsellor at Australia's High Commission in Ottawa.

Human Smuggling

Issues regarding human smuggling, asylum seekers, and refugees may be raised in Minister Dutton's bilateral conversation with Minister Hussen shortly after your meeting (scheduled for 9:00 a.m. on June 27).

Human smuggling is a key migration security priority for Australia. Australia's Operation Sovereign Borders (OSB) is a military-led border security operation aimed at combating maritime people smuggling and protecting Australia's borders. The OSB Joint Agency Task Force (JATF) is a whole-of-government initiative, supported by a wide range of federal government agencies.

Canada has adopted a whole-of-government approach to address the issue of mass arrivals by instituting *Canada's Migrant Smuggling Prevention Strategy* headed by the Privy Council Office, and participation of RCMP, CBSA and GAC.



UNCLASSIFIED

[Redacted]

Such efforts allow the RCMP to work in collaboration with foreign authorities to help prevent the illegal migration taking place.

Optional Protocol to the Convention against Torture

Ratification of OP-CAT requires parties to establish and maintain a National Preventive Mechanism which will proactively monitor detention facilities, including immigration detention facilities, to ensure that they prevent torture and mistreatment in areas of detention. Australia intends to ratify the Optional Protocol to the Convention against Torture (OP-CAT) by December 2017. You may wish to ask what considerations were weighed in applying OP-CAT to Australian immigration detention centres.

[Redacted]

Tab 2E

**UNCLASSIFIED****SCENARIO NOTE FOR THE MINISTER****BILATERAL MEETING WITH AMBER RUDD****Issue**

You are scheduled to have a 30-minute meeting with Amber Rudd, the Secretary of State for the Home Department (Home Secretary) of the United Kingdom (UK). The meeting builds on previous bilateral meetings with UK officials where you discussed issues of mutual interest, including countering radicalization to violence, national security legislation, accountability and review, the terrorism threat level, and the cyber threat environment.

Potential Discussion Topics include:

The bilateral meeting will provide the opportunity for you to brief Secretary Rudd on the proposed changes to Canada's national security framework, and to continue discussions on key national security issues addressed in the FCM and Quintet meetings (CVE, encryption, etc).

New National Security Legislation

Secretary Rudd may be eager to understand the changes to Canada's accountability framework as well as timing of when the legislation could be enacted. You could provide an overview of key elements around changes in transparency, information sharing and oversight.

Key Messages:

- **Canadians strongly support taking additional measures to improve accountability and transparency with respect to our national security.**
- **Canada remains committed to working with the UK and Five Eyes to further intelligence cooperation. Transparency and accountability means building a better relationship with citizens and raising awareness about the value of the intelligence community' work to enhance security.**

Countering Terrorism

According to British authorities, approximately 850 people from the UK have travelled to support or fight for violent extremist organizations in Syria and Iraq, and half of these individuals have since returned to the UK.

In the June 21 UK "Queen's Speech" to open Parliament, the UK government committed to a counter-terrorism (CT) review, including a review of CT legislation, as well as a new Commission for Countering Extremism.

**UNCLASSIFIED**

Human Trafficking

The session on human trafficking (referred to as “modern slavery” by the UK government) will be directed toward information sharing.

Some key messages you may wish to reiterate during the bilateral meeting are:

Criminal Information Sharing

- **Canada is supportive of exploring options to improve information sharing between Five Eyes countries on known criminals, in order to prevent criminals, such as sex offenders and human traffickers, from entering our countries.**
- **Any agreement on the sharing of criminal conviction records with Five Eyes countries, especially as it pertains to sex offenders who travel, must respect and be in accordance with existing legislation, including the Sexual Offender Information Registration Act (SOIRA) and Canadian privacy legislation.**

Modern Slavery/Human Trafficking

- **Canada is committed to combatting human trafficking and better protecting its victims, who are among society’s most vulnerable. Collaboration and improved information sharing on human trafficking are critical to our collective efforts to counter human trafficking.**
- **Canada has adopted a collaborative and multi-pronged – “4P” - approach in its fight against human trafficking: prevention, protection, prosecution, and partnership building. We work closely with provinces and territories, Indigenous communities, law enforcement, community organizations and international partners to combat human trafficking.**
- **We support further discussion on our countries’ challenges and best practices in investigating trafficking routes, sharing investigative information, and on exploring options for joint operations.**

Border Cooperation

The CBSA primarily engages with its UK equivalent, Border Force (BF), in multilateral and regional fora, such as the Five Country Conference (FCC) and Border Five (B5). Both organisations share similar mandates including border management, targeting and intelligence gathering.



UNCLASSIFIED

Cyber Security (Responsive)

Should Minister Rudd raise cyber, you may wish to note existing cooperation in the Ottawa 5 fora as well a mention of Canada's intention to rollout an updated national cyber security strategy and cyber governance in the fall.

The UK's November 2016 National Cyber Security Strategy sets out the themes of: defence against the threat; deterrence of hostile actions against the UK, its people, businesses and allies; and development of the cyber security industry; enhancement of cyber security skills; and strengthening of the scientific research base. In October 2016, the National Cyber Security Centre was established to consolidated cyber operational responsibilities and capabilities.

The UK's new plan dedicates over £1.9 billion (approximately \$3.3 billion) to four principal goals:

- Tackling cybercrime and being one of the most secure places in the world to do business;
- Increasing resilience to cyber-attacks on UK interests in cyberspace;
- Helping to shape an open, vibrant and stable cyberspace domestically and globally; and
- Building the cyber knowledge, skills and capability needed to underpin all cybersecurity objectives.

At the June 2017 meeting of the Ottawa 5 in Australia, Principals discussed domestic legislative and policy frameworks and examined responses to real world examples. Current Ottawa 5 priorities include: improving the collective understanding of the activities of key cyber actors; sharing information on collective cyber incident responses (including through joint exercises); and improving and collective understanding of cyber aspects of export control issues.

Tab 2F

SCENARIO NOTE FOR THE MINISTER

BILATERAL MEETING WITH SECRETARY JOHN KELLY (U.S.)

Issue

You are scheduled for a bilateral meeting with U.S. Secretary of Homeland Security, John Kelly. Background information and key messages follow.

Given the short duration of the meeting and the regular exchanges at all levels, this meeting is expected to provide an update on the Government's legislative agenda and border issues notably:

- Overview of proposed changes to Canada's national security framework;
- Expected next steps on Entry/Exit;
- Status of Preclearance legislation; and
- Managing irregular migration.

In addition, we have prepared responsive material:

- Enhanced aviation security and collaboration on counter terrorism;
- Management of summer surge and border wait times;
- [REDACTED]
- Cannabis;
- [REDACTED]
- [REDACTED]

Legislative update

Topic: Overview of the new national security legislation

[REDACTED]

Key Messages:

- **Note that Canadians strongly support taking additional measures to improve accountability and transparency with respect to our national security. An example of this interest are the over 79,000 responses received during the online consultation process alone.**
- **Underscore that Canada remains committed to working with U.S. and to intelligence cooperation through the Five Eyes. Transparency and accountability in the context of this legislation means building a better relationship with citizens and raising awareness as to the value of the work the intelligence community does in enhancing security.**
- **Highlight the key changes of interest to the U.S. notably:**

Highlight the key changes [REDACTED]:

- **Enhanced accountability through the creation of the National Security and Intelligence Review Agency (NSIRA);**
 - **Increased oversight through the creation of an Intelligence Commissioner;**
 - **Improved transparency through a 6-point commitment to sharing national security information with Canadians; and**
 - **Clarified processes for the sharing of information and redress through improvements to the *Secure Air Travel Act* and revisions to the *Security of Canada Information Sharing Act*.**
- **Provide assurance that we will continue to work closely on national security issues with U.S. counterparts so that we can both keep our citizens safe in a manner that safeguards their rights and freedoms.**

Topic: Expected next steps update on Entry/Exit

Under Entry/Exit, Canada and the U.S. would share biographic information on all travellers crossing at common land ports of entry. Pending the passage of Bill C-21, Canada has been providing biographic information on U.S. citizens entering Canada at the land border since last August, in addition to the information about third-country nationals and permanent residents which Canada and the U.S. have been exchanging since 2013. Bill C-21, an *Act to amend the Customs Act*, was introduced in June 2016 and would enable Canada to fully meet its commitment to the U.S. and share information on all travellers crossing the land border. Upon Royal Assent of C-21, the enabling regulatory amendments would need to be published before fully implementing. It has been a year since the introduction of Bill C-21 that would complete Canada's Beyond the Border Action Plan commitment with respect to Entry/Exit. [REDACTED]

Key Messages:

- **Express the Government's commitment to move Entry/Exit legislation through Parliament; and note that sharing of biographic information on third country nationals and permanent residents, and on U.S. citizens entering Canada at the land border is working well.**
- **Note that upon Royal Assent of the legislation, the Government will be positioned to bring forward enabling regulations allowing for the full implementation of Entry/Exit at the land border.**

Topic: Status of Preclearance legislation

On June 14, Bill C-23 completed clause-by-clause review at Committee and will be moving to report stage. The amendments were minimal and included: a legislative requirement to train U.S.

clearance officers as per the Preclearance Agreement; a five year review of the Preclearance Act; and a clause indicating that Canadians can contact senior Canadian officials regarding any concerns they may have with the exercise of certain officer authorities.

[REDACTED]

For Canada to be in a position to ratify the new Agreement, we need to pass legislation, approve regulations and address implementation issues

[REDACTED]

Key Messages:

- **Highlight the recent progress of preclearance legislation; Emphasize that it continues to be a legislative priority and that the next step is for the Bill to be referred to the Senate.**
- **Note that Canada continues to work on the required regulations and implementation issues that need to be addressed before ratification,**

[REDACTED]

Border issues

Managing irregular migration

Irregular migration from the U.S. to Canada throughout 2017 has placed significant strain on RCMP and CBSA resources between and at ports of entry, as well as border communities in Emerson, Manitoba and Lacolle, Quebec.

[REDACTED]

During your most recent call with Secretary Kelly, you both agreed to share information on current trends and flows. Current indicators are as follows:

- From January 1, 2017, to May 22, 2017, 5,384 people made asylum claims after crossing the border from the U.S. at or between ports of entry.

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Longer-term measures will be required to address the irregular migration issue. Strengthening border integrity will also require close cooperation with U.S. law enforcement partners. [REDACTED]

[Redacted]

For you, this meeting will be an opportunity to 1) emphasize the need to strengthen border integrity, and 2) underscore the need to maintain an ongoing bilateral dialogue on irregular migration.

Key Messages:

- **Underscore the importance of working together to keep the land border flowing effectively, while ensuring security at and between ports of entry.**
- **Acknowledge the significant efforts made by the CBSA to address regular and irregular migration** [Redacted]
- **Note the need to have officials continue to discuss meaningful ways to address irregular migration issues, including through:**
 - **the exchange of trends to better understand the drivers for irregular migration; and**
 - [Redacted]

Responsive Issues

Topic: Enhanced aviation security

We expect Secretary Kelly will take the opportunity to build on the counter terrorism cooperation discussions of the Five Country Ministerial meeting by sharing his current thinking on ways to enhance aviation security. DHS has been considering a series of measures related to airport personnel management and passenger screening, including: improving identification of insider threats and vetting of airport employees, detection of suspicious travelers, enhanced screening of personal electronic devices, and enhanced sharing of traveler information (e.g. watchlists, advanced passenger information).

[Redacted]

Key Messages:

- [Redacted]
- [Redacted]
- **Note that Canada remains committed to rigorous aviation security in order to order to protect our citizens against in-air threats, and we would look forward to a continuing this conversation as details around some of these measures are developed.**

Topic: Management of summer surge and border wait times

Border wait times, especially during the increased summer traffic, continue to be an area of concern for border stakeholders. As was recently pointed out by Ambassador MacNaughton, this trend could be exacerbated by interest in the celebrations for Canada 150. One of the ports of entry most often faced with summer line ups is the Peace Bridge, and ongoing construction that is planned over the summer could add to the usual pressure. It is worth noting, however, that travellers in this area do also have the option of the Rainbow Bridge, the Queenston-Lewiston Bridger and the NEXUS-only Whirlpool Bridge. The U.S. may take this opportunity to seek assurances that efforts are being made to prepare for the summer surge.

Key Messages:

- **Recognize the importance of reducing border wait times in the interest of trade and tourism. Note that CBSA works with bridge operators to ensure adequate traffic management and movement of travellers.**
- **CBSA continues to plan and make every effort to forecast traffic patterns and volumes, and adjust staffing levels during peak travel periods to minimize processing times and unnecessary delays at border crossings.**

Topic: Cannabis

On April 13, 2017, the Government introduced legislation (Bill C-45) to legalize and strictly regulate cannabis. The proposed Cannabis Act would create a legal framework for controlling the production, distribution, sale and possession of cannabis in Canada. Following Royal Assent, the proposed legislation would allow adults to legally possess (30 grams in public) and use cannabis. The Bill would also, for the first time, make it a specific criminal offence to sell cannabis to a minor and create significant penalties for those who engage young Canadians in cannabis-related offences.

s.13(1)(a)

s.15(1) - Int'l

s.21(1)(a)

Attorney General Sessions is a vocal opponent of marijuana (medical and recreational), and has asked the U.S. DOJ to review its related policies on enforcement. In the spirit of increased U.S. DOJ action on this issue, he wrote to Congress seeking a lift of the prohibition of the use of U.S. DOJ funding to “prevent certain states from implementing their own State laws” related to the legalization of medical marijuana. He has expressed that this is partially based on concerns that organised crime has infiltrated the legal marijuana business, and it would therefore be “unwise for Congress to restrict the discretion of the Department of Justice to fund particular prosecutions.” You may want to signal that public education, including implications for cross-border travel, is a key part of the proposed legislation.

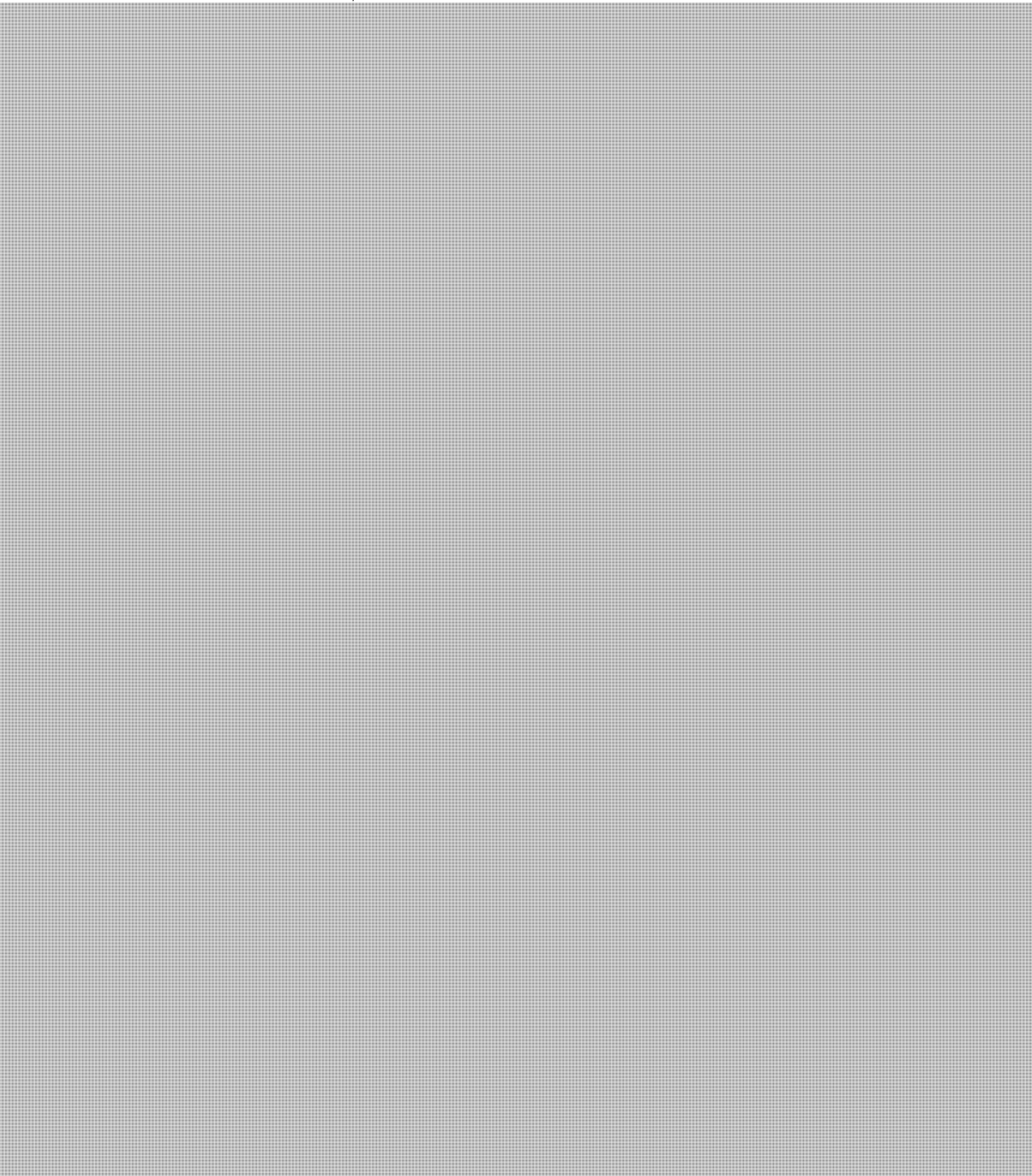
Key Messages:

- **Note the Government’s intentions to bring the proposed Cannabis Act into force no later than July 2018. Highlight that this will be done alongside a robust public awareness and education campaign to inform Canadian travelers, as well as international visitors, of the rules around cannabis possession.**
- **Underscore that the movement of cannabis and cannabis products across international borders would remain a serious criminal offence.**
- **Emphasize that Canada takes its international obligations very seriously and will continue to engage in constructive dialogue with the U.S. and other international partners throughout the legislative process.**

s.13(1)(a)

s.15(1) - Int'l

s.21(1)(a)



Page 460
is not relevant
est non pertinente

Tab 3



Session 1

Threat Briefing & Counterterrorism

Session Lead

Minister Ralph Goodale, Canada

CSIS, Canada

Participating Ministers

| | |
|-----------------------|----------------|
| George Brandis | Australia |
| Peter Dutton | Australia |
| Ahmed Hussen | Canada |
| Jody Wilson-Raybould | Canada |
| Christopher Finlayson | New Zealand |
| Michael Woodhouse | New Zealand |
| Amber Rudd | United Kingdom |
| John Kelly | United States |
| Jeff Sessions | United States |

Tab 3A

FOR OFFICIAL USE ONLY

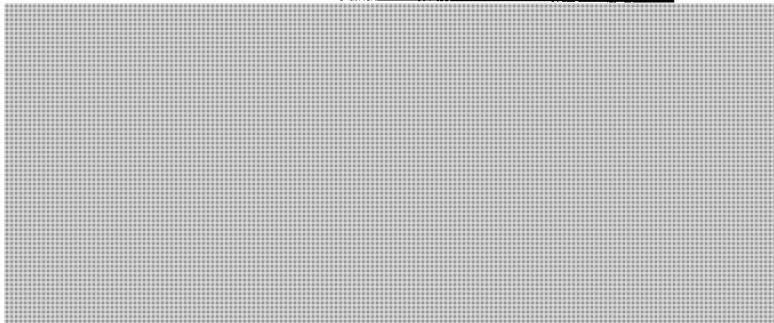
Public Safety
CanadaSécurité publique
Canada**FCM 2017 – Session I Scenario Note****Intelligence Briefing & Counterterrorism****Sequencing**

This session will last 90 minutes and will be held at the Top Secret level. It is essential for the smooth functioning of the conference that the time limits be respected in this session. While the other Ministers are encouraged to ask questions during the intelligence briefing, Minister Goodale is encouraged to limit introductory remarks from anyone except him, as the chair and host.

N.B.: Due to the security requirements of this session, delegates (e.g. departmental staff, ministerial staff) who do not have a Top Secret clearance will not be permitted to remain in the room. They will be invited to return at the conclusion of this session (approximately 9:30 am).

Part 1: Introduction and Opening Remarks (5-10 minutes)

- CAN/Minister Goodale will deliver brief opening remarks (see Talking Points).
- CAN/Minister Goodale will briefly introduce the other Ministers, and will then invite CSIS representatives to speak.

Part 2: CSIS Intelligence Briefing (45 minutes)**Part 3: Informal Discussions (40 minutes)**

- CAN/Minister Goodale will invite UK Home Secretary Amber Rudd to speak for 5 minutes about the recent terrorist attacks in London and Manchester and the UK government's response.
- Ministers will be free to speak on any subject they choose; CAN/Minister Goodale will moderate discussion.

Talking Points**Opening Remarks**

- **Ministers, Secretaries, Attorneys General and distinguished guests, welcome to the fourth Five Country Ministerial meeting.**

FOR OFFICIAL USE ONLY



Public Safety
Canada

Sécurité publique
Canada

- **Along with the Canadian host of the Quintet of Attorneys General, the Honourable Jody Raybould-Wilson, and in collaboration with my colleague, the Honourable Ahmed Hussen, Minister of Immigration, Refugees and Citizenship, I am honoured to host the Five Country Ministerial, and we are very pleased to meet with you all here today. This meeting is a testament to our longstanding, close, and highly trusted relationship.**
- **Our five countries have a long history of cooperation, supporting each other through troubled times.**
- **Recent threats and attacks have not deterred our commitments to one another, but have only strengthened our bonds, and our pledge to tackle crimes and threats together.**
- **Like other countries, we have faced serious and immediate security challenges both at home and abroad.**
- **During our meeting today, we will discuss the role of the Internet in radicalization and violence, and how to mitigate the threats from returning foreign fighters.**
- **We also discuss the importance of welcoming immigrants and those fleeing persecution to our countries, while at the same time recognizing the necessity of defending our borders by using the latest technology.**
- **Later today, we will discuss with the Attorneys General of the Quintet how to further work on the information-sharing mechanisms between our five countries.**
- **Finally, we will discuss how to cooperate with each other and with communications service providers on issues of law enforcement and encryption, and we will work towards a common response on cyber-security.**

FOR OFFICIAL USE ONLY



Public Safety
Canada

Sécurité publique
Canada

- **We know all too well that these security issues are not just abstract. Recently, whether in London, Manchester, Melbourne or Sainte-Foy, radicalized individuals perpetrated horrific acts of terrorist violence that led to numerous casualties. We stand by those affected by these and other attacks, and offer our sincerest condolences.**
- **Ladies and gentlemen, we have a serious and important task ahead of us today, and I look forward to a frank and fruitful discussion between friends.**
- **It is my pleasure to introduce the Ministers, Secretaries and Attorneys General present today:**
 - **From Canada:**
 - **Myself, Minister of Public Safety and Emergency Preparedness;**
 - **My colleague and co-host of our Joint Session with the Quintet this afternoon, Jody Raybould-Wilson, Minister of Justice and Attorney General of Canada**
 - **My colleague Ahmed Hussen, Minister of Immigration, Refugees and Citizenship**
 - **(To your right) from Australia:**
 - **Attorney-General George Brandis, and Minister of Immigration and Border Protection Peter Dutton.**
 - **From New Zealand:**
 - **Attorney-General Christopher Finlayson and Minister of Immigration Michael Woodhouse**
 - **From the United Kingdom:**
 - **Home Secretary Amber Rudd**
 - **From the United States**
 - **Secretary of Homeland Security John Kelly, and Attorney General Jeff Sessions**
- **My colleagues from the Canadian Security Intelligence Service will now proceed with an overview threat briefing. Following the briefing, our colleague from the UK will present some brief remarks on the recent terrorist attacks on the United Kingdom.**
- **Thank you.**

FOR OFFICIAL USE ONLY

Public Safety
CanadaSécurité publique
Canada

(After briefing: CAN/Minister Goodale will invite UK/Home Secretary Rudd to speak for 5 minutes; then, moderate informal conversation)

- **I will now invite Home Secretary Rudd to speak on the recent attacks in the UK and on lessons drawn from them.**
- **Thank you very much to Home Secretary Rudd for sharing the UK lessons learned through these tragic circumstances. I would now like to invite you to share your thoughts on the threats we are collectively facing today and your views on how to address them, starting with Attorney General Brandis.**

Responsive Talking points:

On recent attacks in the United Kingdom

- **Canada offers its condolences and support to the United Kingdom following the recent attacks in Manchester and London. Prime Minister Trudeau has spoken to Prime Minister May to indicate Canada's solidarity and intention to fully cooperate with the UK on issues of terrorism and radicalization.**

Developments since last FCM

- **Since the last FCM, the Government of Canada has undertaken an unprecedented engagement with all sectors of society on national security oversight issues.**
- **In the 2017 budget, the Government of Canada prioritized the protection of critical infrastructure, including energy infrastructure, across the country; the government will work with communities across Canada to safeguard important facilities and institutions.**

Terrorism and Radicalization:

- **The Action Plan of the Working Group on Countering Violent Extremism, which we will consider later in the day, would take important steps in our cooperative approach towards fighting violent extremism.**

- **Canada's terrorism threat level remains at Medium, its level since October, 2014. Canada is vigilant and prepared for the threat of terrorism within our country.**

FOR OFFICIAL USE ONLY



Public Safety
Canada

Sécurité publique
Canada

- ***In August, 2016, Canadian ISIS sympathizer Aaron Driver died in a confrontation with police after he detonated an explosive device in the back seat of a taxi. I am proud and grateful for the fast and effective response of law enforcement in this incident; but it reminds us of the work that we have ahead of us in countering radicalization.***
- ***The principal terrorist threat to Canada remains the possibility of violent extremists carrying out attacks within our borders.***
- ***Attacks such as the one in Sainte-Foy, Québec, also remind us of the growing dangers of violent right-wing extremism.***

Cybersecurity and Encryption

- ***Last year, the Government of Canada held wide consultations on cybersecurity. Canada has the most computers per capita of any country in the world, and we are committed to helping keep Canadians safe online.***
- ***Canada is committed to finding the right balance between protecting the rights of individuals and organizations to protect their data, and the legitimate needs of law enforcement to access data during investigations.***

Refugees, Migration and Human Trafficking

- ***Canada is very proud of having welcomed more than 40,000 Syrian refugees to our country over the past year. We are committed to ensuring the safety, security and health of Canadians and refugees in migration issues.***
- ***Our Government has a longstanding commitment to protect the vulnerable, tackle crime and safeguard Canadians and their families in their homes and communities.***
- ***Canada was among the first countries to ratify the United Nations Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children.***

FOR OFFICIAL USE ONLY

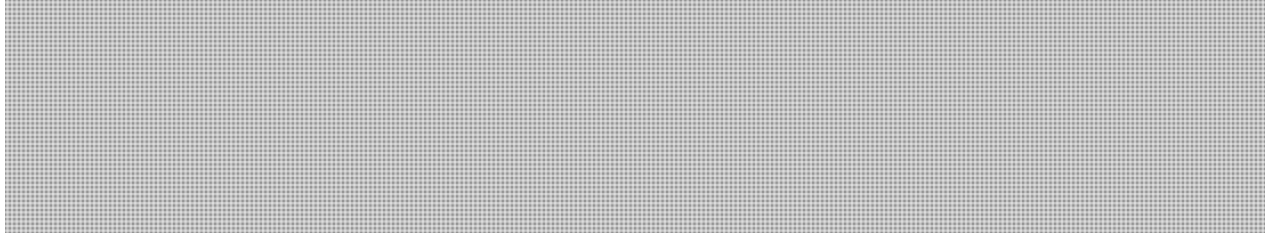


Public Safety
Canada

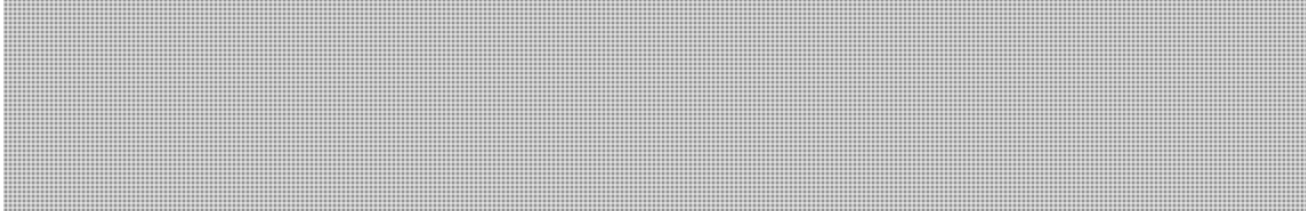
Sécurité publique
Canada

Recent FVEY CT Developments

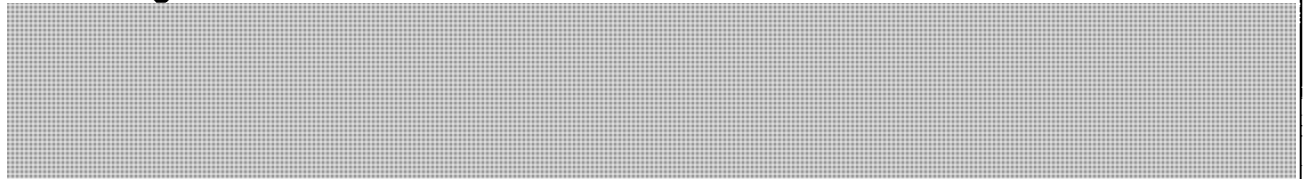
Australia



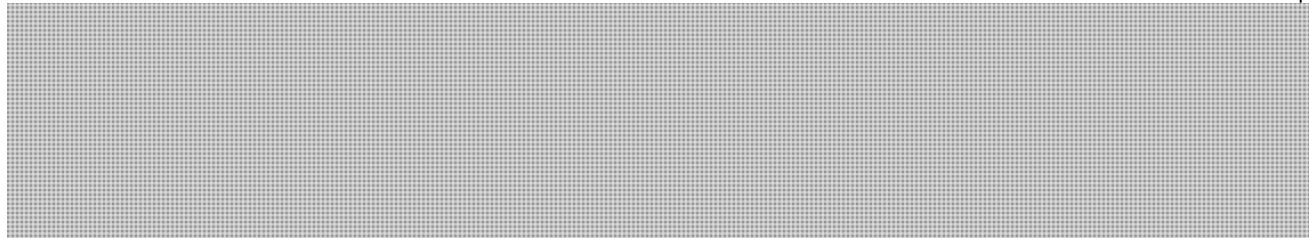
New Zealand



United Kingdom



United States



Tab 4



Session 2

Countering Violent Extremism

Session Lead

Minister Ralph Goodale, Canada

Participating Ministers

| | |
|-----------------------|----------------|
| George Brandis | Australia |
| Peter Dutton | Australia |
| Ahmed Hussen | Canada |
| Jody Wilson-Raybould | Canada |
| Christopher Finlayson | New Zealand |
| Michael Woodhouse | New Zealand |
| Amber Rudd | United Kingdom |
| John Kelly | United States |
| Jeff Sessions | United States |

Tab 4A

FOR OFFICIAL USE ONLY



Public Safety
Canada

Sécurité publique
Canada

FCM 2017 – Session II Background Note

Countering Violent Extremism

Sequencing

CAN/Minister Goodale will chair this session, which includes three segments.

CAN/ Minister Goodale will present the Working Group's Action Plan for endorsement (15 minute presentation, including 2 videos).

(TAB 4F),

(TAB 4G)

Talking Points

*As Canada is leading this session, a detailed scenario note, which includes all your talking points, is provided in **TAB 4B**.*

*The Action Plan and a summary of the Action Plan are provided (**TAB 4D & TAB 4E**).*

Expected Position of the FVEY

Also of note, the UK government announced in its Speech from the Throne the creation of a new Commission for Countering Extremism. Its role will be to "identify examples of extremism and expose them; help the Government identify new policies to tackle extremism; and support the public sector and civil society in promoting and defending pluralistic values across all our communities."

s.15(1) - Int'l

s.21(1)(a)

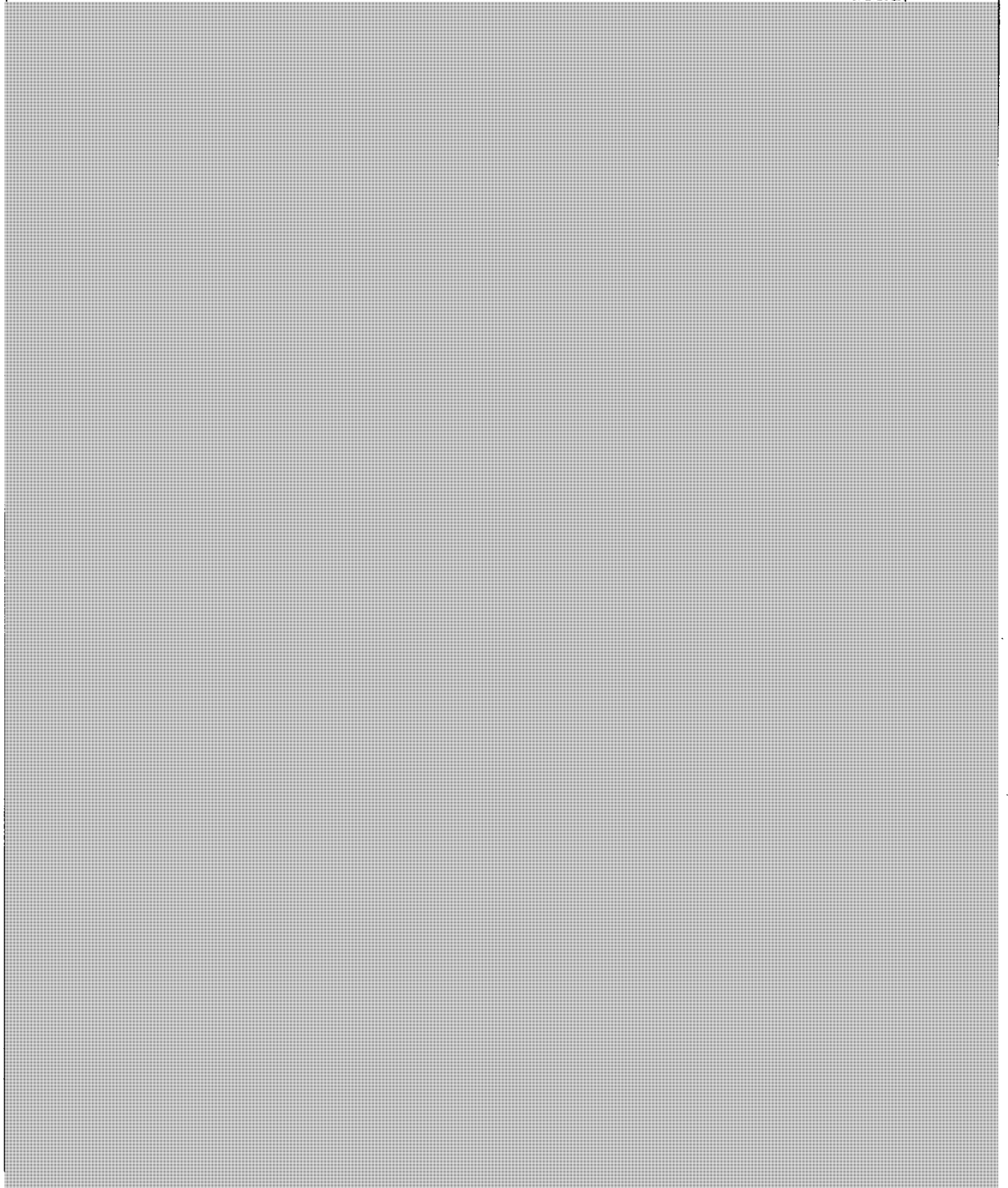
FOR OFFICIAL USE ONLY



Public Safety
Canada

Sécurité publique
Canada

After a recent DAESH claimed attack in Melbourne on June 5th which left one dead,



Tab 4B



Public Safety
Canada

Sécurité publique
Canada

Scenario Note

for

Minister Goodale

Minister of Public Safety and Emergency Preparedness

**Five Country Ministerial – Remarks and Talking Points on
Countering Violent Extremism**

Monday, June 26, 2017

Ottawa, Ontario

Word count for Opening Remarks: 1,032 (8.5 minutes @ 120wpm), plus two videos

| | |
|--------------|--|
| 09:30 | <i>You will open the first session on Countering Violent Extremism with your Opening Remarks</i> |
| | <p>Colleagues, our next agenda item is countering violent extremism.</p> <p>This topic is at the heart of our mandates as Ministers tasked with ensuring the safety and security of our citizens.</p> <p>Our governments have been grappling with the threat of violence by those radicalized by intolerant ideologies, and we have seen heinous acts – even in the last few weeks.</p> <p>We witnessed the tragic events in Manchester, London, and Melbourne, and our thoughts and prayers were with your cities – especially with the victims and their families.</p> <p>Canada is not immune to the threat of violent extremism. This past January, a young man terrorized an Islamic Cultural Centre in the province of Quebec.</p> |

Given recent attacks, we all share a common goal to work together to put a stop to this violence.

That's why I think this discussion is critical.

In Canada, some of our cities and communities have been making strides on efforts to counter radicalization to violence in different regions of the country. Our government recognized a need to better coordinate and lead federal and national efforts.

As such, we established an Office for community outreach and countering radicalization to violence to provide national leadership. The Office was formally launched on ----- (tbd).

This office will provide policy leadership, engage with Canadians, and enhance research in the area.

In essence, the goal is for the office to become a Centre of Excellence.

We want this office to work with international partners, and provide global leadership, including by being a co-chair of the Five Country Ministerial – CVE Working

Group [REDACTED]

Over the last year, this Working Group has mapped out an Action Plan to advance mutual priorities, which they are asking us to endorse today.

[REDACTED]

I will speak briefly on four of the priority areas now and one later on in the agenda when we get the issue of returning foreign terrorist fighters.


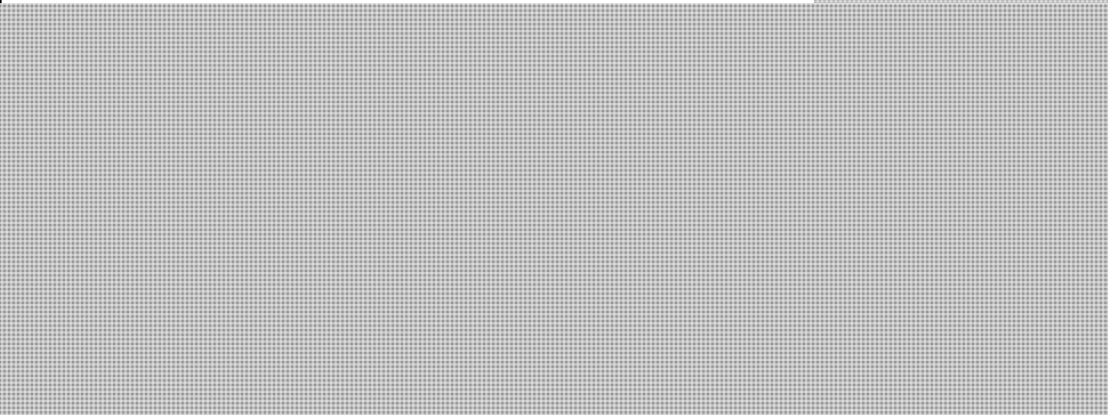

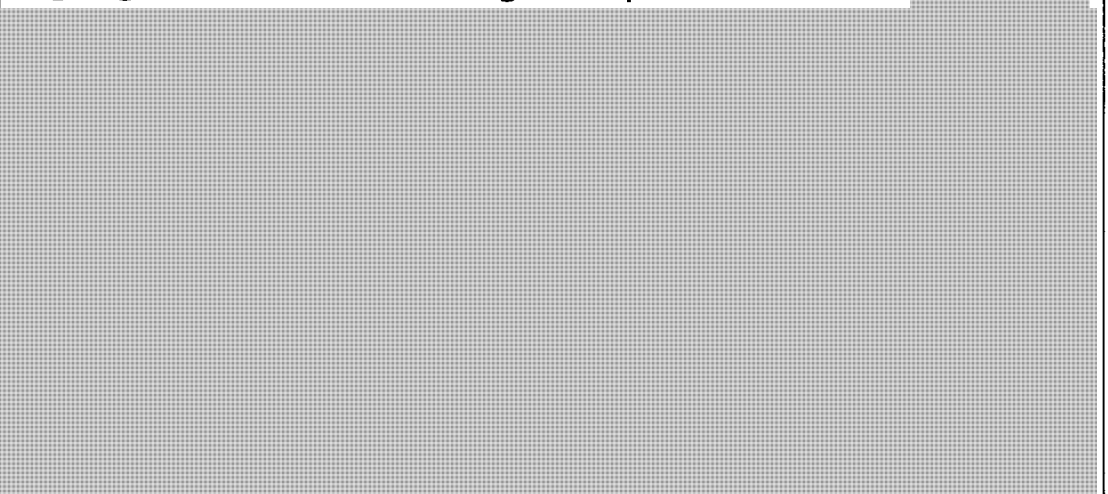
The first theme is central to Canada's approach to our own domestic efforts [REDACTED]

In Canada, what we know is that radicalization to violence looks different across our country.

We know the threat is specific to the local context and for this reason we are investing in approaches that are driven at the local-level and respond to the needs of the community.

I would like to show you two videos that highlight some of the local approaches in Canada in which we are

| | |
|---------------------|--|
| | <p>investing.</p> <p>Each of these initiatives has intervention components designed to prevent youth and young adults from being radicalized to violence.</p> <p>The first video is an education video produced by a non-governmental organization in the city of Montreal, known as the Centre for Prevention of Radicalization Leading to Violence.</p> <p>The video is informed by current research, and describes a hypothetical example of a young man radicalizing to violence, inspired by extreme right-wing ideology.</p> |
| <p>09:35</p> | <p><i>You will show the first video produced by the Centre for Prevention of Radicalization Leading to Violence. The video will play for 5 minutes.</i></p> |
| | <p>The second video describes another approach to intervention, the multi-agency, or "Hub Model" approach. This model is being used in a number of Canadian cities, such as Calgary and Ottawa.</p> |

| | |
|---------------------|---|
| | <p>The video features Shawna Coxon, a member of City of Toronto police service, describing how it works.</p> |
| <p>09:40</p> | <p><i>You will show the second video by the Toronto Police Service. The video will play for 4 minutes.</i></p> |
| | <p>That is why I am pleased that our officials </p> <p></p> <p>This brings me to the other priority area I would like to highlight from the Working Group's Action Plan </p> <p></p> |

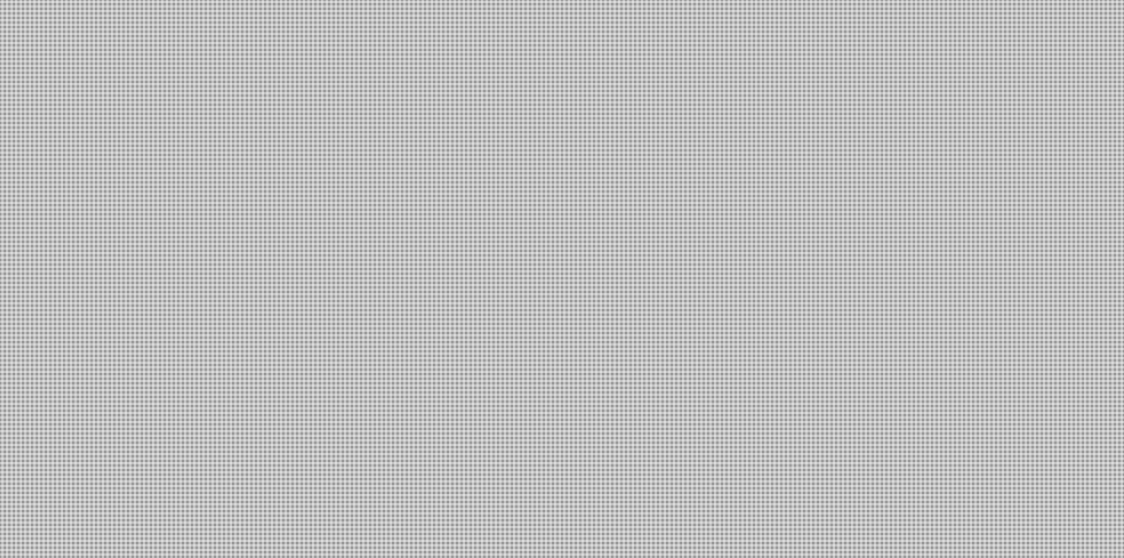
[REDACTED]

Consistent has been the strong, common focus on better understanding what works to address threats at the individual, group and community level.

For example, we know from research about lone actor terrorists and small group cells that close friends or family members often see meaningful signs of change before an attack or a decision to travel to a conflict zone. It is important, then, for community members to know what to do with this information, and feel comfortable coming forward to authorities.

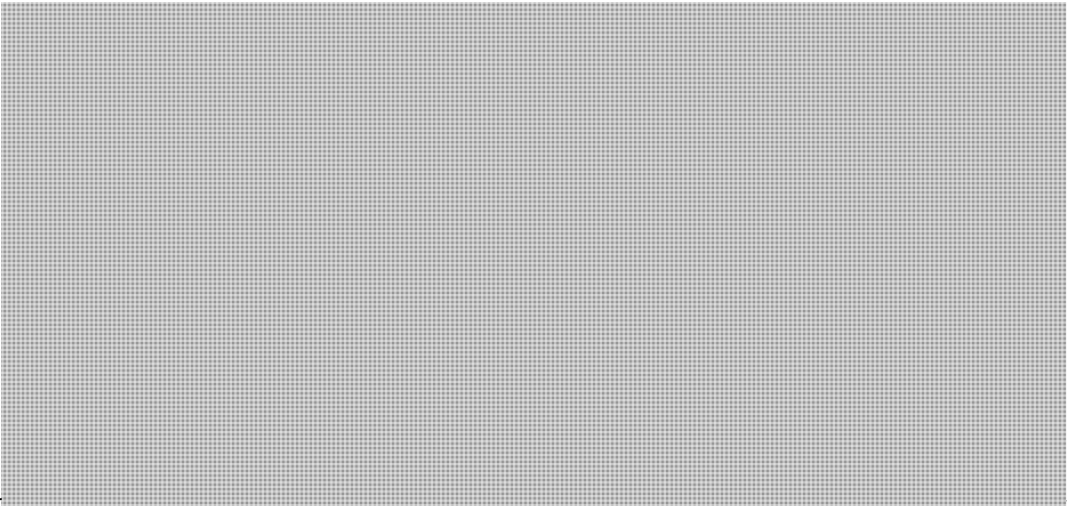
Relationships of trust with law enforcement and other professionals are crucial. Studies in Canada [REDACTED] [REDACTED] show the importance of effective community policing to build trust. We continue to improve on learning about what works to support those close to individuals at risk.

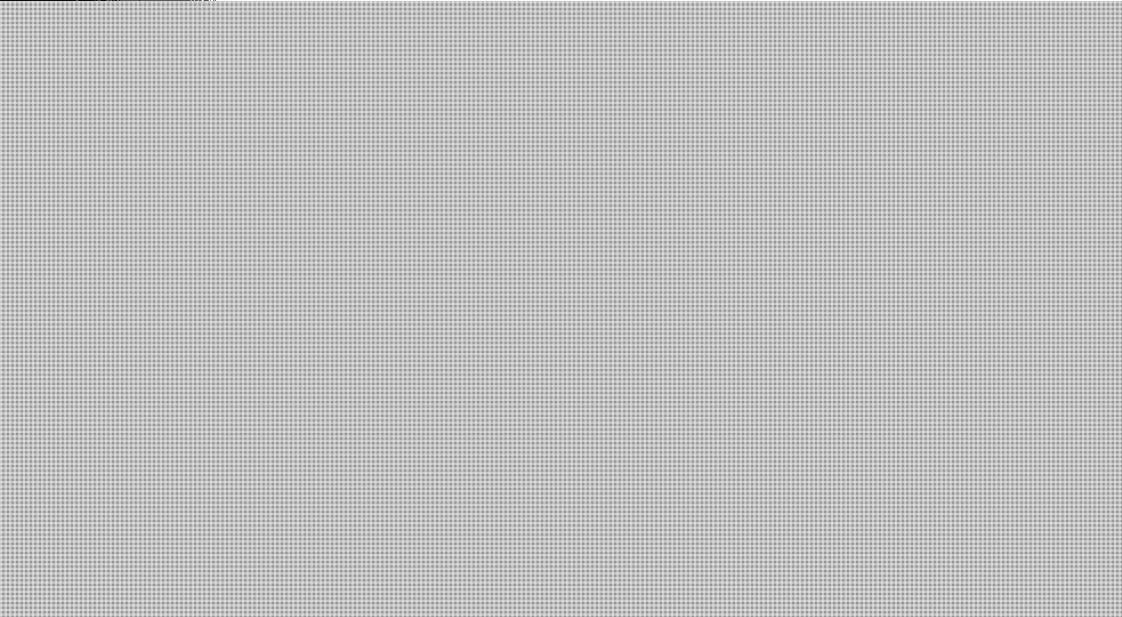
And I am encouraged that as part of the Action Plan [REDACTED]



This kind of research will directly support our efforts to bring better resources to those working on the frontlines of countering radicalization to violence.

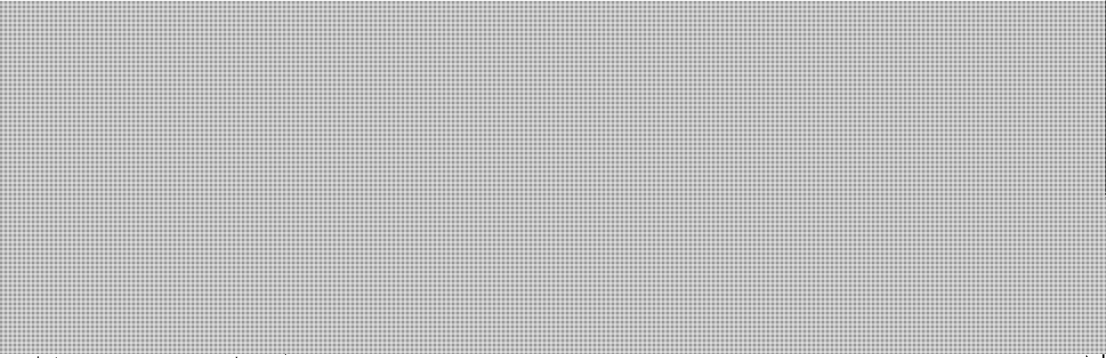
One of the reasons I am supportive of the Action Plan is because of how it will bring a stronger, more focused approach to working together on what works, and on bringing that knowledge to practice.





The Working Group has identified this as a priority area, and will look to advance work in the coming year.

For example, officials may facilitate discussions



They may also give space to civil society organizations, or other groups, such as youth, to channel their efforts into positive discussions to impact change.

Our next priority area in the Working Group's Action

| | |
|---------------------|--|
| | <p>Plan, [REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>Canada is open to doing more to address the online space, and we are open to discussing what should be done, such as increasing digital literacy of parents and youth, and supporting alternative narratives.</p> <p>[REDACTED]</p> |
| <p>09:50</p> | <p><i>Secretary Rudd will speak</i> [REDACTED]</p> <p>[REDACTED]</p> <p><i>Following Secretary Rudd's remarks, you will chair a discussion among Ministers.</i></p> |

I am supportive of engaging with communications service providers to hear about some of the innovative tools and methods they are using to direct away from violent extremist content.

On the issue of removal of online terrorist content, Canada has a legislative framework to remove online propaganda. To date, the legislation has not been used.

(Note: this line may need to be updated if there are public announcements on changes to Canada's national security framework.)

I am definitely supportive of any efforts by the major companies to support younger companies in how to deal with online terrorist content.

I am also supportive of efforts to engage civil society organizations to promote alternative narratives.

For example, in Canada we have invested in initiatives such as, Project SOMEONE.

This initiative is a web-based portal of multimedia materials aimed at preventing hate speech and building

resilience towards radicalization that leads to violent extremism.

The materials target youth, school and community members, public policy officials, as well as the broader public.


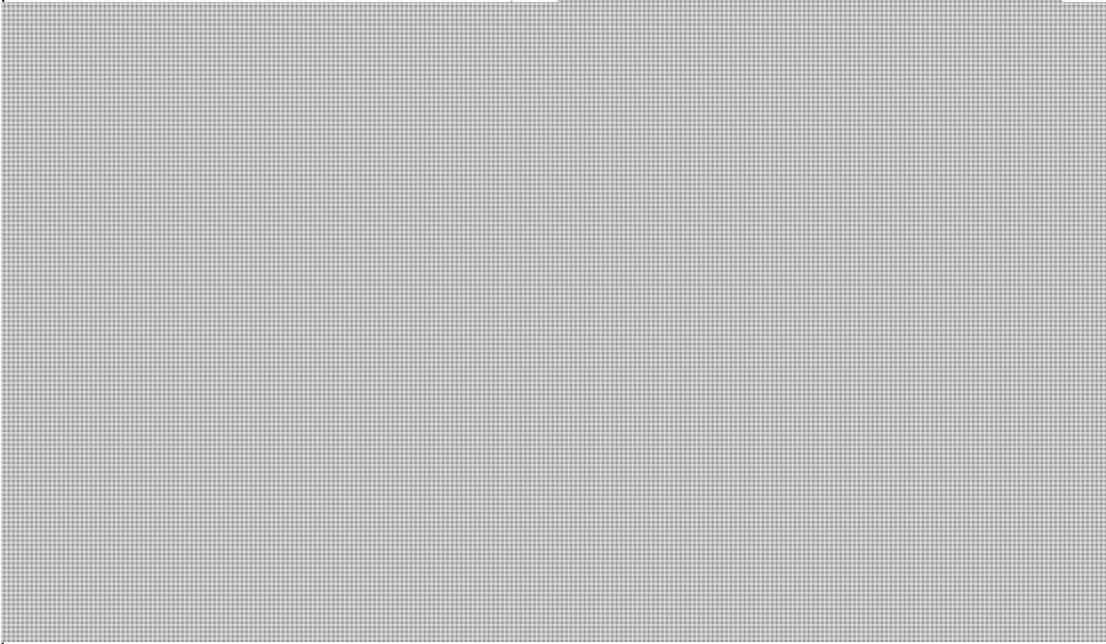

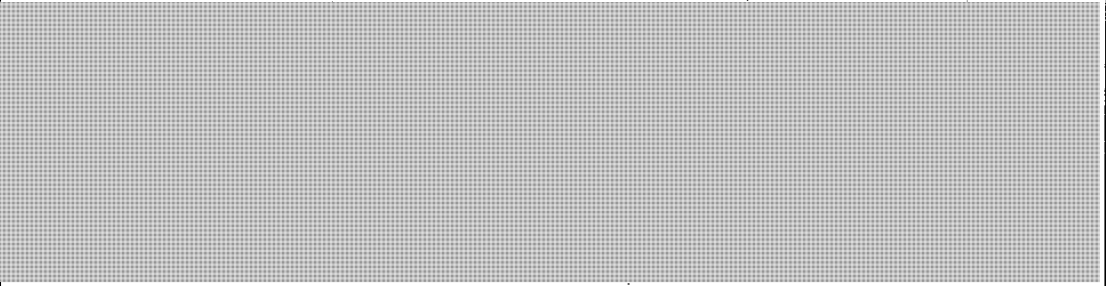
The focus of the materials is on the development of critical thinking and information literacy skills, and encouraging democratic dialogues in online and offline spaces.

These are the types of initiatives that we would be pleased to see private industry supporting.

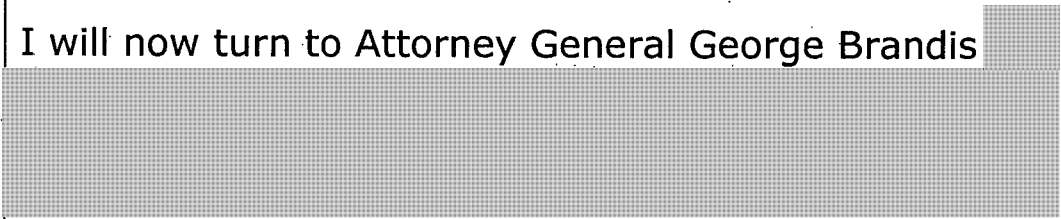
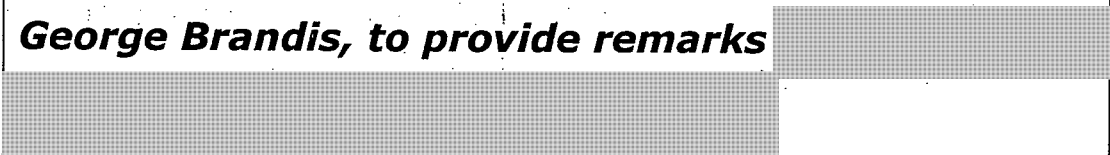
Of course, Canada is happy to work with the United Kingdom, as well as other keen partners such as the United States, to advance our CVE priorities with private industry.

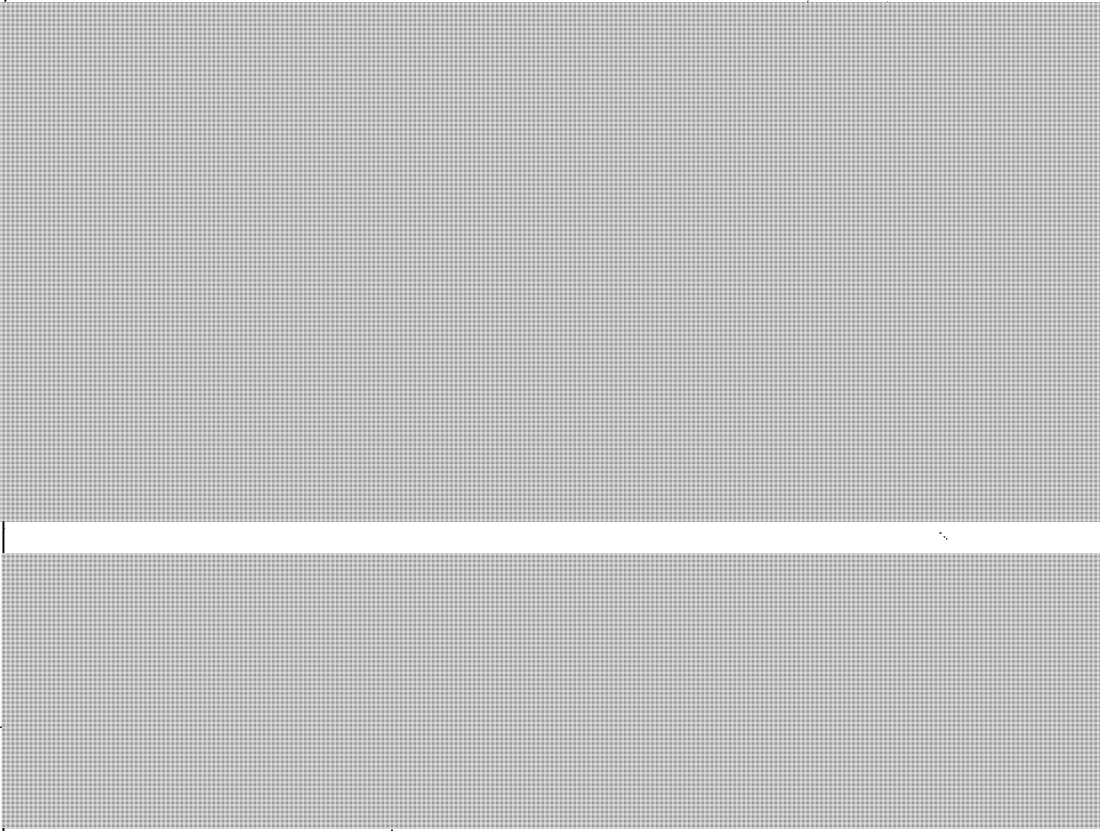
Responsive intervention

You may wish to respond with the following lines.

| | |
|---------------------|--|
| | <p>I understand and appreciate </p>  <p>Canada views the internet as a platform for free expression and dialogue, including diverse and dissenting points of view.</p> |
| <p>10:30</p> | <p><i>As the Chair of the discussion, you will close to the discussion</i> </p> |
| |  |

| | |
|--------------|---|
| 10:33 | <i>You will now open the session on</i> [REDACTED] [REDACTED] |
| | <p>The next issue for discussion is the last priority area in the Working Group's Action Plan – [REDACTED] [REDACTED]</p> <p>In Canada, we don't anticipate a large influx of returning foreign fighters as compared to what is being seen across Europe, for example; however we do recognize the threat these individuals may pose to Canadian communities.</p> <p>In particular, we must better understand the complexities relating to women and children who may be returning. Further, we must do our part to support the integration of these groups into their communities.</p> <p>Of course, Canada is a federation and we are working with our provinces and territories, as well as the local-level, to identify points of entry where we can support integration.</p> |

| | |
|--------------|---|
| | <p>That said, we are in the early stages to responding to this issue, and I look forward to hearing about your approaches.</p> <p>I will now turn to Attorney General George Brandis</p>  |
| 10:35 | <p><i>You will turn to the Australian Attorney General George Brandis, to provide remarks</i></p>  <p><i>Following Attorney General Brandis' remarks, you will summarize the agenda items and decisions.</i></p> |
| | <p>I think this discussion has been quite informative. I would like to summarize some of the decision points I think we have come to.</p> <p>My colleagues, I think there are compelling reasons to endorse this Action Plan, and I believe our officials have identified a number of initiatives that advance our international cooperation.</p> |

| | |
|--------------|---|
| | <p>If we are all comfortable with the Working Group's Action Plan, I think we can direct our officials to carry out the work in it.</p>  |
| 10:45 | <i>End of CVE session.</i> |

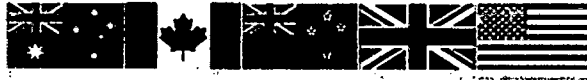
Tab 4C

s.15(1) - Int'l

s.21(1)(a)

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



FCM 2017 – Agenda Items

Countering Violent Extremism

DECISION SOUGHT / ACTIONS TO BE TAKEN

The Five Country Ministerial – Countering Violent Extremism Working Group has developed a draft action plan to advance key priority themes (see attachment). It is proposed that an overview document providing the key priorities articulated in the draft action plan is presented to Ministers for their endorsement, and potential public release in the form of a communiqué.

The meeting itself will focus on two priority areas articulated in the action plan, [REDACTED]

As part of first priority area, [REDACTED]

the forum are:

their three initial goals for

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



As part of second priority area on the issue of

DESCRIPTION

BACKGROUND

At their meeting in February 2016, Ministers approved:

RECENT DEVELOPMENTS

The Five Country Ministerial – Countering Violent Extremism Working Group met on March 7 and 8, 2017 to discuss common priorities and set an action plan to accomplish common objectives, which reflects the guidance provided by Ministers in February 2016.

CHAMPION/S

Canada will introduce the action plan and will set the stage with an overview of what we know, key knowledge gaps, and how joint research and evaluation efforts will be pursued in 2017-18 to address these needs.

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



ANNEXES

- CVE Action Plan Overview
- Detailed Action Plan
- International Industry-led Forum Background Paper
- Draft Joint Letter to CSPs

Tab 4D

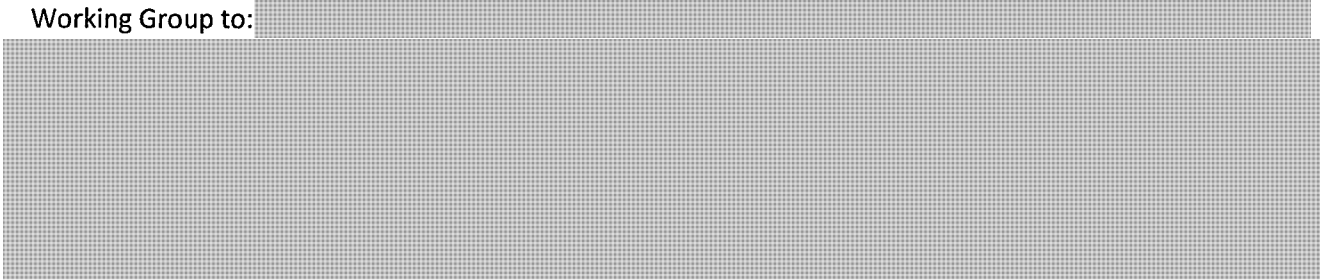
FOR OFFICIAL USE ONLY

DRAFT

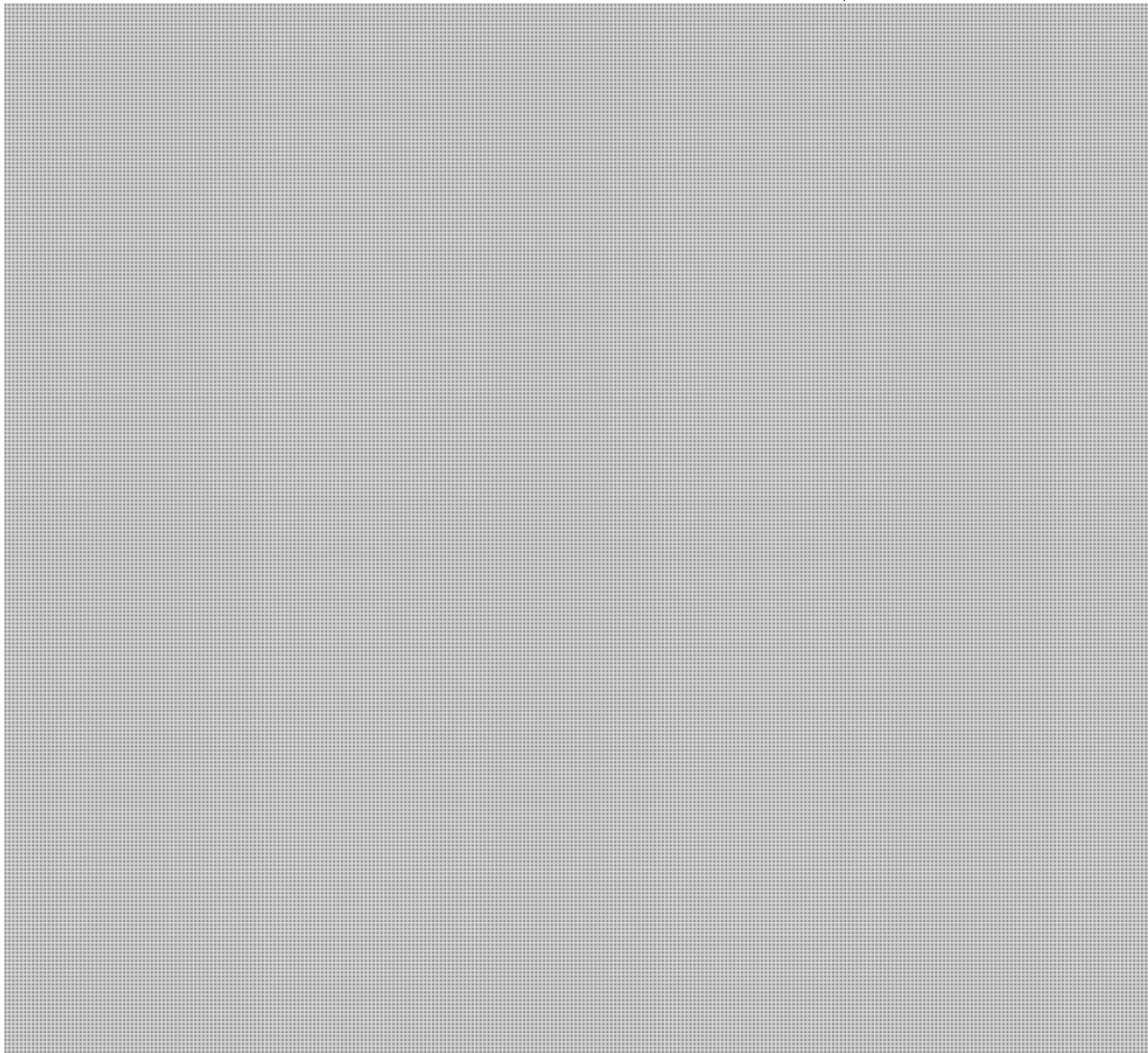
Five Country Ministerial – Countering Violent Extremism Working Group

Summary of Working Group Action Plan

In June 2016, Five Country Ministerial (FCM) Ministers directed the Countering Violent Extremism (CVE) Working Group to:



The outcomes within each five areas can be summarized as:



ANNEX 1

It is anticipated that following the June 2017 FCM meeting, a communiqué will be released on behalf of all Ministers.

DRAFT

Tab 4E

**Pages 500 to / à 504
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1) - Int'l

**of the Access to Information
de la Loi sur l'accès à l'information**

Tab 4F

International Industry-led Forum for tackling terrorist online content Background for Five Eyes Members

Major online Communications Service Providers agreed to take more responsibility to ensure the internet is not a safe space for terrorists to communicate and spread their propaganda. Companies publicly committed to establishing an international industry-led forum to tackle terrorist use of the internet.

1. On 30 March 2017 the UK Home Secretary, Amber Rudd, chaired a roundtable with Communications Service Providers (CSPs) including Google, Facebook, Twitter and Microsoft to urge them to be more proactive in tackling terrorist use of the internet.
2. [REDACTED]
3. Subsequent to the roundtable Google, Facebook, Twitter and Microsoft made a public commitment to look at options for establishing an industry-led forum focused on tackling terrorist and extremist content online.
4. Their three initial goals are:
 - to encourage the further **development of technical tools** to identify and remove terrorist propaganda
 - to **support younger companies** that can benefit from the expertise and experiences of more established ones
 - to **support the efforts of civil society organisations** to promote alternative and counter-narratives.
5. They are clear that this work must be global in nature and must also avoid duplicating existing efforts.
6. We hope to see the forum launch by the end of this year and will support industry to progress this work swiftly.
7. To ensure the success of this work and real investment by industry to this important issue we hope to secure [REDACTED] support for the forum and collective agreement on the initial priorities set out by the companies. A collective and consistent message from international partners will help us ensure momentum is maintained and companies have a clear mandate from the [REDACTED] community to make this forum a success.
8. In supporting this work [REDACTED] will also want to consider: sharing relevant research and analysis, encouraging small and emerging platforms in their nations to join the forum, sharing learning/best practice and expertise to help shape the forum.

Tab 4G

Page 508

**is withheld pursuant to section
est retenue en vertu de l'article**

15(1) - Int'l

**of the Access to Information
de la Loi sur l'accès à l'information**

Tab 5



Session 3

Refugees & Migration

Session Lead
Secretary Amber Rudd, United Kingdom

Participating Ministers

| | |
|-----------------------------|-----------------------|
| Peter Dutton | Australia |
| Ahmed Hussen | Canada |
| Jody Wilson-Raybould | Canada |
| Michael Woodhouse | New Zealand |
| Amber Rudd | United Kingdom |
| John Kelly | United States |

Tab 5A

FOR OFFICIAL USE ONLY

Public Safety
CanadaSécurité publique
Canada**FCM 2017 – Session III Scenario Note****Refugees and Migration****Sequencing**

CAN/Minister Goodale will welcome back the participants after the health break, and turn to the UK/Secretary Rudd.

UK/Home Secretary Rudd will introduce and the Refugees and Migration discussion (TAB 5B)

CAN/Minister Hussen will then introduce the Operation Syrian Refugees report (TAB 5C) and Canada's key lessons learned from the experience. He will also speak to international action on the migration crisis, including the development of the Global Compacts.

Then AUS/Minister Dutton will speak to Refugee Screening and Secretary Rudd will open the floor for discussion.

CAN/Minister Goodale will then introduce the topic of technology innovation at borders (TAB 5D), and open the floor for final comments.

CAN/Minister Goodale will close the discussion and invite the Ministers and Attorneys General to join him for a private lunch in the Director's boardroom.

Talking Points**IRCC/Minister Hussen key messages:**

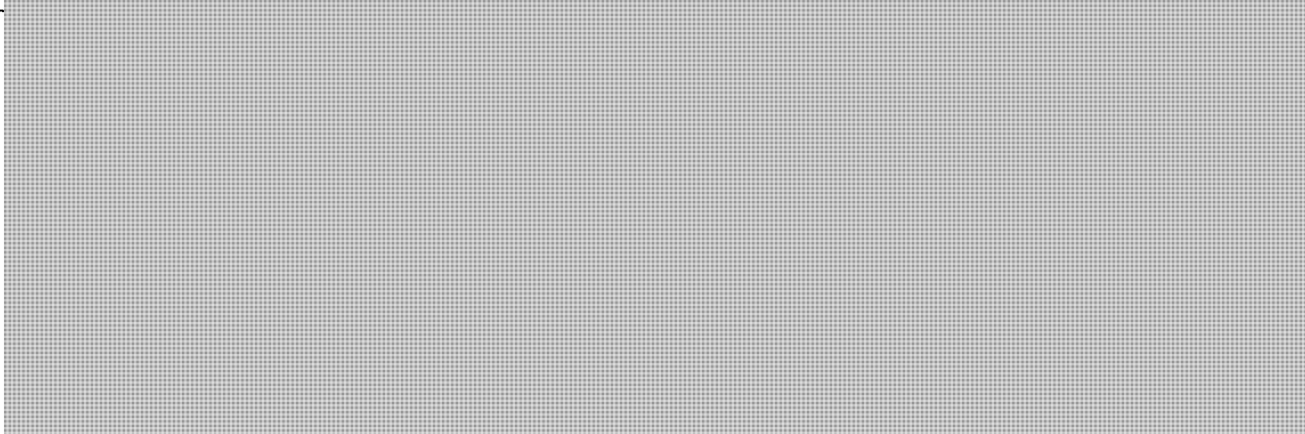
- To speak to the Operations Syrian Refugees Lessons Learned Report, which was a Canadian commitment from the 2016 FCM, and reinforce that large scale national responses to refugees can be well implemented without compromising security
- To underscore the positive societal contributions of immigration in contributing to Canada's well-being and economic prosperity, recognizing that immigration programs are not without risks and challenges.

FOR OFFICIAL USE ONLY



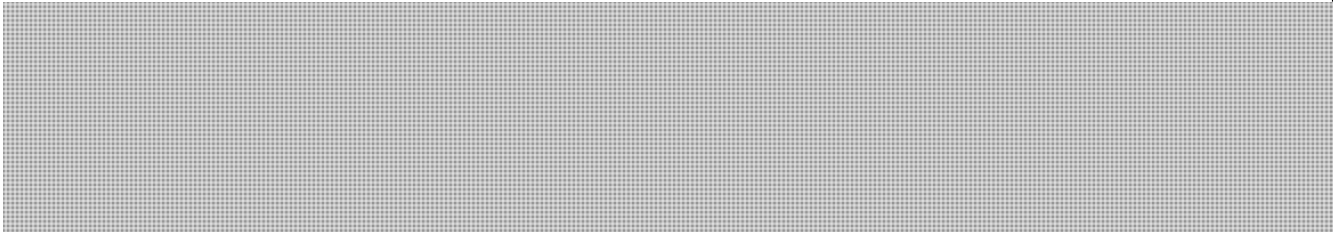
Public Safety
Canada

Sécurité publique
Canada



CAN/Minister Goodale on Border Technology

- **Ensuring the free and secure flow of legitimate people and goods through our respective borders is a shared Five Eyes priority. The use of border technology plays an increasingly critical role in meeting this objective.**



- **A first meeting of Border Five / Migration Five Information and Communication Technology officials was held in Canberra, Australia in March 2017.**



- **This forum was stood up to identify, assess and develop common solutions to shared border management challenges and explore transformational solutions that can be pursued jointly.**
- **It will also be important that the correct experts are identified to ensure that the legal, privacy, and policy implications surrounding identity management are identified and addressed in collaboration with the B5 and M5.**
- **I will firstly turn to my colleague Minister Hussen to share his views.**



Public Safety
Canada

Sécurité publique
Canada

Minister Hussen response to Border technology

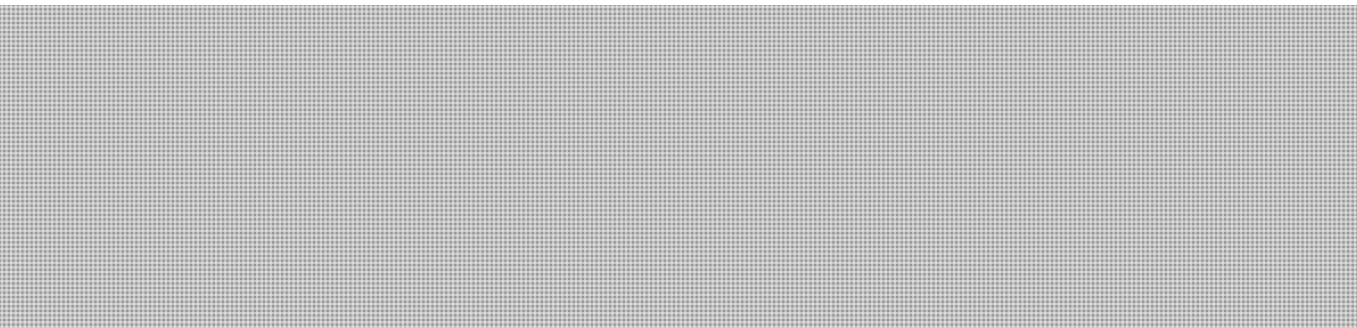
- *Technology underpins the work of my department and essentially all immigration programs. It is also needed to leverage our bilateral work on biographic and biometric information sharing and to conduct data analytics modelling that is being used to facilitate the identification of risk trends.*
- *I would support the proposal for the M5 and B5 initiative on border technology as a means to help us assess our respective investments in the coming years*

CAN/Minister Goodale after everyone has shared their view:

- **I will now close this Session on Refugees and Migration. Thank you to the UK and Australia for working on this proposal, and to everyone for making this session productive.**
- **This concludes the FCM only part of the day. This afternoon, we will begin the joint segment of our meeting with our Quintet colleagues.**
- **I would like to invite the Ministers, Secretaries and Attorneys General present to follow me to the Director boardroom for a private lunch.**

Expected Positions of the FVEY

Migration Flows/Global Compacts



Border Technology

Australia has shown a keen interest in this work; the Australian Border Force (ABF) is actively progressing toward their "Future Traveller Programme 2020" vision. Work is also being done on electronic boarding passes, i.e., the use of smartphones for boarding passes for international travel, as well as premium traveller facilitation services.

The **U.S.** will most likely have a great interest in the "border of the future" topic. As part of their

s.13(1)(a)

s.15(1) - Int'l

s.21(1)(a)

FOR OFFICIAL USE ONLY



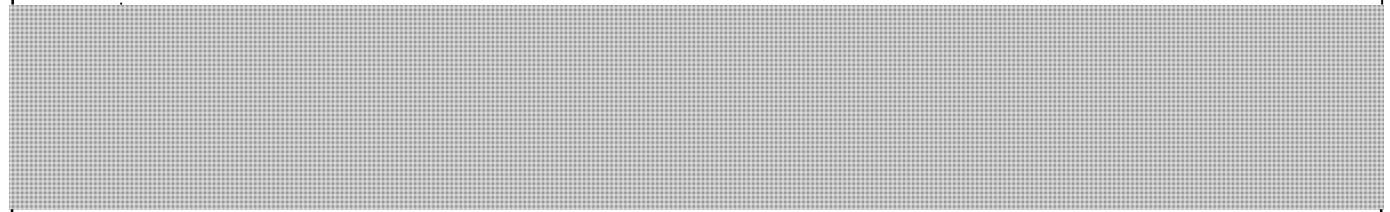
Public Safety
Canada

Sécurité publique
Canada

most recent aviation security strategy, the U.S will enhance Personal Electronic Devices screening, and deploy next-generation screening tools, such as computed tomography technology, to better detect threat items.

BACKGROUND

Border Technology



Canada and Australia launched an SRTP connection in April 2017

There is also interest in examining the feasibility of expanding membership of Trusted Traveller programs (such as NEXUS, Global Entry, Smart Gate, etc.) to all five countries with one application.

An analysis of the "border of the future" should build on the strategic work that Canada, the United States and Australia have already conducted. This analysis should focus on how border technologies such as facial recognition, smart-gates, and border kiosks can be securely integrated with biometrics, while also enabling intelligence to flow to border front line officers in real-time.

Tab 5B

FOR OFFICIAL USE ONLY
FIVE COUNTRY
MINISTERIAL



the UN Offices in Geneva, New York and Vienna, and other regional migration meetings will feed into the process.

This global compact on migration will continue to be discussed in a variety of international forums throughout the year.

Screening

SUGGESTED COMMUNIQUÉ LINE

CHAMPION/S

United Kingdom, Canada, Australia

ANNEXES

- *Canadian Syrian Refugees Report*
- *Innovation and Border Technology*
- *Trusted Traveller Update*
- *Secure Real-Time Platform Progress Chart*

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(a)

FOR OFFICIAL USE ONLY

FIVE COUNTRY
MINISTERIAL



vetting, including biometric exchanges through the Secure Real Time Platform, have demonstrated considerable value for immigration and border agency partners.

Further discussion will focus on how the five countries can advance facilitating the flow of known travellers in as seamless a way as possible, while maintaining the integrity of our borders.

BACKGROUND

The international movement of people is having a profound impact globally which is felt in all five countries. Our challenge is to find long-term and sustainable solutions that advance planned, comprehensive national migration systems, while at the same time addressing irregular migration challenges

While there may be little international appetite for a new global governance regime on migration, we have the opportunity to develop new and innovative responses to the high level of migration. As world leaders in migration, we can work together on encouraging states to develop planned, comprehensive migration systems that will benefit both the countries and migrants, as well as coordinating our approaches to combating human smuggling and trafficking.

On refugee screening, the foundation for biometric checks between border agencies for vetting purposes is well established.

RECENT DEVELOPMENTS

Refugees / Migration

On 19 September 2016, the UN Secretary General held a High Level Event on Large Movements of Refugees and Migrants. States adopted the New York Declaration for Refugees and Migrants – and committed to launching a process of intergovernmental negotiations leading to the adoption of a Compact on refugees and a Compact on safe, orderly and regular migration before the end of 2018.

The Comprehensive Refugee Response Framework (CRRF), annexed to the New York Declaration, sets out the operational framework for the Refugee Compact. The outcomes of pilot responses, thematic consultations, and negotiations will culminate in the presentation of the Refugee Compact to the UN General Assembly for adoption in 2018.

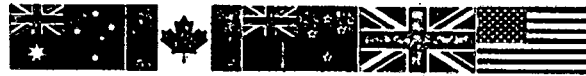
A UN modalities resolution adopted in March 2017 paves the way for formal consultations on the Migration Compact between April 2017 and January 2018. Six thematic sessions are being held at

s.15(1) - Int'l

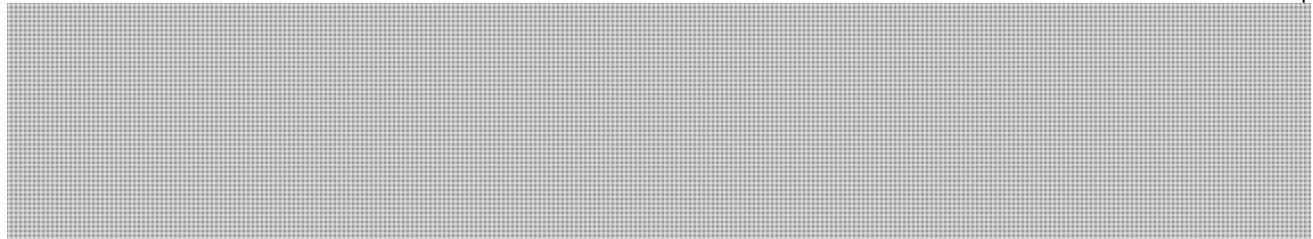
s.21(1)(a)

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



pace with evolving threats and take advantage of new opportunities, Ministers may consider directing officials to:



Finally; Ministers to take note of the Canada's Lessons Learned Paper on Operation Syrian Refugees, and how it achieved resettlement of 25,000 refugees in a three month period. This initiative demonstrates that it is possible to undertake significant refugee resettlement in ways that do not compromise security and these lessons may inform future responses to addressing refugee flows.

DESCRIPTION

Over 244 million people are international migrants; 21.3 million of whom are refugees. While a majority of people who migrate use legal channels to seek a better life, pursue studies, or reunite with their families, there are also people genuinely seeking protection elsewhere (fleeing persecution or other harms, escaping civil unrest and war, etc.), while others are searching for new economic opportunities and travelling through irregular channels. These movements contribute to humanitarian and security challenges, making migration one of the most pressing issues of our time. Current migration and refugee systems in many countries are not able to cope with the scale of international migrants. These systems are neither meeting the urgent needs of those seeking refuge, nor the aspirations of other migrants, and can contribute to instability in countries of origin, transit and destination.

With regard to refugees, Canada's lessons learned report on their experience of resettling 25,000 Syrian Refugees in a three month period will provide Ministers with an idea of what our countries can achieve in situations where the decision is that resettlement is the preferred option, and an indication of some of the challenges in implementing such an initiative.

The process launched at the UN General Assembly last year to negotiate two new Global Compacts on refugees and on safe, orderly, and regular migration – to be adopted in September 2018 – aims to increase international cooperation on migration and refugees and is an opportunity to develop planned and comprehensive national migration systems and address irregular migration, whilst providing more support to those in need. Well managed legal migration can enhance economic, social and cultural benefits for both countries of origin and destination, and poverty reduction in low income countries, yet can also pose significant challenges. We also need to tackle irregular migration, including by addressing drivers and instability in source and transit countries as well as understand and address pull factors to destination countries.

With regard to security screening, cooperation between our countries on migrant and refugee

FOR OFFICIAL USE ONLY

s.15(1) - Int'l

s.21(1)(a)

FOR OFFICIAL USE ONLY

FIVE COUNTRY
MINISTERIAL



FCM 2017 – SESSION III

Refugees/ Migration/ Screening

DECISION SOUGHT / ACTIONS TO BE TAKEN

- Recognize States have the sovereign right to control their own borders effectively
- Maintain a clear distinction between refugees (and others who qualify for protection under national and international law) and economic migrants

Thirdly; This agenda item will also consider the work of the Migration 5 resettlement working group, progress made on enhancing screening processes and the opportunities to further utilise non-traditional screening techniques to support more robust decision making, including social media and open source materials.

FOR OFFICIAL USE ONLY

Tab 5C

FIVE COUNTRY
MINISTERIAL



**Canada's Operation Syrian Refugees:
Lessons Learned**

Canada's Operation Syrian Refugees – Lessons Lear

In the fall of 2015, responding to the humanitarian crisis in the Middle East and calls from the Canadian public, Immigration Refugees and Citizenship Canada (IRCC) began plans to resettle 10,000 Syrian refugees by September 2016. Planning was well underway, when in November 2015 the Canadian government made a subsequent commitment to resettle 25,000 Syrian refugees by February 29, 2016. The initiative was called Operation Syrian Refugees (OSR).

While the timelines for this commitment were extremely ambitious, Canada mobilized resources from all non-urgent business to focus on this national project and worked with the United Nations High Commissioner for Refugees (UNHCR) to identify a large number of registered refugees that could potentially be resettled within the identified timeframe. Working with existing and former departmental personnel and trusted partners further helped manage the scope of this significant endeavour.

To ensure that the operation would meet its objectives, the Federal Emergency Response Plan (FERP)¹ was invoked to facilitate coordination among federal departments and external partners. More than 10 federal departments and agencies were directly involved in the operation.

Canada had resettled large numbers of refugees quickly before. For example, in 1972, almost 7,000 Asian refugees were resettled to Canada from Uganda; in 1979, 60,000 Indochinese were resettled in Canada, and in 1999, 5,000 Kosovars were airlifted to Canada. However, none of these approached the scale and timelines of Operation Syrian Refugees. This operation, especially to maintain appropriate security and screening standards, required a resource intensive, expedited process that was unique from the other large-scale resettlement initiatives previously undertaken by Canada.

Refugees Supported Under Operation Syrian Refugees (OSR)

| Breakdown by category | Number of Syrian refugees |
|--|---------------------------|
| Government-Assisted Refugees (GAR) | 14,994 |
| Privately-Sponsored Refugees (PSR) | 8,954 |
| Blended Visa Office-Referred Refugees (BVOR) | 2,224 |
| Total | 26,172 |

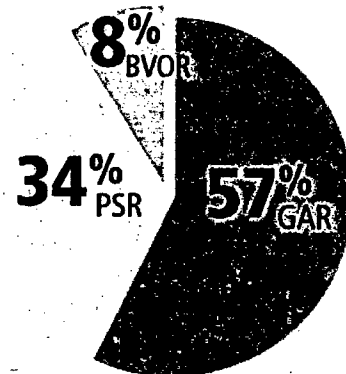


Figure 1. Breakdown by refugee category

In total, 26,172 refugees arrived in Canada between November 4, 2015 and February 29, 2016. Refugees coming to Canada fall into one of three categories: Government-Assisted Refugees (GAR), Privately-Sponsored Refugees (PSR) and Blended Visa Office-Referred Refugees (BVOR). GARs are supported by the

¹ The Federal Emergency Response Plan (FERP) is the Government of Canada's "all-hazards" response plan. It provides a framework for effective integration of effort both horizontally and vertically throughout the Federal Government. It also provides the mechanisms and processes to coordinate the structures, the capabilities, and the resources of federal government institutions, non-governmental organizations and the private sector into an integrated emergency response.

Canada's Operation Syrian Refugees – Lessons Learned

Government of Canada (or the province of Quebec²) for the first twelve months after arrival. PSRs are supported financially and emotionally for twelve months by non-government organizations or groups of private individuals who demonstrate the capacity and desire to undertake the sponsorship. Support for BVORs is shared between the Government of Canada and private sponsors, with government financially responsible for the first six months and the private sponsor the latter six months, plus twelve months of social and emotional support.

Most Syrian refugees came to Canada via Lebanon (54%), Jordan (34%), and Turkey (9%) and arrived by government chartered planes at Toronto Pearson Airport or Pierre Elliott Trudeau Airport in Montreal. From these two hubs, refugees were welcomed in over 250 communities across the country, settling in 10 Canadian provinces and one territory.

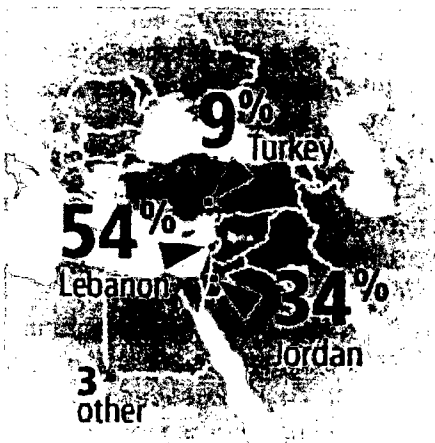


Figure 2. Countries of immediate origin

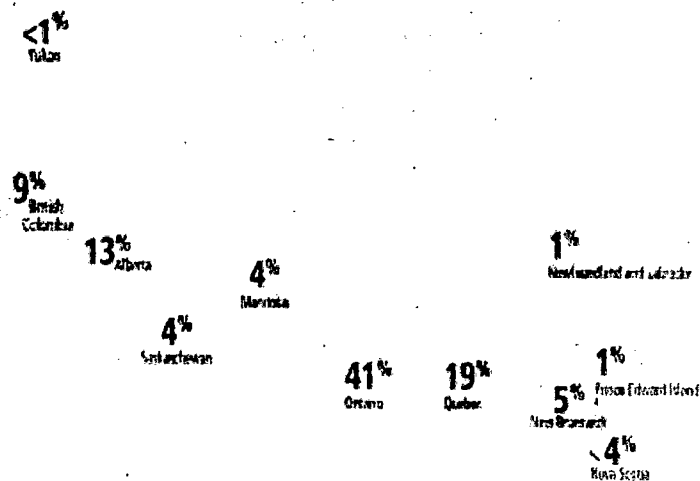


Figure 3. Distribution of refugees across Canada

Approach to Operation Syrian Refugees (OSR)

The process for resettlement of the refugees took place in the five phases:

1. Identifying Syrian refugees to come to Canada

In November 2015, Canada had several thousand mainly Privately-Sponsored Refugee applications already in process that were expedited through this initiative. Canada then worked with the UNHCR in Jordan and Lebanon and with State officials in Turkey to identify Syrian refugees in their databases to be resettled in Canada. To allow visa officers to focus interviews on security, criminality and medical screening, unless there was evidence to the contrary, visa officers were to presume that Syrians fleeing the conflict met the definition of a genuine refugee³. Therefore, the criteria used was that the individual

² Quebec receives federal block payments from the Government of Canada to support their independent immigration program.

³ Although the UNHCR had not formally designated Syrians fleeing the conflict as *prima facie* refugees (the UNHCR's comprehensive delineation of every subset of society as convention refugees) the situation amounted to a *prima facie* eligibility situation from Canada's perspective.

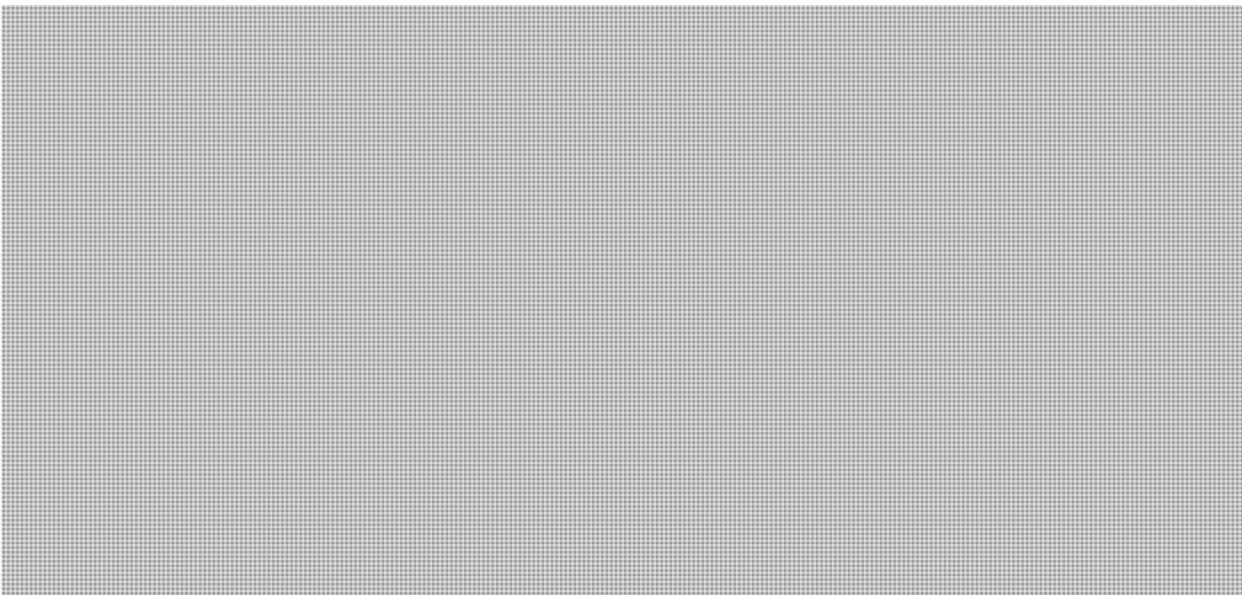
Canada's Operation Syrian Refugees – Lessons Learnt

was a Syrian national or stateless person who was a former resident of Syria, living outside of Syria, and registered with the UNHCR or the government of Turkey.

Canada identified triage considerations which were provided to the UNHCR to assist in identifying the most vulnerable persons, while aiming to screen out those more likely to pose risks. This process prioritized complete families, women at risk, and LGBTI cases. Unaccompanied minors or separated children, persons inadmissible under Canadian legislation (e.g. polygamous marriages, security concerns), and single adult males of fighting age⁴ were not considered for this project.

2. Processing Syrian refugees overseas

Immigration processing was completed in Amman, Beirut and Turkey. Global Affairs Canada provided whole-of-government coordination for the deployment abroad and subsequent repatriation of a total of 1,095 Canadian personnel who served at different times during OSR, including members of Canada's Department of National Defence, who provided support to the process. In Beirut and Amman, Canada established stand-alone Operation Centres, to streamline processing, providing space that the Embassies lacked and putting partners under one roof to efficiently reduce the number of interactions necessary per application. Clients completed their application forms with English-Arabic speaking contractors to reduce errors, save time, and accommodate the issue of illiteracy. Documents were then scanned and further, both strategically and randomly, checked for fraud by on-site Canada Border Services Agency (CBSA) experts. The International Organization for Migration scheduled interviews for refugees with Canadian immigration officers. CBSA and Public Safety experts were available at the Operations Centres for immigration officers to consult, also providing interview support to the officers. Full medical immigration screening was done for communicable diseases such as tuberculosis. CBSA, in collaboration with our national security agencies, conducted and processed security screening on all applicants in accordance with domestic legal frameworks and international arrangements. For instance, biometrics, such as fingerprints and digital photos were collected and checked against immigration and security databases.



⁴ Exceptions were made for LGBTI individuals or those residing with their parents/siblings as part of complete family units. Fighting age was defined as 18-55 years-of-age.

Canada's Operation Syrian Refugees – Lessons Learned

3. Transportation to Canada

Canada engaged with host countries to rapidly facilitate exit permits, including for example, paying exit fines for refugees who were out of status in Lebanon. Transportation to Canada was largely by private charter aircraft (after two initial military flights). Before flights departed, Canada Border Services Agency (CBSA) officers confirmed the identity of boarding refugees. Preparing the flight manifests and matching them with the travel documents, travellers, and exit permits was an enormously complicated and time-sensitive task. Global Affairs Canada and CBSA supported over 150 Operation Syrian Refugees flights by liaising with partner countries in the Middle East and Europe to obtain diplomatic clearances and permissions for overflight, landing and/or refuelling.

4. Welcome in Canada

Charter flights arrived in Toronto or Montreal at airport terminals that had been specifically retrofitted to welcome hundreds of refugees per day. Following arrival in these Welcome Centres, all refugees were processed by CBSA officers for admission into the country. This included final verification of identity and screening for signs of illness. As per the Immigration and Refugee Protection Act, refugees were granted Permanent Resident status upon arrival, and began their settlement process with the support of service providers and other government agencies that were co-located in the airport Welcome Centres.

5. Settlement and community integration

After arrival, Privately Sponsored Refugees (PSRs) and Blended Visa Office Referred Refugees (BVORs) continued directly to the community where their private sponsor was located. Government Assisted Refugees (GARs) were matched with communities where settlement supports were in place. Most continued to their new home communities across Canada shortly after arriving in the country. For those whose final destination had not been determined by the time they arrived, temporary accommodation was provided until they were moved to their host communities.

For GARs, various services were made available to help them become participating members of Canadian society as quickly as possible. These services are provided by specialized Service Provider Organizations (SPOs) and include:

- port of entry services at the airport Welcome Centres such as providing winter clothing and onward travel coordination; interpretation/translation; temporary accommodation, including meals and a small amount of money;
- support from resettlement service providers in destination cities for general orientation, including introduction to public transit, shopping, mail, emergency services; financial orientation, including explaining Canadian currency, budgeting, opening a bank account; links to federal and provincial programs, including how to obtain a provincial health care card and driver's license; information and orientation services that help newcomers settle in their community and integrate into Canadian society, counselling, information on gender equality, and orientation sessions on life in Canada.

Private Sponsors provided similar orientation and services for PSRs and BVORs. All three groups of newcomers have access to help in finding and retaining employment and English or French language training.

Canada's Operation Syrian Refugees – Lessons Learnt

Federal Spending on Operation Syrian Refugees and Other Contributions

In 2015-16, the Government of Canada spent approximately CAD \$385 million on this initiative⁵, which was \$70.3 million less than planned. Lower costs for transportation and overseas processing, in addition to unused contingency funds, all contributed to the initiative coming under budget. These figures include a \$100-million contribution made by Canada to the UNHCR to meet the needs of people affected by the Syrian refugee crisis, of which \$10 million was allocated to help the Refugee Agency select eligible Syrians for resettlement in Canada by February 2016.

Support of Canadians

The broad support for this initiative among Canadians was reflected in the millions of dollars in financial and in-kind contributions made by non-federal, non-governmental, and corporate partners. For example, to support Syrian refugees arriving in the country, Canada's five major banks donated a total of \$1-million to the Canadian Red Cross and Canadian National Railway donated \$5 million to the Welcome Fund for Syrian Refugees. Other organizations provided services, including information and referral services to ongoing community supports such as language classes, translators, community-based mental health care, medical services and long-term accommodations.

Individual Canadians also donated about \$32-million to charitable organizations providing relief to Syrian refugees, which the Government of Canada matched with an equal contribution to the United Nations Children's Fund (UNICEF).

Best Practices of Operation Syrian Refugees (OSR)

Taking a Horizontal Approach

Resettling over 25,000 refugees in Canada between November 4, 2015 and February 29, 2016 was made possible by the coordinated efforts of multiple federal organizations, the UNHCR, the International Organization for Migration, the governments of Lebanon, Jordan and Turkey, provincial, territorial and municipal governments in Canada, non-governmental organizations (NGOs), corporate and community private sponsors, as well as the broad support of Canadians across the country. This level of collaboration was unprecedented in Canada and necessary given over 250 communities across Canada have welcomed refugees. The Government of Canada provides settlement services to refugees through several hundred Immigration, Refugees and Citizenship Canada-funded service provider organizations in large and small communities across Canada. The initiative was able to bring together the necessary goodwill, expertise and capabilities from local, national, and international levels into a coordinated effort. In the Canadian context, national security is a shared responsibility among many federal, provincial and municipal organizations. Coordination among all public safety experts was essential.

Establishing a Governance Structure and Operations Focal Point

The implementation of the Federal Emergency Response Plan (FERP) was an effective way to organize the various departments and agencies involved in this operation. This tool defined the roles and responsibilities of each federal organization based on their respective enabling legislations and fields of expertise. Despite initial unfamiliarity by many with this response plan mechanism, it did provide a clear governance structure, which assisted the decision-making process. The Canada Border Services Agency nominated their Vice President of Operations as their agency's FERP lead. Given his in-depth operational and tactical knowledge,

⁵ Figures include \$80.9M in expenditures that departments absorbed within existing funding levels.

Canada's Operation Syrian Refugees – Lessons Learned

he could act as a 'Strategic Information Hub' to share key information to all relevant actors. This improved communication and reduced the pressure on all CBSA staff and interlocutors.

The Government Operations Centre⁶ (GOC) was also engaged early on to help ensure a rapid response and ongoing coordination between the range of partners. The use of the Centre as the coordination mechanism for Phases Four and Five to ensure smooth operations was well-received by stakeholders and departments. To meet the 24/7 demands of OSR, the GOC added 250 surge staff to their existing personnel. Also, keeping the media and Canadians informed and engaged through public events and announcements was key to the successful reception of the refugees.

Appointing of a Special Coordinator

Along with creating governance structures at the highest levels for the OSR initiative, the federal government created the temporary position of Special Coordinator for Syrian Refugees at IRCC and filled it with a respected and experienced former senior government official. The Coordinator served as the public face of the initiative, facilitating stakeholder coordination and building momentum among provinces, territories, municipalities, settlement and resettlement agencies, the voluntary sector, and private sector. She conducted outreach to help disseminate timely information and build commitment among all parties who would welcome Syrian refugees to Canada. Under her leadership, services were coordinated with the aim of providing timely, targeted delivery and a smooth transition for arriving refugees and their communities.

Using the International IRCC Network Effectively

Coordinated parallel processing by IRCC offices in Canada and in missions abroad, in conjunction with the Operations Centres and embassies in the operations zone, allowed OSR to progress around the clock. For example, at 6 pm Beirut time, Ottawa came online and staff would open the day's electronic client folders and create e-clients, generating case numbers, and populate all the processing fields in the Global Case Management System⁷. The Canadian Embassy in Paris provided liaison with the Government of Quebec⁸, and the Canadian Embassy in Mexico provided additional data entry of security forms for older applications that had not been completed at Operations Centres.

⁶ The Government Operations Centre (GOC) provides an integrated federal emergency response to events of national interest. It provides 24/7 monitoring and reporting, national-level situational awareness, warning products and integrated risk assessments, as well as national-level planning and whole-of-government response management.

⁷ The Global Case Management System is Immigration, Refugees and Citizenship Canada's single, integrated and worldwide system used internally to process applications for citizenship and immigration services.

⁸ The Government of Quebec manages their own immigration intake, the rules for which are set out in the Canada-Quebec Accord.

Canada's Operation Syrian Refugees – Lessons Learnt

Operating Under One Roof

Overseas Operations Centres were established in Jordan and Lebanon bringing all components necessary for applicant processing under a single roof. Refugees were transported to these centres on International Organization for Migration (IOM) buses for a single day of contact with immigration officials. On the day of contact, refugees completed an identification check, biometric requirements, photos, documents and forms, and their interview. Planning and implementing a single streamlined encounter significantly reduced



Amman Operations Centre

processing times. Additionally, it facilitated communication between the various government and non-government officials involved in the process and it also made it easier for refugees to navigate the complexities of the process. Completing steps such as interviews and medical and security screening concurrently was one of the key adaptations that allowed the government to process more than 25,000 Syrian refugees in roughly 100 days, well above normal processing. For example Canada's level target for 2017 is 40,000.

Lessons Learned

Processing Times & Pre-Arrival Services

Drop-outs can always be expected in such initiatives, however giving refugees more time to settle their personal affairs prior to departure could reduce these incidents. By the time refugees first met Canadian officials they had already fled their homes, leaving most of what they held dear behind. Travel to Canada also meant saying goodbye to family, friends, and place of refuge. A lesson for Canadian officials was that even in urgent situations it is possible for processing to be too rapid. The experience on the ground was that some refugees declined resettlement because the process was too rapid. Others who did accept resettlement experienced hardship in being swiftly uprooted from refugee communities and extended family, and were unable to dispose of belongings. Also, the rapid process at times inhibited the refugees from participating fully in pre-arrival services.⁹ As a result, refugees' understanding about life in Canada were at times incorrect, and contributed to some refugees deciding not to travel.

⁹ The Canadian Orientation Abroad (COA), is funded by IRCC and delivered by the International Organization for Migration (IOM). Prior to departure, a general orientation to Canada is provided, including an overview of what to expect on the way to, and after arrival in, Canada; looking for work; rights and responsibilities; culture; money; housing; how to access services; health care; education; etc. Refugees generally receive a 3- or 5-day sessions depending on the needs of the group. A COA Handbook is provided to each participant as part of the session. The Canadian Orientation Abroad was not initially a planned service as part of Operation Syrian Refugees and many refugees did not receive it. Some were able to attend question and answer sessions with COA specialists and the others were given the Handbook at the airport prior to departure. This resulted in newcomers arriving in Canada having gaps in knowledge and arriving with inaccurate assumptions.

Canada's Operation Syrian Refugees – Lessons Learned

Lesson: After February 2016, Syrian refugees approved for resettlement generally travelled four to eight weeks following a positive decision on their case. This provided them with sufficient time to conclude their affairs, to say their good-byes and to receive some initial orientation about life in Canada.

Cross Referenced Files

Linked cases¹⁰ were often identified at the interview stage, and sometimes even as late as after arrival in Canada. As a result, some families were not prepared to depart for Canada due to extended family members waiting for processing. Additionally, rapid processing for one part of a family and slower timelines for another often meant that even linked extended family members were sometime separated (for example, elderly family members needing additional medical screening).

Lesson: In future rapid operations, IRCC should have more robust plans and procedures to link extended family early in the process and as much as possible, keep them together through settlement phase in Canada.

Arrivals in Canada

Focusing on two ports of entry, namely Toronto Pearson International Airport, and Montréal–Pierre Elliott Trudeau International Airport, worked well. Upon arrival, refugees were welcomed and processed for admission to Canada by Border Services Officers who confirmed identities and conducted customs and immigration inspections. Refugees were also processed for immigration identification documents, checked for signs of illness as per the Quarantine Act, issued Interim Federal Health Program certificates to ensure refugees had medical coverage. They left the airport process as permanent residents of Canada.

Lesson: Consideration should be given to arrival times in Canada. Late evenings/middle of the night arrivals, resulted in congestion, overtime and staffing issues.

Transitioning from Temporary to Permanent Housing

Securing permanent accommodation for this refugee group was challenging for Service Provider Organizations (SPO) and communities. Finding appropriate and affordable housing was particularly difficult for Syrian refugee families that were significantly larger (compared to other refugee cohorts). Larger homes can generally be found in smaller communities, but those communities often do not have the full range of settlement services. In addition, approximately 46% of the 25,000 Syrian GARs that arrived to Canada between December 2015 and February 2016 are children under 14 years of age. Many GAR families stayed in hotels for several weeks before being transported to their settlement community. The initial lack of activities to engage these youth was a significant challenge for families.

Lesson: Analyze and distribute refugee family resettlement information widely to SPOs and provinces/territories and as early as possible to better support planning and arrival/settlement preparation activities, including accommodation in tight urban housing markets. In situations where a very large number of minors are arriving in Canada at once, activities and programming should be planned and implemented in temporary accommodations, even if they are only residing there for a short time.

Communication of Accurate and Complete Refugee Settlement Requirements

Accurate refugee profile information that allows for the mobilization of appropriate resources, including accounting for particular settlement challenges (e.g. high medical needs, large family sizes) of the incoming

¹⁰ Situations where extended family units were processed separately. E.g. an elderly parent processed independent of her children and their families when they want to travel and be settled together.

Canada's Operation Syrian Refugees – Lessons Learnt

population was not always fully collected by immigration officers for other partners and stakeholders. These information gaps had an impact on the preparation for arrivals that contributed to challenges in planning and developing the necessary resources (i.e. specialized programming or supports) to provide timely and targeted services to these refugees. The shift of immigration officers every few weeks aggravated this situation.

Lesson: Ensure the necessary training, quality assurance checks of interview notes, and follow up with officers to ensure the collection and compilation of comprehensive, accurate information (profile, destining, and arrivals) to IRCC staff, partners and stakeholders to ensure effective resettlement planning.

Follow Up on Operation Syrian Refugees

Since OSR, Canada has continued to resettle more Syrian refugees and evaluate their progress in settling into Canadian society. As of January 29, 2017, over 40,000 refugees had arrived in Canada. The Government of Canada continues to monitor the progress of all refugees resettled during this initiative.

A Rapid Impact Evaluation (RIE) was conducted by Immigration, Refugees and Citizenship Canada to assess the early outcomes of the Operation Syrian Refugees. The evaluation was targeted in nature and examined the Syrian refugees admitted to Canada between November 4, 2015 and March 1, 2016 and who were part of the 25,000 Syrian refugee commitment. Data collection took place between June and September 2016, and included focus groups with Syrian newcomers, surveys with adult Syrian refugees, as well as other key lines of evidence. Early indicators show that Syrian newcomers are generally integrating into Canada at the same rate as previously resettled refugees. At the time of the survey in mid-2016, many of the Syrian refugees resettled by March 1, 2016 had begun using settlement services, including a high number of adults

attending information and orientation sessions, and receiving a needs assessment and referrals for services. Around half of adult Privately Sponsored Refugees (PSRs) had found employment, compared to 10 per cent of Government Assisted Refugees (GARs). The vast majority of Syrian refugees who were not working at the time were looking for work or intended to look for work in the near future. It should be noted however that only a little over 44 per cent of refugees who entered



Syrian Family Arriving in Canada

Canada were of full-time working age. Further, most of the people not looking for work at the time, indicated it was because they were primarily taking language classes or taking care of children. A subsequent IRCC survey found that 95 per cent of GARs and 75 per cent of PSRs had enrolled in some form of language training. The majority of GARs surveyed (67.5 per cent) indicated they were happy or very happy with the city in which they were settled. PSRs had a higher level of satisfaction, with 74.5 per cent were happy or very happy with the city to which they were destined.

Canada's Operation Syrian Refugees – Lessons Learned

Conclusion

Bringing 25,000 Syrian refugees to Canada in a four-month period without compromising high quality security screening was made possible by the ongoing commitment and support of Canadians across the country, significant public and private resources and a nimble professional public service. It also required the diversion of significant resources in time and money by government to accomplish the objectives on time and on budget. Multiple organizations, including more than ten federal departments and agencies, the UNHCR, the International Organization for Migration, the governments of Lebanon, Jordan and Turkey, provincial, territorial, and municipal governments across Canada, non-governmental organizations, corporate and community private sponsors, worked together to accomplish a clear and common objective.

Since Operations Syrian Refugees, Canadian views towards immigration and refugees have remained positive. The Government of Canada has continued to welcome refugees from Syria and elsewhere, with a stronger focus now on working with provinces and territories, service provider organizations, and communities to ensure refugees are successfully integrated. The Government of Canada is also placing a renewed focus on ensuring the delivery of high-quality settlement services as well as ensuring a rigorous approach to data in order to accurately measure outcomes.

Tab 5D

s.15(1) - Int'l

s.21(1)(a)

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



FCM 2017 – Agenda Items

Innovation and Border Technology to Manage Identity

DECISION SOUGHT / ACTIONS TO BE TAKEN

What is the action sought from the Ministers at the FCM regarding this issue? (e.g. expected results, agreement on coordinated approach, approval of principals or document, discussion on lessons learned, etc.)

A)

B)

C)

DESCRIPTION

Short description (1-2 lines) of the topic/issue as it is understood in the FCM context

Innovation and Border Technology to Manage Identity

BACKGROUND

What has FCM done in the past regarding this issue? How this issue has evolved in the last years? What are the significant gaps remaining?

A shared Five Eyes (FVEY) priority is ensuring the free and secure flow of legitimate people and goods through our respective borders. The use of border technology plays an increasingly critical role in meeting this objective. In recent years, there have been important technical developments in FVEY fora.

FCM Ministers are mandated to ensure that our immigration and border management systems are efficient in preventing the entrance of *malafide* individuals. The ability to verify the identity of travellers in real-time at the border is critical. Developing innovative technology to manage identity is needed by all FVEY partners in order to improve front-line decision-making.

s.15(1) - Int'l

s.21(1)(a)

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



Canada has also undertaken various innovative border technology processes. In Spring 2017, the next generation Primary Inspection Kiosks (PIKs) were deployed in phases at major Canadian international airports. Upon arrival, travellers will use a PIK to 1) verify their travel documents, 2) confirm their identity and 3) complete an on-screen declaration. Canada is also investing in remote Traveller processing technology, whereby travellers will be able to be processed remotely at Ports of Entry after staffed hours of service. Our FVEY partners are also developing innovative border technologies. For example, New Zealand is in the process of updating its SmartGates, which enable automated border processing of inbound and outbound passengers.

RECENT DEVELOPMENTS

What additional information is needed for the ministers to understand this issue?

In recent years, FVEY countries have experienced increased traveller volumes, especially through the air mode. FVEY partners have also experienced unprecedented numbers of refugees and irregular migrants from the Middle East and Africa via land and sea routes since 2014. Canada has experienced a significant spike in border crossing by irregular migrants since 2017.

s.15(1) - Int'l

s.21(1)(a)

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



| |
|---|
| CHAMPION/S |
| <i>Which country or countries will lead the discussion on this issue at the Ministerial (please detail if sub-subjects involved)?</i> Canada |
| ANNEXES |
| <i>What annexes/background papers are attached to this document?(e.g. ANNEX 1: Detailed Action Plan)</i> |

Tab 5E

**Pages 538 to / à 540
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1) - Int'l

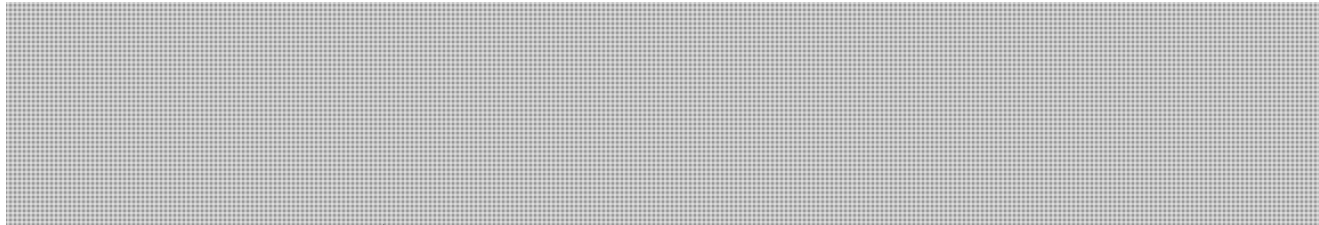
**of the Access to Information
de la Loi sur l'accès à l'information**

Tab 5F

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Session III: Migration and Refugees
Attachment: Status of Trusted Traveler Cooperation

Background



By working to expand membership in each country's respective programs and developing more bilateral and trilateral trusted traveler programs, five country partners can provide their citizens with increased facilitation benefits while strengthening and maintaining vetting standards and enhancing security. Trusted traveler programs allow customs and immigration officials to gather information on potential or frequent travelers in advance for use in screening, and can predetermine whether travelers are lower risk to both facilitate travel and focus screening resources on unknown and high risk travelers.

Current Status



UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

NEXUS members receive expedited screening at airports in both countries, have access to NEXUS lanes at 20 major land border crossings in Canada and 24 locations at U.S. ports of entry and have access to the TSA Pre ✓® lanes at 171 airports in the United States.

- Since 2012, five country partners have developed new tools for vetting and screening travelers and through Five Country Conference and Border Five traveler facilitation efforts have made great strides towards making the traveler experience more streamlined and convenient and improving cooperation on screening.

Next Steps

- Fully implement the U.S.-UK-Canada Trusted Traveler program – **Mid-2017**
- Integrate Australia and New Zealand into this arrangement – **TBD**

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Tab 6



Public Safety
Canada

Sécurité publique
Canada

FCM/QUINTET LUNCH

Session Lead

Minister Ralph Goodale, Canada

Participating Ministers

| | |
|-----------------------|----------------|
| George Brandis | Australia |
| Peter Dutton | Australia |
| Ahmed Hussen | Canada |
| Jody Wilson-Raybould | Canada |
| Amber Rudd | United Kingdom |
| Christopher Finlayson | New Zealand |
| Michael Woodhouse | New Zealand |
| Jeff Sessions | United States |
| John Kelly | United States |

Tab 6A

FOR OFFICIAL USE ONLY



FCM 2017 – Lunch Scenario Note

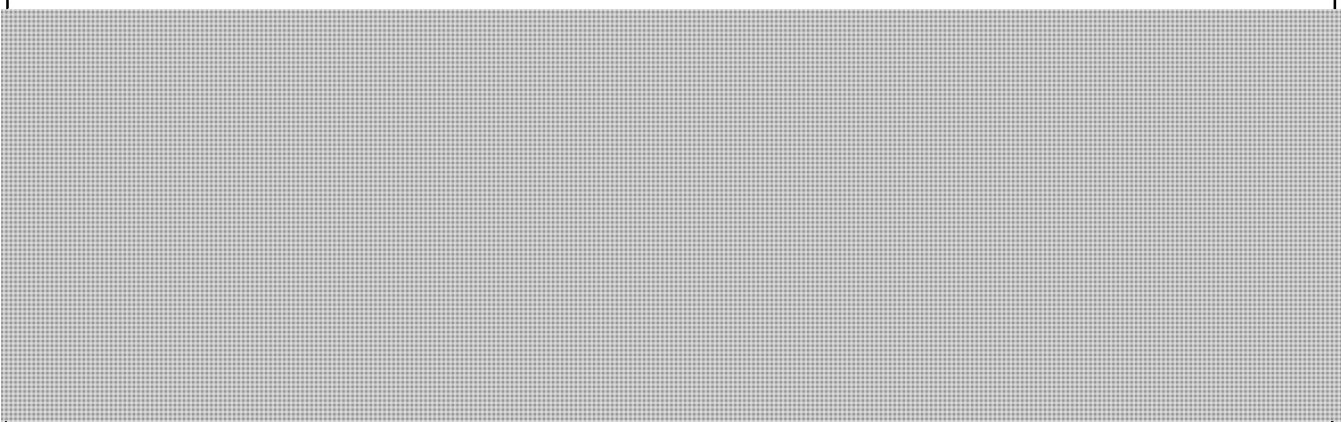
Transparency/Accountability in National Security

Sequencing

CAN/Minister Goodale will introduce the topic and update Ministers on Canada's latest plans for transparency in the context of national security (approx. 10 minutes (TAB 6B)).

Given that this discussion will take place over lunch, a more informal conversation is anticipated to follow.

Expected Position of the FVEY



Background

The Government of Canada has made a commitment to national security transparency. This commitment will see the Government provide Canadians with more information on national security efforts, so they are able to understand what the Government does to protect national security, how it does so in a way that aligns with Canadian values, and why this work is important. Canadians will also be consulted on future substantive change to the national security framework.

The National Security Transparency Commitment consists of six principles. They are:

1. Departments and agencies will **release information** that explains the main elements of their national security activities and the scale of those efforts.
2. Departments and agencies will **enable and support Canadians in accessing national security-related information** to the maximum extent possible without compromising the national interest, the effectiveness of operations, or the safety or security of an individual.
3. Departments and agencies will **explain how their national security activities are authorized in law and how they interpret and implement their authorities in**

FOR OFFICIAL USE ONLY



Public Safety
Canada

Sécurité publique
Canada

line with Canadian values, including those expressed by the Charter.

4. Departments and agencies will **explain what guides their national security-related decision making** in line with Canadian values, including those expressed by the Charter.
5. The Government will **inform Canadians of the strategic issues impacting national security** and its current efforts and future plans for addressing those issues.
6. To the extent possible, the Government will **consult stakeholders and Canadians during the development of substantive policy proposals** and build transparency into the design of national security programs and activities.

The Government will begin implementing these principles immediately. For example, we are in the process of centralizing information on national security activities into one website. Over the course of the next year, officials will work with an advisory group of stakeholders and experts to develop an action plan to establish priorities and guide further implementation. In addition, when the Government introduces new security programs, these principles will be reflected in the program's design.

Tab 6B

Lunch Address Summary

- Cover larger range of mandate (principles stretching beyond NS, mandate given by PM)
- Bill C-22
 - Other Five Eyes' systems as inspiration/models for NSICoP
 - Role and features of NSICoP
- Coming Special Advisor (The Office)
- Introduction of Bill C-59
 - Role of consultations and what we heard
 - Commitments on Transparency (the what, why, and how of national security work)
- Government's choice: openness or defensiveness
- Benefits of transparency
- CVE Action Plan (Five Eyes WG, coordination, enhanced transparency efforts)
- Alignment with similar efforts in other 5 countries

Remarks

for

The Honourable Ralph Goodale

**Minister of Public Safety and Emergency
Preparedness**

**Five Country Ministerial – Luncheon Address on
Transparency**

CSIS HQ

June 26, 2017

Check Against Delivery

Word Count: 1120 (10 minutes)

Good afternoon, everyone. We have had a productive morning so far, and I am very much looking forward to this lunchtime discussion.

While national security concerns are certainly at the top of my agenda, the responsibilities of the department I lead stretch beyond national security.

Guided by the mandate instructions given to me by Prime Minister Trudeau, I also have the opportunity to advance measures of longstanding personal importance, such as better supporting our first responders.

With regard to national security, it is an immense honour and challenge to steer the ship towards ensuring our efforts are not only effective, but **respective** of the rights and freedoms that our citizens cherish.

This is a goal for which all western democracies must continually strive, no matter the threats we face.

That brings me to another of the mandate items entrusted to me by the Prime Minister — the creation of a committee of Parliamentarians to review the work of government departments and agencies involved in national security and intelligence work.

Among this forum, and indeed when compared to other western countries, Canada is the outlier in this regard. So, we took a close look at the review systems in other countries, particularly those of the Five Eyes, in developing our own.

That led to Bill C-22, an Act to establish a National Security and Intelligence Committee of Parliamentarians, which recently received royal assent.

While C-22 is tailored to the Canadian reality, its existence is informed and inspired by the systems in place in your countries, and is all the better because of that.

It will go a long way to reassure the public that the national security and intelligence activities being carried out in its name are effective and uphold their rights and freedoms.

The NSICoP will have extraordinary access to classified information to provide a whole new dimension of scrutiny over every federal department and agency involved with security and intelligence work.

Since this assignment is new to Canada, most domestic and international experts have advised us to proceed on NSICoP in a careful and measured way. They've told us to give the new committee the time and opportunity to learn the deadly serious task it is undertaking, to earn the confidence and respect of the intelligence and security agencies it will be scrutinizing, to develop sensible ways of interacting with the other expert review bodies that already exist, to get to know and understand the international security and intelligence context, and to build trust among Canadians.

We have heeded that advice. Indeed, for these reasons, we have built-in an automatic review of NSICoP after five years to ensure that all the lessons learned in the meantime can be acted upon in a timely manner.

I am very proud that our Government has been able to deliver on this initiative, bringing us in line with the enhanced accountability that exists in your countries.

[I am also close to announcing / I have recently announced] the appointment of a Special Advisor to head [name of new Office / a new office responsible for community outreach and countering radicalization to violence], which was another task given to me by the Prime Minister.

The Office will provide national leadership on Canada's response to radicalization to violence, coordinate talent and expertise, provide support to municipal, community and grassroots efforts, and enhance the evidence base on this issue.

While early in the legislative process, I also want to take a moment to outline another key national security achievement for Canada.

Bill C-59, an Act respecting national security matters, was introduced just last week in Parliament and fulfills another key commitment we made to Canadians.

The new legislation will modernize and enhance our security and intelligence laws - to ensure our agencies have the tools necessary to protect Canada and Canadians within a legal and constitutional framework that safeguards our rights and the open, inclusive, generous, democratic nature that makes our country what it is.

To get us to that point, we undertook unprecedented public consultations in which tens of thousands of views were received and greatly informed the legislation we have put to Parliament.

Not surprisingly, we heard Canadians unequivocally want effectiveness, accountability, and transparency from their security and intelligence agencies.

That is why, accompanying this important legislation, we have made a National Security Transparency Commitment.

This will hold the Government to consulting its citizens on national security policies, promoting understanding of national security efforts, and reflecting our rights and values in the work we do.

This is of paramount importance, now more than ever.

The ability to undertake national security activities is dependent on our citizens' trust and confidence, which we cannot earn unless citizens understand the **what, how, and why** of national security work.

Who better to impart and contextualize that knowledge than the very departments and agencies doing that work?

Citizens will come to their own conclusions on the national security activities of our governments. Those conclusions can be informed directly by Government or informed by others, such as the media or review bodies. When solely the latter, officials are in a reactive position, forced to correct inaccuracies, clarify misconceptions, and contextualize partial information.

It's not an easy shift – national security and intelligence organizations can be, by their very nature, hesitant to openness.

But, colleagues, as the elected officials responsible for these organizations, we can provide encouragement, impetus and motivation to make this shift because we know our constituents are hungry for it.

Just as we need to get out ahead of the threats we face, we need to get out ahead of our citizens desire for understanding not only the response, but also how their rights are being respected in the process.

It is infinitely preferable for security and intelligence agencies to make a concerted effort to be more open, obviously with due regard to the all the tradecraft, sensitivities and secrets at play.

Colleagues, Canada believes that we can, and should, to the degree possible, engage and inform our citizens on issues as fundamental as national security.

And so, we have proposed five principles that we can commit to together, reflecting a mutual commitment on an issue of mutual importance to our countries and the Five Eyes as a partnership.

To support their implementation, a working group of officials from all Five Eyes countries could share best practices, coordinate implementation of transparency measures, and identify opportunities' to enhance transparency of the Five Eyes partnership.

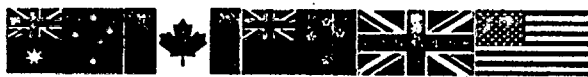
I note that this proposal aligns with several principles and programs set forward in several of your own countries, so perhaps I could turn to all of you to offer additional perspectives as we delve into this discussion.

Thank you. Bon appetit.

Tab 6C

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



FCM 2017 – Agenda Items

National Security Transparency

DECISION SOUGHT / ACTIONS TO BE TAKEN

It is proposed that Ministers, recognizing that information is necessary to citizens' confidence in national security institutions, agree to the following transparency principles and discuss potential next steps to implement the principles within their respective agencies.

1. Citizens should have access to information that enables them to understand the main elements of national security activities and the scale of those activities.
2. Countries have a particular responsibility for appropriately managing personal information. Countries should make clear the controls on the collection, use, maintenance, and dissemination of personal information. Citizens should have access to the information about them, to the greatest extent possible, consistent with the need to protect classified or sensitive information (under exemption provisions established by law).
3. Countries should work to make the legal framework that authorizes national security activities clear, by explaining and enhancing understanding of its use and interpretation.
4. Countries should engage in proactive efforts to engage citizens and explain trends in the national security threat environment and discuss the implications and potential policy responses.
5. Countries should continue to take steps to protect information where disclosure could compromise operational security or the safety and security of employees.

To support implementation of these principles, a working group of officials from all Five Eyes countries will share best practices, coordinate implementation, and identify opportunities to enhance transparency of the Five Eyes partnership.

DESCRIPTION

Five Eyes countries have a mutual interest in protecting our national security. We also have a common democratic responsibility to assure our citizens that we are doing so in a way that respects rights and freedoms and the law. Indeed, Five Eyes' countries ability to undertake national security activities, and cooperate internationally, is dependent on the democratic support of their respective citizenries. Transparency is key to establishing this legitimacy by providing citizens with the information necessary to develop confidence in their government's national security policies.

BACKGROUND

As democracies, all government actions are dependent on citizen's trust and confidence (democratic legitimacy). In order for such confidence to be developed in security institutions, citizens must understand:

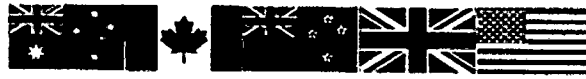
- **what** their national security institutions do and do not do,
- **how** their national security institutions undertake this work, and how it is done in a manner consistent with their values; and,
- **why** this work is necessary.

s.15(1) - Int'l

s.21(1)(a)

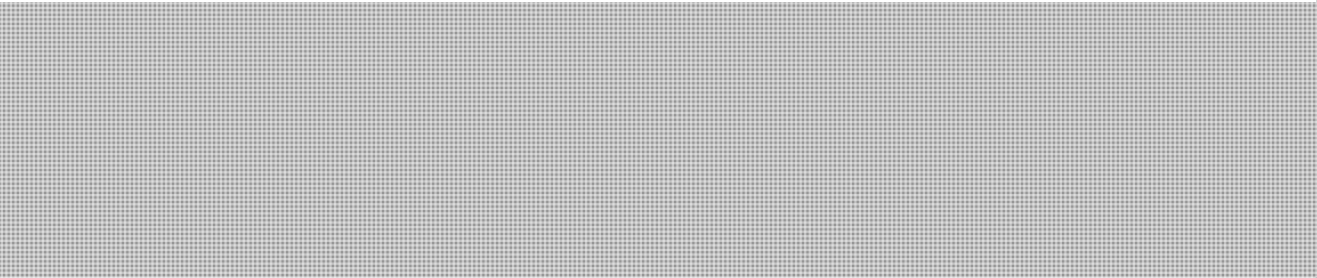
FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



In one way or another, citizens will form an understanding of the what, how and why of national security and intelligence. If security and intelligence institutions do not provide citizens with adequate information, their understanding of security and intelligence activities will be formed through 'leaks,' as seen with the Snowden documents, or through the media, as often seen with technological issues, such as mobile device identifier technology (IMSII catchers). This puts security and intelligence institutions in the position of playing catch up, and damages the credibility of institutions.

Transparency looks to proactively provide citizens with information that helps them understand the what, how, and why of national security work. It does not involve the indiscriminate release of information. Rather, it entails the purposeful proactive release of information that is sufficient to form confidence in institutions without compromising operational security. It also means managing non-release information in a way that can enable future release, as appropriate. At all times, the security and integrity of operations is paramount.



RECENT DEVELOPMENTS

All Five Eyes countries are members of the Open Government Partnership. They have, therefore, endorsed the Open Government Declaration and are committed to:

- increasing the availability of information about governmental activities;
- supporting civic participation;
- implementing the highest standards of professional integrity throughout their administrations; and,
- increasing access to new technologies for openness and accountability.

Governments are continually moving towards implementation of these actions. The principles proposed by Canada (above) are meant to apply open government principles within the national security and intelligence context.

CHAMPION/S

Canada will outline its planned activities for national security transparency and lead a discussion on the importance of national security transparency and potential next steps by the Five Eyes.

ANNEXES

None.

Tab 7



Session 4

Security Cooperation & Law Enforcement

Session Lead
Secretary John Kelly, United States

Participating Ministers

| | |
|-----------------------|----------------|
| George Brandis | Australia |
| Peter Dutton | Australia |
| Ahmed Hussen | Canada |
| Jody Wilson-Raybould | Canada |
| Amber Rudd | United Kingdom |
| Christopher Finlayson | New Zealand |
| Michael Woodhouse | New Zealand |
| Jeff Sessions | United States |
| John Kelly | United States |

Tab 7A

FOR OFFICIAL USE ONLY



Public Safety
Canada

Sécurité publique
Canada

FCM 2017 – Session IV Scenario Note

Security Cooperation and Law Enforcement

Sequencing

CAN/Minister Goodale will invite his co-host Minister Wilson-Raybould to say a few words about the joint section of the FCM meetings.

U.S./Secretary Kelly will lead this session and open with a discussion about Terrorist Watchlist Sharing, and then open the floor for discussion.

U.K./ Home Secretary Rudd will then lead a discussion on Criminal Information Sharing and Human Trafficking, and open the floor for discussion.

The Canadian response on each item will be led by CAN/Minister Goodale.

CAN/Minister Hussen may intervene on the SRTP role in information sharing.

CAN/Minister Wilson-Raybould may also have comments on Human Trafficking.

At the end of the session, the Canadian delegation will help guide Ministers to the location of the family photo.

Talking Points

- **Welcome back. This afternoon, we will begin the joint portion of our day with the Quintet members, thus continuing the practice first instigated last year in Washington, D.C.**
- **I would like to invite my colleague and co-host of the FCM/Quintet 2017, the Attorney General Jody Wilson-Raybould to say a few words.**
[Minister Wilson-Raybould to provide opening remarks]
- **Thank you Jody. I will turn to my colleague Secretary John Kelly to introduce the session on Law enforcement and security cooperation.**

Terrorist Watchlist Information Sharing

- **Current threats and global trends require border and immigration**

FOR OFFICIAL USE ONLY



Public Safety
Canada

Sécurité publique
Canada

officials to have the necessary information and tools to ensure they can identify and properly screen individuals along the entire travel continuum.

- **The sharing and use of terrorist watchlist and criminal history information is a critical aspect of the Canada Border Services Agency's (CBSA) border management efforts and the Government of Canada's counter-terrorism and counter-crime initiatives.**
- **Improving FVEY access to and use of information concerning criminal history and known and suspected terrorists will enable the CBSA to improve screening and frontline decision-making on cases regarding admissibility and immigration.**
- **The *Secure Air Travel Act* allows for information sharing arrangements with other countries.**
- **In 2016, we concluded an arrangement with the U.S. that allows for the exchange of "no-fly" lists.**
- **Agencies in Canada share information with domestic and foreign partners in accordance with clearly established policies regarding the relevance, reliability and accuracy of information.**
- **Of course information must be shared in accordance with the relevant laws regarding personal information, privacy and human rights.**

Criminal Information Sharing

- **Canada is supportive of exploring options to improve information sharing between Five Eyes countries on known criminals, in order to prevent criminals, such as sex offenders and human traffickers, from entering our countries.**
- **However, any agreement on the sharing of criminal conviction records with Five Eyes countries, especially as it pertains to sex offenders who travel, must respect and be in accordance with existing legislation, including the *Sexual Offender Information Registration Act (SOIRA)* and Canadian privacy legislation.**

FOR OFFICIAL USE ONLY



Public Safety
Canada

Sécurité publique
Canada

- **Overall, Canada's legal framework guides law enforcement information sharing practices. To ensure that disclosures are lawful, information sharing must take place on a case-by-case basis.**
- **In addition, there are a number of legislative and definitional issues that would need to be examined amongst the five countries to determine the feasibility of the proposed enhancements to information sharing.**
- **The Five Eyes Law Enforcement Group operates independently from the Five Country Ministerial and other similar Five Eyes groups. Given its current governance structure, it may not be the most effective form to coordinate and advance the proposed actions.**

Modern Slavery/Human Trafficking

- **Canada is committed to combatting human trafficking and better protecting its victims, who are among society's most vulnerable. Collaboration and improved information sharing on human trafficking are critical to our collective efforts to counter human trafficking.**
- **Canada has adopted a collaborative and multi-pronged – "4P" - approach in its fight against human trafficking. Various federal government departments and agencies work together to focus their efforts on prevention, protection, prosecution, and partnership building. We work closely with provinces and territories, Indigenous communities, law enforcement, community organizations and international partners to combat human trafficking.**
- **We support further discussion on our countries' challenges and best practices in investigating trafficking routes, sharing investigative information, and on exploring options for joint operations.**

s.15(1) - Int'l

FOR OFFICIAL USE ONLY

s.21(1)(a)



Public Safety
Canada

Sécurité publique
Canada

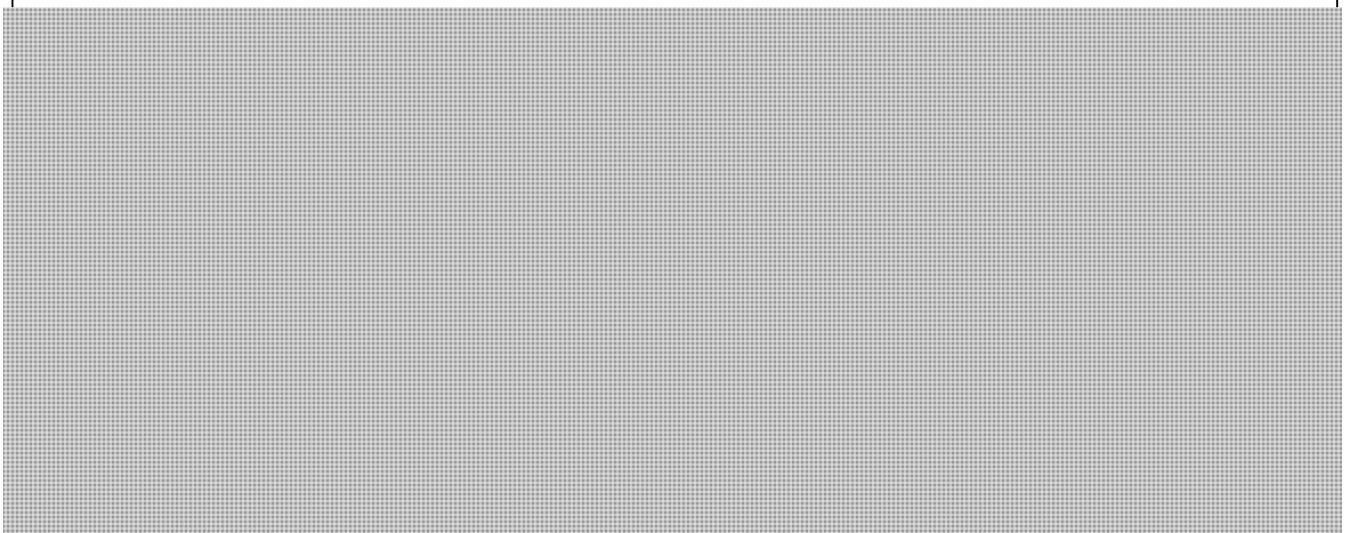
- **Enhanced FVEY collaboration and information sharing in the area of human trafficking will position frontline border officials to better identify and disrupt human traffickers at POEs. This is increasingly important given the growing number of individuals seeking asylum or refugee status in Canada.**

SRTP role in Information Sharing (IRCC/Minister Hussen may comment on this point)



- **The benefits of SRTP accrue on a daily basis, both through enhanced screening decisions and facilitated travel for low risk clients. These benefits will continue to grow as Canada increases information sharing volumes commensurate with increased collection capacity.**
- **To recommend against expanding the use of the SRTP to include criminal information until we have addressed the legislative, policy, and technological changes required to do so.**

Expected Position of the FVEY



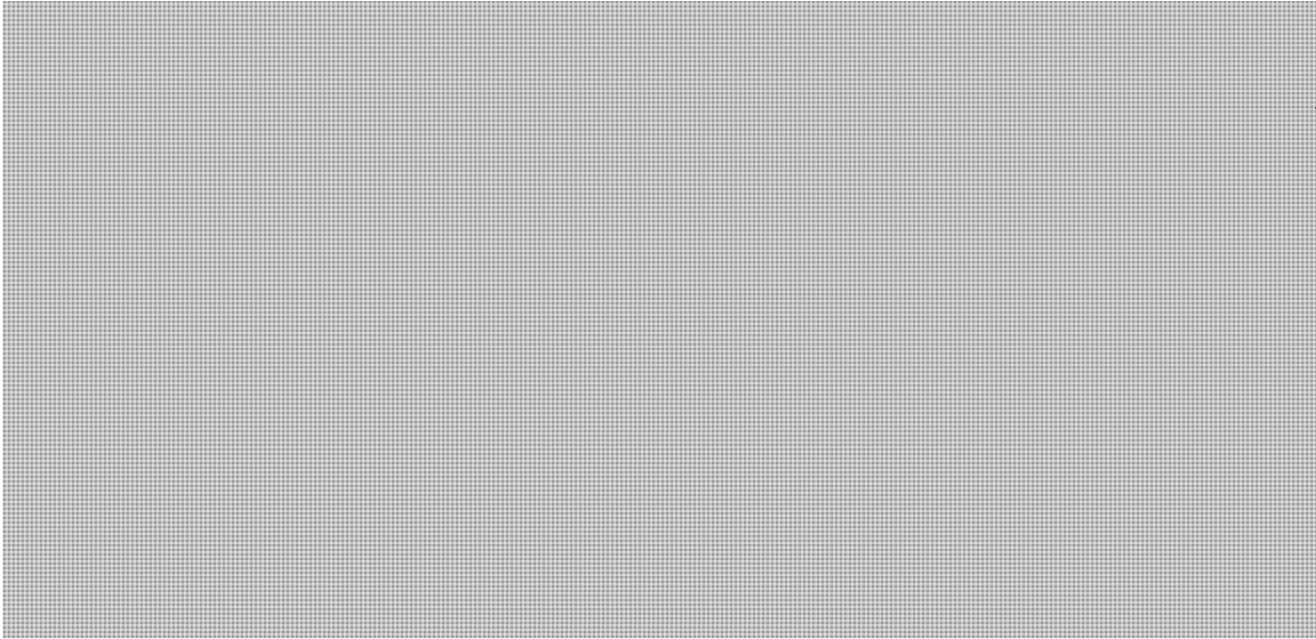
FOR OFFICIAL USE ONLY



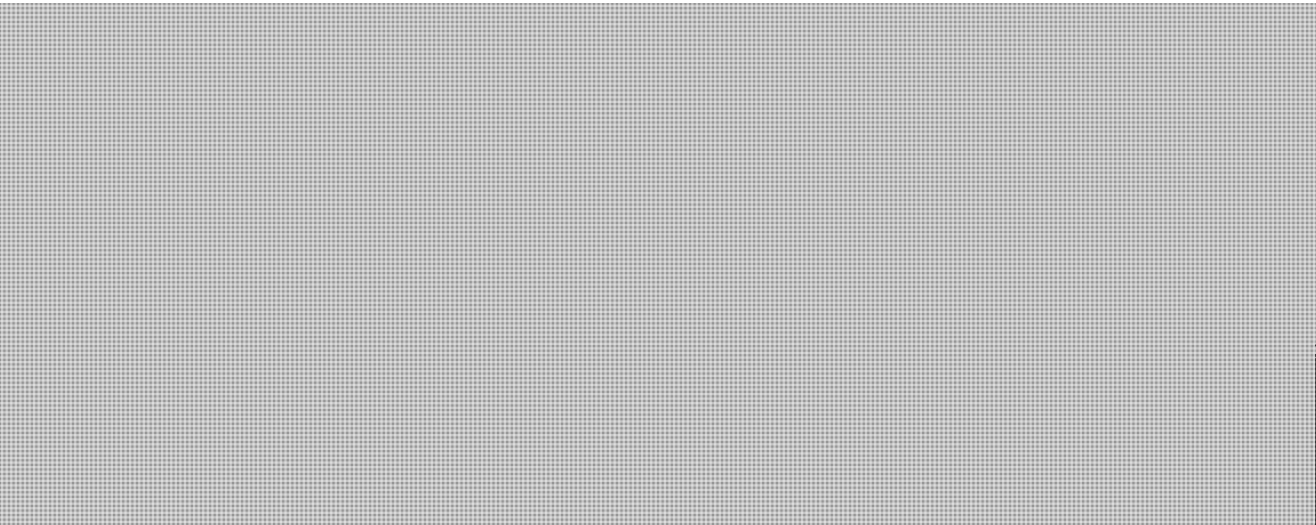
Public Safety
Canada

Sécurité publique
Canada

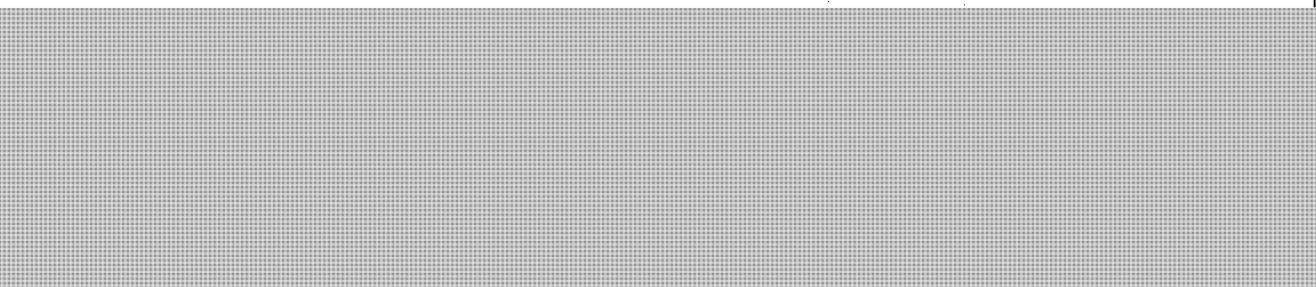
Criminal Information Sharing



Modern Slavery/Human Trafficking



SRTP role in Information Sharing





Public Safety
Canada

Sécurité publique
Canada

BACKGROUND

Terrorist Watchlist Information Sharing

The *Secure Air Travel Act*, which came into force in August 2015, provides the legal authority for the Minister of Public Safety and Emergency Preparedness to enter into a written arrangement with a foreign governments to share the list created as part of the Passenger Protect Program. This list includes the name, known alias, date of birth and gender of persons whom the Minister has reasonable grounds to suspect may pose a threat to aviation security, or may be travelling by air for the purpose of committing certain terrorism offences.

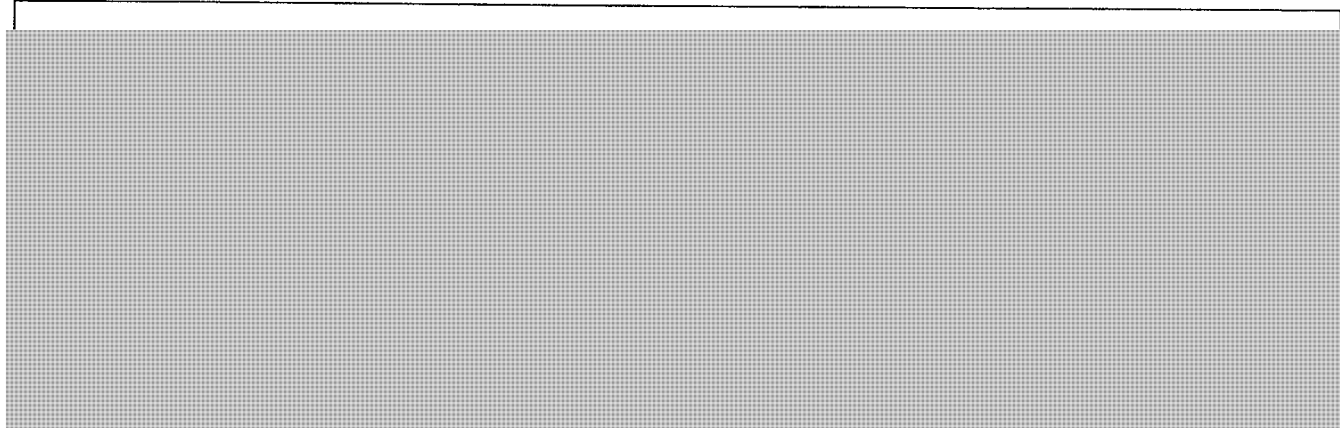
Criminal Information Sharing

FOR OFFICIAL USE ONLY



Public Safety
Canada

Sécurité publique
Canada



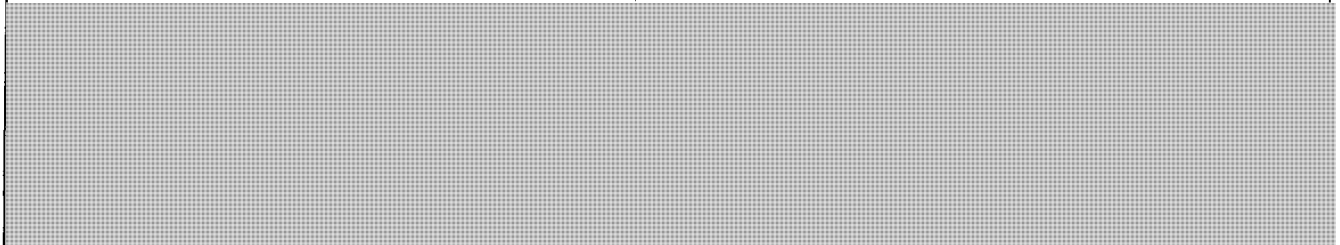
Modern Slavery/Human Trafficking



The National Action Plan to Combat Human Trafficking has provided the framework for the Government of Canada's response to combat human trafficking. While the National Action Plan ended on March 31, 2016, federal departments and agencies continue anti-trafficking work as the formal evaluation is being completed and the way forward is determined

The Human Trafficking Taskforce, comprised of officials from 18 federal departments, is the primary federal coordinating vehicle for anti-human trafficking efforts. Its members meet regularly, as well as with provincial and territorial counterparts to facilitate the ongoing development of policies and tools.

S RTP role in Information Sharing



Tab 7B

s.15(1) - Int'l

s.21(1)(a)

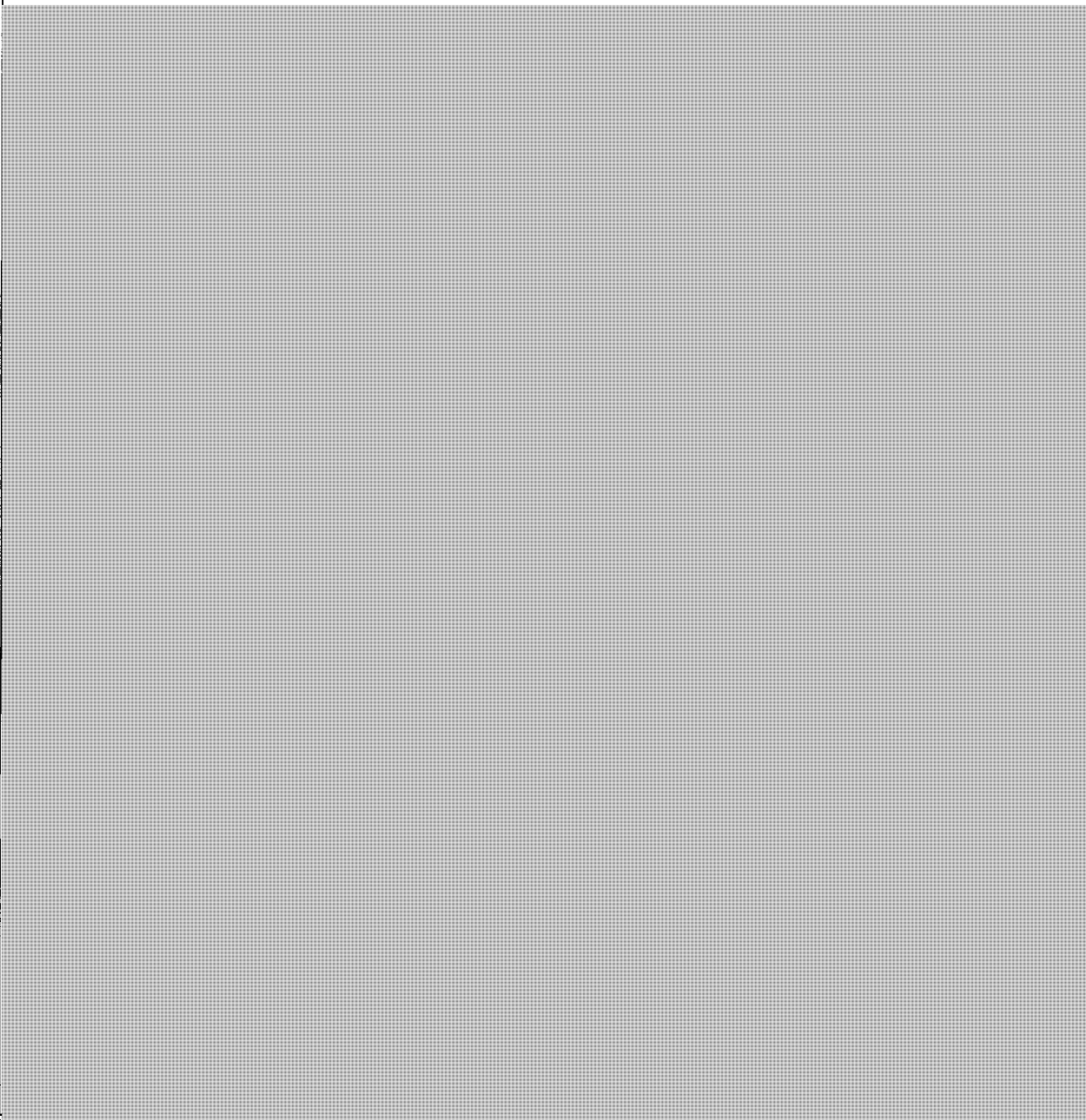
FOR OFFICIAL USE ONLY

FIVE COUNTRY
MINISTERIAL



Session IV: Security Cooperation and Law Enforcement

DECISION SOUGHT / ACTIONS TO BE TAKEN

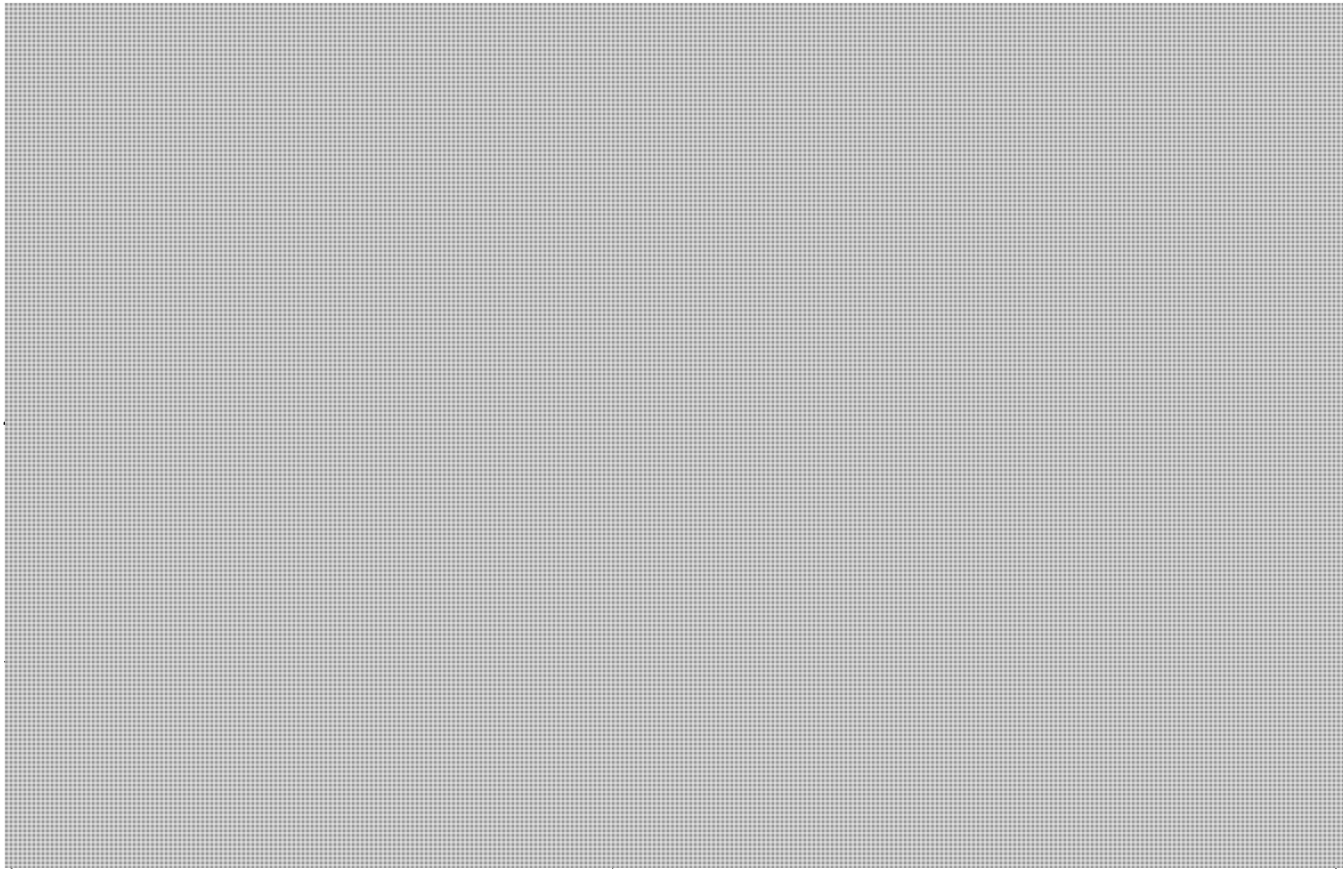


FOR OFFICIAL USE ONLY

s.15(1) - Int'l

s.21(1)(a)

FOR OFFICIAL USE ONLY

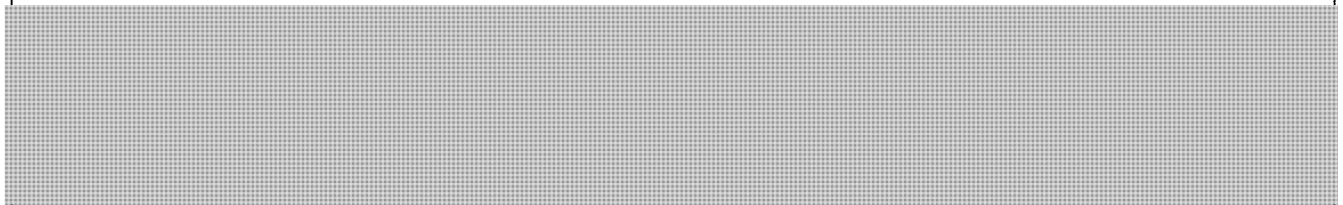


DESCRIPTION

The Five Eyes security, immigration, and justice agencies collectively are responsible for ensuring the security and law enforcement of our citizens, including by ensuring known criminals and terrorists are identified. Improving access to and use of criminal and terrorist identities known to any of the Five Eyes will help our countries to deny entry to individuals who may pose a risk to the public and are inadmissible under national law, either in advance of travel or at the border.

Agreements to share criminal histories facilitate the sharing of conviction records (criminal histories) for wider public protection purposes in-country. These agreements allow for countries to notify each other where a national of the other's country is convicted of any offence, **proactively and at the point of conviction** so that law enforcement agencies in the person's 'home' country can build a picture of their national's domestic and overseas criminal history. As own nationals cannot be denied entry at the border law enforcement can use notifications of criminal convictions to take public protection steps.

For individuals who cannot be denied entry, law enforcement and immigration authorities will be able to consider public protection measures that might be appropriate on the basis of an individual's previous convictions. In addition, our respective judiciaries may be able to consider an offender's previous criminal records overseas when sentencing.



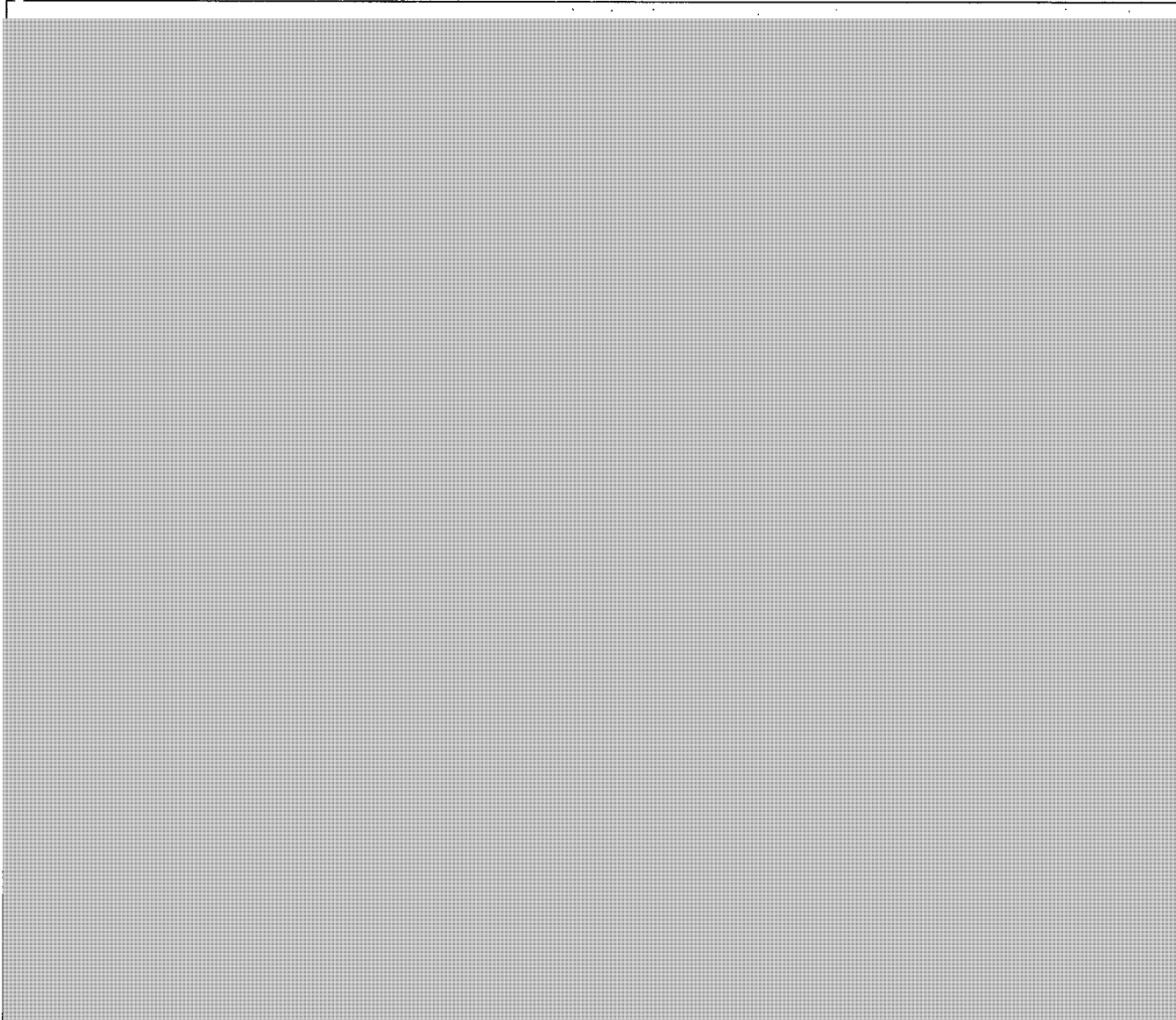
BACKGROUND

FOR OFFICIAL USE ONLY

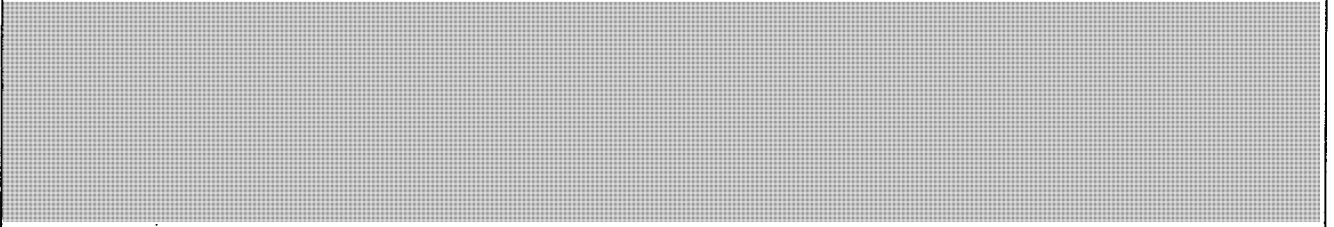
s.15(1) - Int'l

s.21(1)(a)

FOR OFFICIAL USE ONLY



Law enforcement also plays a vital role in managing the risks posed by returning offenders, protecting the public from potential future harm. This includes ensuring sex offenders cannot get jobs working with children and violent offenders cannot obtain firearms licenses.



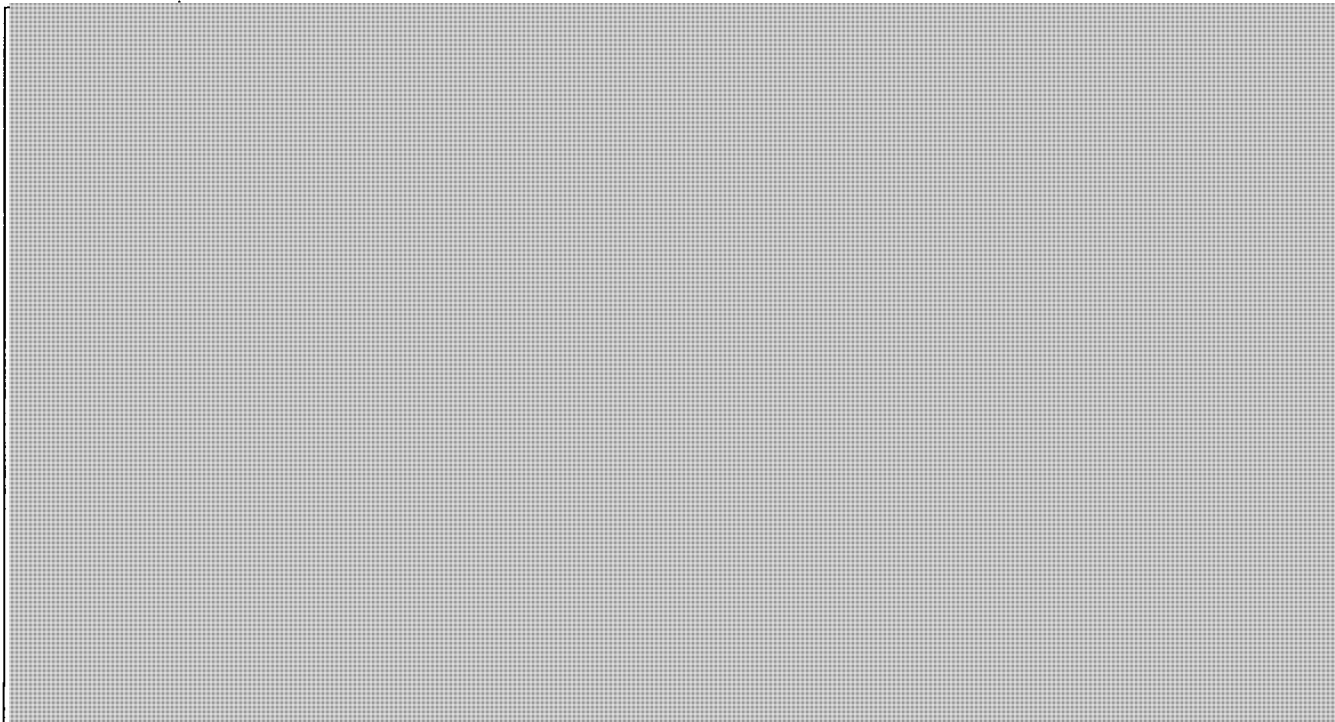
RECENT DEVELOPMENTS



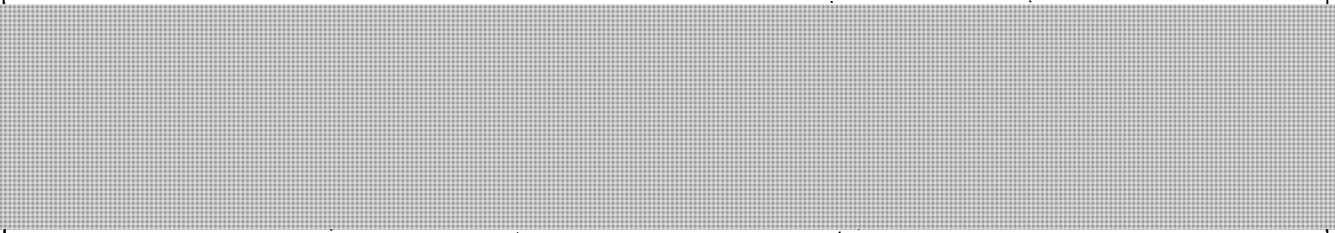
s.15(1) - Int'l

s.21(1)(a)

FOR OFFICIAL USE ONLY



SUGGESTED COMMUNIQUE LINE



CHAMPION/S

U.S. and UK.

ANNEXES

- Attachment A: Status Update on Secure Communications

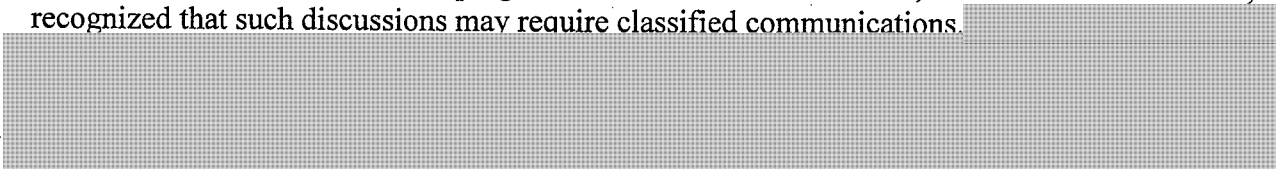
Tab 7C

UNCLASSIFIED//FOR OFFICIAL USE ONLY

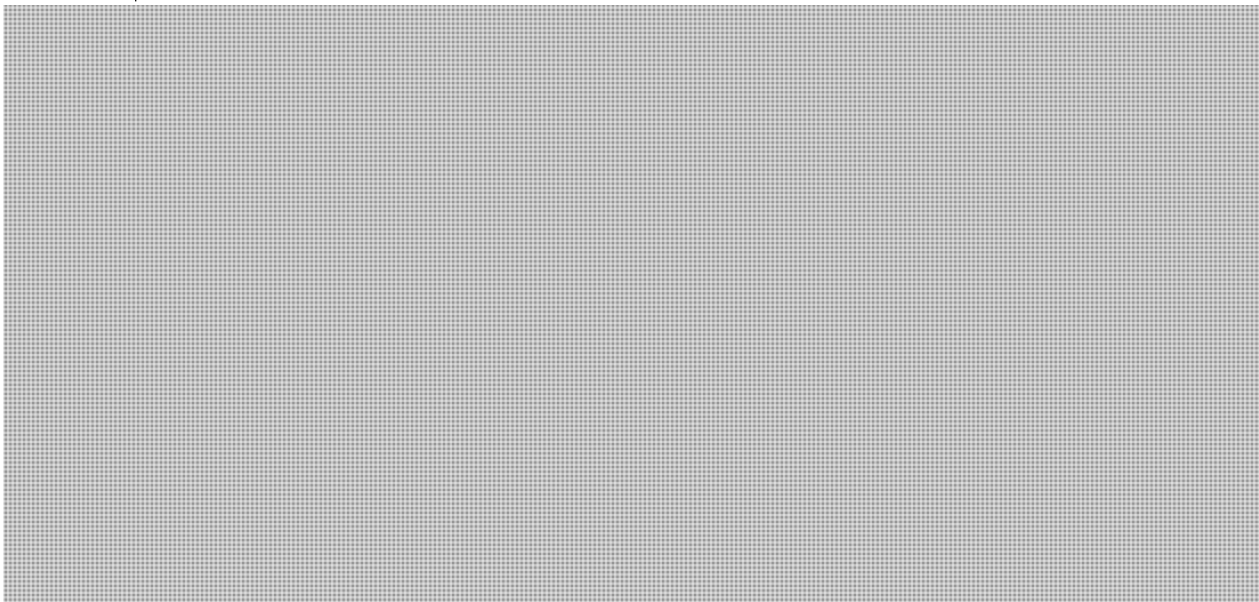
**Session IV: Security Cooperation and Law Enforcement
Attachment A: Secure Communications Connectivity**

Background

DHS and the UK's Home Office established Secure Video Teleconference (SVTC) capability in August 2016 and concluded a series of successful operational calls between the DHS Counterterrorism Coordinator and the Head of the Office of Security and Counterterrorism (OSCT). This capability allows our agencies to have real-time bilateral dialogues regarding current threat streams. The Five Country Ministerial (FCM) Executive Steering Group (ESG), which meets regularly to discuss progress on Ministerial deliverables, as well as current threats, recognized that such discussions may require classified communications.



Current Status



Next Steps



UNCLASSIFIED//FOR OFFICIAL USE ONLY

Tab 8



Session 5

Encryption & Cyber Security

Session Lead

Attorney General George Brandis, Australia

Participating Ministers

| | |
|-----------------------|----------------|
| George Brandis | Australia |
| Peter Dutton | Australia |
| Ahmed Hussen | Canada |
| Jody Wilson-Raybould | Canada |
| Amber Rudd | United Kingdom |
| Christopher Finlayson | New Zealand |
| Michael Woodhouse | New Zealand |
| Jeff Sessions | United States |
| John Kelly | United States |

Tab 8A

FOR OFFICIAL USE ONLY



Public Safety
Canada

Sécurité publique
Canada

FCM 2017 – Session V Scenario Note

Encryption & Cyber Security

Sequencing

AUS/ Attorney General Brandis will introduce the session and the Encryption topic and proposal, and then open the floor for discussion.

CAN/Minister Wilson-Raybould will answer first for Canada, and then she will turn to CAN/Minister Goodale.

Time permitting, CAN/Minister Goodale will then introduce the topic and proposal regarding Cyber Security and open the floor for discussion.

Talking Points

FOR OFFICIAL USE ONLY

Public Safety
CanadaSécurité publique
Canada

Cyber Security and Response to Critical Cyber Incident

- **Cyber security is a critically important issue. Our national security and public safety depend on our ability to prevent, respond to, and recover from cyber-attacks. Equally important, our economic prosperity depends on our ability to develop the knowledge and skills necessary to take advantage of the new digital economy.**
- **In Canada, we are committed to increasing not only our own domestic cyber security and technical skills, but also those of our allies, and we believe that collaboration amongst our Five Eyes allies is crucial to the development of the capabilities and skills necessary to keep us safe and prosperous.**
- **The work of our nations across all of the domains in which we cooperate on cyber security, from cyber incident response and cyber policy coordination to law enforcement and intelligence, laid the foundation for effective coordinated responses to incidents like the ones we saw in April 2017 and May 2017 (WannaCry).**
- **We have accomplished a lot. Nevertheless, there is significantly more collaborative work that can, and should, be done to ensure that we are able to develop the coordinated policy decisions and incident responses necessary to address the threats we face and to take advantage of the opportunities presented by the growing digital economy.**
- **FCM Ministers should encourage increased coordination at the Ottawa 5 (strategic policy coordination) and Usual 5 (operational incident response) tables, and support their commitment to digital innovation.**
- **I'm looking forward to hearing your views on this topic.**

Expected Positions of the Five Eyes

FOR OFFICIAL USE ONLY

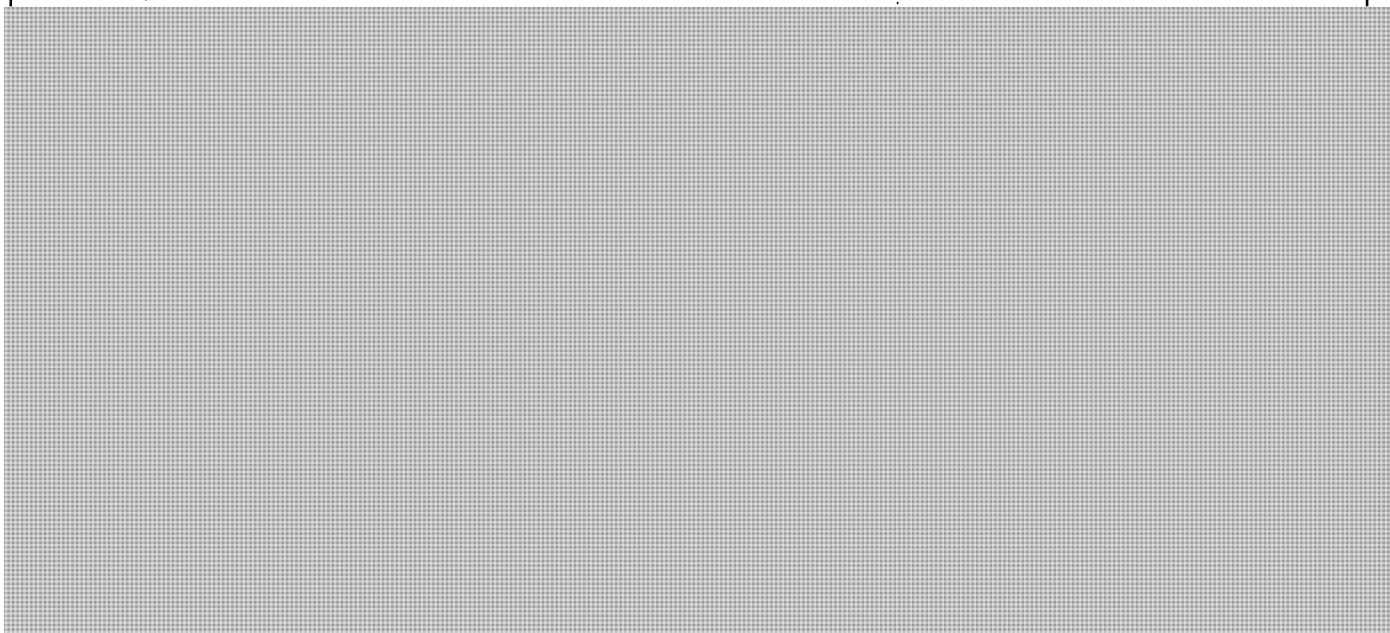


Public Safety
Canada

Sécurité publique
Canada



BACKGROUND

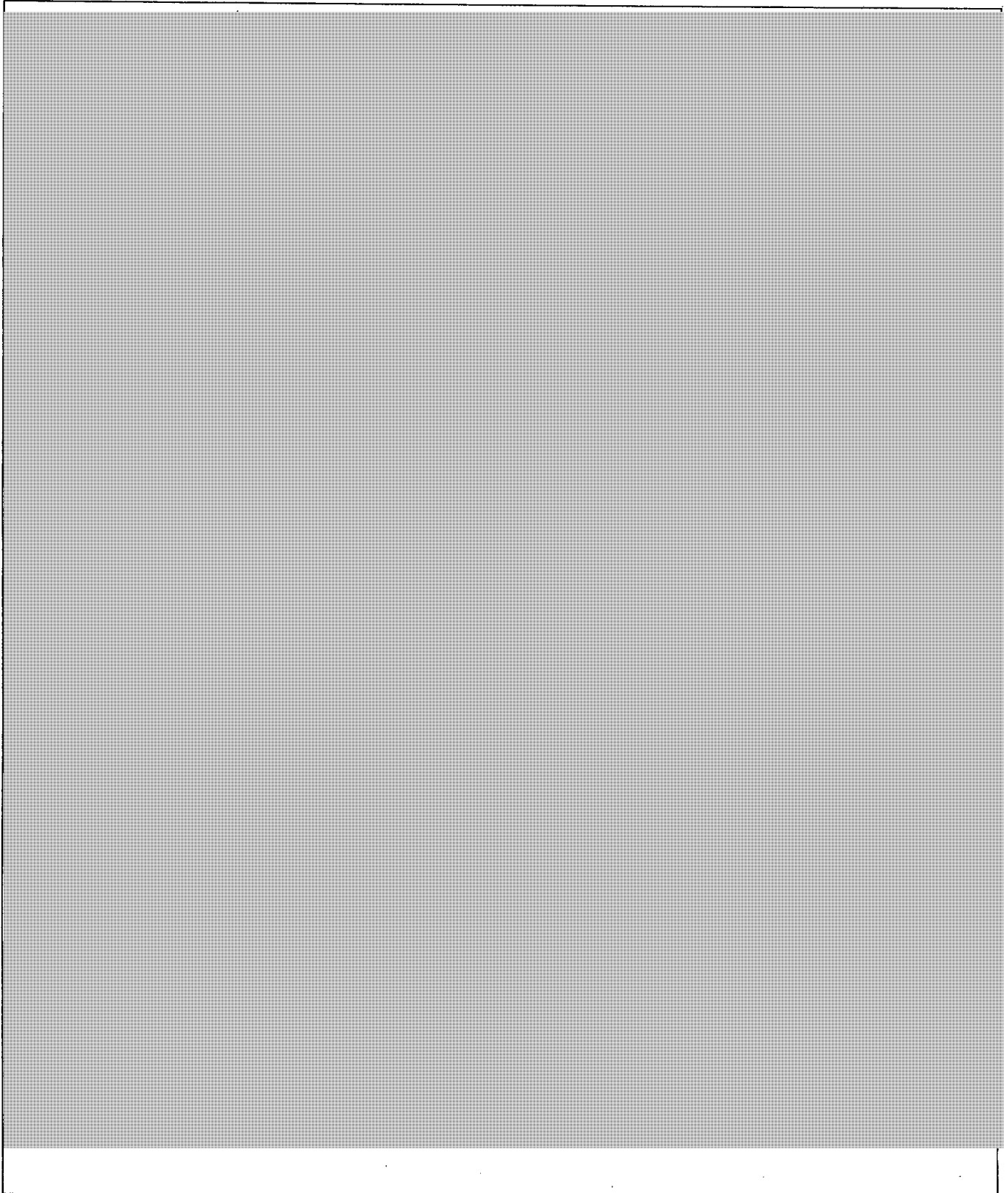


FOR OFFICIAL USE ONLY



Public Safety
Canada

Sécurité publique
Canada





Public Safety
Canada

Sécurité publique
Canada

Cyber Security and Response to Critical Cyber Incident

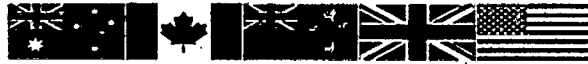
WannaCry:

- In relation to WannaCry, the role of the Government of Canada in this event was largely messaging and coordination as the main vendor released a number of patches to address the vulnerabilities leveraged by the malware.
- Government of Canada systems were not impacted by this event and overall ransomware had very little impact in Canada compared to other nations.
- The Canadian Cyber Incident Response Centre (CCIRC) was fully engaged with our domestic and international partners to understand the scope and scale of this activity; and to provide any assistance that may be requested.
- CCIRC has notified potentially impacted Canadian organizations. These notifications provide recipients with the information needed to identify and locate the potentially infected hosts within their infrastructure. CCIRC additionally contacted a number of Critical Infrastructure Sector organizations to ensure that they were aware of our products, as well as the gravity of the situation.

Tab 8B

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



FCM/Quintet Joint Meeting 2017 – Agenda Items

Session V: ENCRYPTION

DECISION SOUGHT / ACTIONS TO BE TAKEN

This agenda item asks the Ministers to indicate their support for a common approach, pursued individually by each of the Five Eyes countries, when engaging with communications service providers regarding reasonable assistance to the operations of law enforcement and national security agencies.

Ministers should discuss a shared position regarding the assistance that our countries should reasonably expect from communications service providers and device manufacturers. Ministers should also discuss ways to address challenges posed by encryption, such as more robust collation of examples and sharing mechanisms amongst Five Eyes law enforcement partners.

To improve the level of assistance provided by communications service providers and device manufacturers, Ministers should:

1. **[Discuss] a common approach to service providers based on the stakeholder engagement plan** prepared by the Quintet Experts Working Group on Cybercrime.
2. **Discuss the level of assistance** that can be reasonably expected of communications service providers and device manufacturers in providing law enforcement access to data under each country's laws.
3. **Agree to collate and share** examples where ubiquitous encryption has impacted investigations, to be presented to providers and to be used to help build public understanding, awareness and support for approaches to encryption that support the requirements of law enforcement and appropriately protect privacy.
4. **Reinforce the value** of encryption in protecting sensitive personal and commercial data and as a core element of good cybersecurity, while recognizing the legitimate need of law enforcement to obtain lawful access to data in investigations to protect public safety.

DESCRIPTION

In the past few years, strong encryption has become increasingly prevalent on hardware, operating systems, social media and other software applications. Encryption is increasingly implemented in a manner that prevents law enforcement and national security agencies from obtaining critical information during investigations. In particular, end-to-end encryption has made it difficult to access the content of communications through lawful interception. Encryption has been implemented more broadly in the following ways:

- encryption of information contained on computers, smartphones and other devices seized by law enforcement agencies (device encryption);
- encryption of stored communications and other information held on cloud-servers by service providers (encryption of 'data at rest'); and
- encryption of communications passing real-time over the networks ('data-in-motion' or end-to-end encrypted communications).

The Quintet of Attorneys-General has acknowledged that engagement with communications service providers could form part of the response to the challenges posed by encryption. Service providers can provide a range of assistance to agencies and investigations, including:

- developing technical solutions that permit law enforcement to lawfully obtain critical, yet encrypted

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



information in transit, stored on electronic devices, and stored in the cloud pursuant to lawful process;

- providing voluntary disclosures of non-content data upon request from law enforcement from non-US Five Eyes countries;
- working with governments to find technical solutions to certain encryption designs that result in unrecoverable data for law enforcement; and
- providing robust assistance in emergency situations.

The need for criminal law enforcement agencies to be able to obtain necessary and lawfully approved information generated from their devices/services in an intelligible format is critical to the protection of public safety. There would be benefit in consistent messaging from Five Eyes countries' about these issues, including during engagement with communications providers. It is important to communicate the need to consider the providers' business interests, including reputational risks and privacy-orientated marketing, as well as the needs of law enforcement agencies and public safety. This includes supporting encryption and its benefits for cybersecurity and privacy protection, as well as personal rights and freedoms, and recognizing that these goals are not inconsistent with lawful access solutions. Relevant practical examples of circumstances in which encryption has hindered investigations across jurisdictions can help make the case for better assistance both publicly, and in discussions with providers.

Accordingly, at their 2016 meeting the Quintet of Attorneys General asked the Quintet Experts Working Group on Cybercrime to facilitate the exchange of ideas on engaging with providers on the issue of encryption. The Working Group has developed a Stakeholder Management Plan to guide a consistent approach to discussions with communications service providers and device manufacturers, and seeks Ministers' support for the plan.

BACKGROUND

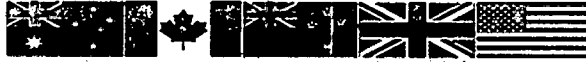
Governments support the use of strong encryption to protect personal, commercial and government information. In addition, communications service providers and device manufacturers enable encryption, often by default, in order to protect the interests of their customers. Privacy advocates and proponents of civil liberties advocate to providers and manufacturers for default encryption as a means to protect personal information.

Encryption underpins modern information and communications technology, and it supports confidence in a secure cyberspace. This strengthens the exercise of rights to free expression and privacy, and also enables e-commerce. Encryption is no longer a tool for experts; it is now available to the general population by default, and is generally regarded as network security best practice. In response to growing public concerns regarding online privacy and cybersecurity it is strongly supported by communications service providers and device manufacturers that employ it to protect the interests of their customers. Technological experts, privacy advocates and proponents of civil liberties have also strongly supported the widespread availability of strong encryption.

However, the proliferation of real-time communications applications that offer end-to-end encryption (where decryption capability is limited to the end user, rendering data unreadable to everyone but the communicating parties) is allowing serious criminals to secure their communications against lawful acquisition and decryption requests by law enforcement agencies. Accordingly, the prevalence of end user encryption severely restricts agencies' access to critical evidence found on computers, smart phones and other devices and transiting telecommunications networks that is needed to protect public safety. For example, full disk encryption offered by popular brands of smartphones can impede lawful searches of those devices. These technologies allow subjects of investigation to protect their communications from an investigation without having taken any intentional steps to hide their activities, and access is impeded when agencies are lawfully authorized to

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



acquire that information.

To adapt to encryption, agencies are using other powers and techniques to obtain information when it is not encrypted. Although alternative collection capabilities can sometimes mitigate challenges by providing access to information when it is not encrypted, such techniques can be expensive, may not be scalable, and do not always guarantee success. They are also only ever a partial solution to the problem posed by ubiquitous encryption. Such capabilities have their limitations (such as cost and longevity), and other strategies (such as an increase in traditional methods of law enforcement and information gathering), will not be enough to mitigate the impact of encryption in the long run.

Ultimately, default encryption where the decryption capability is limited to the end user may prevent lawful access by governments to information for the purpose of investigation. This presents a threat to public safety when access to communications is crucial to prevent and solve crime, or to protect national security. Governments should be able to obtain decrypted evidence where it has lawful authority to do so in order to be responsible for protecting public safety and seeking justice.

RECENT CASE EXAMPLES/DEVELOPMENTS

Westminster

On 22 March 2017, an Islamist inspired terrorist attack occurred in London. A man later identified as Khalid Masood drove into pedestrians on Westminster Bridge before stabbing an unarmed police officer to death at the Houses of Parliament. Masood was shot dead by a close protection officer. Immediately prior to the attack he had connected to the Facebook owned and encrypted WhatsApp messaging service. This triggered a public and media debate in the UK on the issue of end-to-end encryption.

San Bernardino

On 2 December 2015, 14 people were killed and 22 others injured in an attack by Syed Rizwan Farook and Tashfeen Malik in San Bernardino, California. As part of the subsequent investigation, on 9 February 2017 the FBI announced that it was unable to access data on an Apple iPhone that it had lawful authority to search. The manufacturer of the phone, Apple Inc. declined to assist the FBI in overcoming the encryption security features of the device, despite its acknowledged ability to develop a solution to provide such assistance. Apple was then ordered by a US District Court to assist the FBI, but contested the order in court, and also addressed the issue publically in the media. The FBI was able to unlock the phone via assistance from a third party before the issue could be decided by the court.

Subsequently, former FBI Director James Comey indicated that between September 2016 and April 2017, the FBI had been unable to access the content of more than 3,000 mobile devices using appropriate and available technical tools, even though there was legal authority to search these devices. This figure represents nearly half of all the mobile devices the FBI attempted to access in that timeframe.

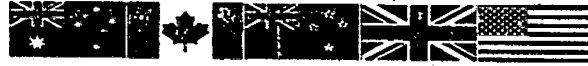
Canada's National Security Consultation

The Canadian government recently conducted an extensive consultation on Canada's national security framework. Encryption, and law enforcement challenges it poses, were part of this consultation. A significant proportion of the feedback indicated privacy concerns and objected to modifying Canada's legal framework to address this problem for law enforcement (over 70% of the responses from the public opposed giving authorities the power to compel decryption). In addition, the House of Commons Committee studying the issues raised in the national security consultation (the Standing Committee on Public Safety and National Security) recently released a report recommending that the government not pursue legislation in relation to this issue, and that the issue be examined further.

SUGGESTED COMMUNIQUE LINE

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



The governments of Australia, Canada, New Zealand, the United Kingdom and the United States support the use of strong encryption by individuals, businesses, and governments in order to protect private and sensitive information. Governments also agree that the proliferation of default encryption for data stored on devices and real-time communications, where decryption capability is limited to the end user severely undermines public safety efforts by impeding lawful access to the critical content of communications during investigations into serious crimes, including terrorism. Governments will continue to cooperate with one another and to work with communications and technology companies to obtain the information needed to protect national security and public safety, while upholding cybersecurity and individual rights and freedoms.

CHAMPION/S

Australia.

ANNEXES

- *Annex 1: Draft – Quintet Experts Working Group on Cybercrime – Encryption Outcome – Stakeholder Management Plan*

Tab 8C

**Pages 594 to / à 601
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1) - Int'l

**of the Access to Information
de la Loi sur l'accès à l'information**

Tab 8D

DRAFT

FOR OFFICIAL USE ONLY

VERSION 18 – June 15, 2017

RDIMS 2213192

FIVE COUNTRY MINISTERIAL

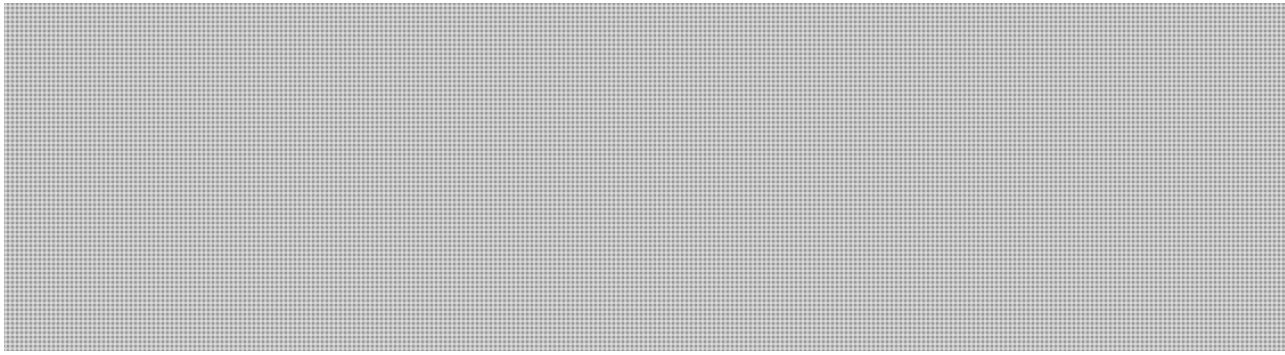


FCM 2017 – Agenda Items
(3 pages maximum)

Five Eyes Collaboration on Cyber Security

DECISION SOUGHT / ACTIONS TO BE TAKEN

What is the action sought from the Ministers at the FCM regarding this issue? (e.g. expected results, agreement on coordinated approach, approval of principals or document, discussion on lessons learned, etc.)



DESCRIPTION

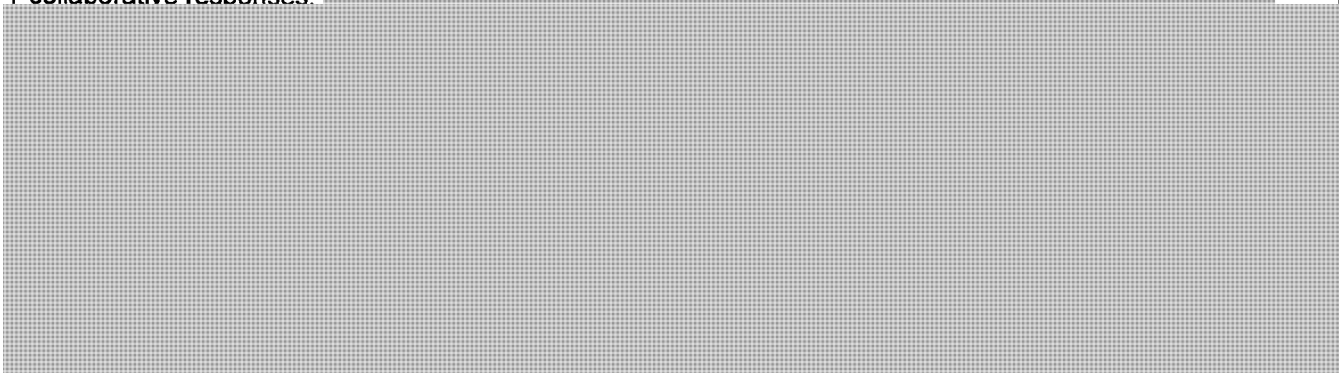
Short description (1-2 lines) of the topic/issue as it is understood in the FCM context

Collaboration across the Five Eyes in addressing cyber security issues within the domains of operational incident response, policy and strategy development, and innovation

BACKGROUND

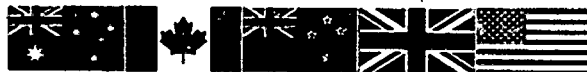
What has FCM done in the past regarding this issue? How this issue has evolved in the last years? What are the significant gaps remaining?

Five Eyes collaboration on cyber security has been recognized by FCM Ministers as well established, long standing, and mutually beneficial. Cyber threats are increasingly international in nature and require collaborative responses.



At the strategic level, Five Eyes countries continue to assess key emerging issues and trends through the

FIVE COUNTRY MINISTERIAL



Ottawa 5 policy coordination group. The group has been a key venue for sharing information and lessons learned on national approaches, all of which have been renewed or reviewed in the last two years:

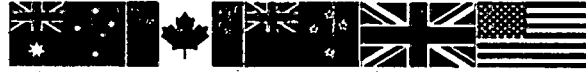
- Australia released its renewed cyber security strategy in April 2016, with priorities including developing a national cyber partnership, creating strong cyber defences, enhancing global responsibility and influence, stimulating growth and innovation, and creating a cyber-smart nation.
- Canada is completing a Cyber Review to take stock of the evolving threats in cyberspace, to understand and explore the ways that cyber security is becoming a driver of economic prosperity, and to determine the appropriate federal role in this digital age.
- New Zealand adopted a new Cyber Security Strategy in 2015 that centers on four goals: cyber resilience, cyber capability, addressing cybercrime and international cooperation. In April 2017, the national CERT officially opened with the mandate to monitor, track and advise on cyber incidents.
- The United Kingdom's November 2016 National Cyber Security Strategy sets out the themes of *defence* against the threat, *deterrence* of hostile actions against the UK, its people, businesses and allies, and *development* of the cyber security industry, enhancement of cyber security skills and strengthening of the scientific research base. In October 2016, the National Cyber Security Centre was established to consolidated cyber operational responsibilities and capabilities.
- The United States adopted the Cybersécurité National Action Plan (CNAP) in 2016 to strengthen federal cyber security, enable private sector organizations and individuals to better protect themselves, disrupt and deter adversary activity, and respond more effectively to incidents. Most recently, the May 2017 Executive Order on cyber security orders a number of government departments to develop a likeminded deterrence and response strategy for malicious cyber incidents.

The Ottawa 5 has also been successful in advancing Five Eyes positions in international fora. The promotion of peacetime norms of state behavior, which originated within the Ottawa 5, is an important example. Gaining international support for these norms is as important as the process of creating them, and the group has provided an important mechanism for developing strategies to promote these norms internationally.

At the October 2016 meeting in Canada,

Digital innovation has become an engine of growth in the 21st century and is now a key driver of economic prosperity in Five Eyes countries.

FIVE COUNTRY MINISTERIAL



RECENT DEVELOPMENTS

What additional information is needed for the ministers to understand this issue?

Recent global cyber incidents have emphasized the importance of close operational coordination amongst the Five Eyes. The April 2017 cyber incident affecting international Managed Service Providers (MSPs), for example

it also demonstrated opportunities for enhancing the efficiency and quality of joint responses, such as sharing approaches to public messaging, which were found to be largely reusable across our nations. The May 2017 WannaCry Ransomware campaign illustrated the speed with which a novel cyber attack can achieve global impact, even though its prevention was straightforward and publicly known in advance of the campaign. Usual 5 coordination clarified how WannaCry's impact varied across nations, helping inform response. Usual 5 members have signaled their intention to continue exchanging information to enhance the Five Eyes ability to respond in a coordinated manner to cyber events that have international implications.

The continued evolution of Five Eyes nations' national cyber security strategies emphasizes the rapid pace of evolution of cyber issues and the need to continually be looking forward. As such, the Ottawa 5 has signaled that it will continue their efforts to identify, study and address emerging cyber issues that continue to pose challenges across the Five Eyes, such as:

With respect to digital innovation and workforce development, recognizing that this is an emerging opportunity for collaboration,

SUGGESTED COMMUNIQUÉ LINE

CHAMPION/S

Which country or countries will lead the discussion on this issue at the Ministerial?

Canada

ANNEXES

There is no annex to this background paper.

Tab 9

Five Country Ministerial 2017**JOINT COMMUNIQUÉ****DRAFT**

We, the interior Ministers, immigration Ministers, and Attorneys General of Australia, Canada, New Zealand, the United Kingdom and the United States met in Ottawa on June 26, 2017, to discuss both national security challenges facing our nations and proactive areas for collaboration. Our five country partnership, founded after the Second World War and strengthened during the Cold War, is more relevant today than ever as we deal with the relentless threats of terrorism, violent extremism, cyber-attacks, and international instability, while retaining our deep commitment to the shared values of democracy, human rights and the rule of law.

Countering violent extremism

[REDACTED]

During the Five Country Ministerial meeting, we agreed on joint efforts to counter the spread of violent extremism and recruitment efforts by extremist groups [REDACTED] that advocate, and utilize violence to achieve their objectives. Ministers agreed to:

- A shared approach to engage with Communication Service Providers to address online terrorist activities and propaganda, and to support a new industry forum led by Google, Facebook, Microsoft and Twitter.
- Collectively enhance knowledge on key issues such as design and support for local-level initiatives and sharing of best practices in prevention and intervention, such as approaches to mitigating the threat posed by returning foreign terrorist fighters and their families.
- Examine the role of traditional and social media and community voices in facilitating or disrupting processes of radicalization to violence or the threat of terrorist propaganda.

Global migration and refugee systems

[REDACTED]

[REDACTED]

Security cooperation on border management and human trafficking

The joint meeting between the Five Country Ministerial and the Quintet of Attorneys General provided the opportunity to discuss the tools available for sharing information on criminal activities, including terrorism and human trafficking. The recent brutal attacks in the UK, Afghanistan and elsewhere also serve as a reminder that Daesh and its affiliates will continue to attack soft targets in public spaces. In order to help prevent these [REDACTED] plots, the Ministers and Attorneys General agreed that sharing information among partners on known criminal and terrorist actors is vital. [REDACTED]

[REDACTED] To enable targeted action, the Ministers and Attorneys General agreed to direct their law enforcement agencies to share experiences of how partners are tackling this global challenge and identify opportunities for joint operations.

Cyber security

Ministers and Attorneys General noted their concerns with the recent cyber-attacks that have affected various institutions and individuals in all of our countries. The "WannaCry" ransomware attack, which began on May 12th and impacted individuals in over 150 countries, is an unfortunate reminder that [REDACTED] cyber-attacks are increasing. [REDACTED]

[REDACTED]

We [REDACTED] today on concrete steps to address issues and new challenges related to countering violent extremism, migration and refugees, security cooperation on border management and human trafficking, and cybersecurity. While our five countries share similar security challenges that predicate this strong collective response, we more

importantly share a history of cooperation, friendship, and common values. We are committed to building on this past cooperation in national security affairs and remain accountable for the steps we have pledged to take today. Throughout these discussions, we ██████████ that building public trust within our countries is required to move forward on national security issues. Enhanced safeguards and greater efforts to promote transparency are critical in this respect.

The Five Country Ministerial and Quintet meeting of Attorneys General were hosted by Canada's Minister of Public Safety and Emergency Preparedness, the Honourable Ralph Goodale, and Minister of Justice and Attorney General of Canada, the Honourable Jody Wilson-Raybould, in collaboration with the Minister of Immigration, Refugees, and Citizenship, the Honourable Ahmed Hussen. They met with their international counterparts from Australia, the United Kingdom, the United States and New Zealand. These included George Brandis, Australian Attorney General; Peter Dutton, Australian Minister for Immigration and Border Protection; Christopher Finlayson, New Zealand Attorney-General; Michael Woodhouse, New Zealand Minister of Immigration; Amber Rudd, United Kingdom Home Secretary; Jeremy Wright, United Kingdom Attorney General; John Kelly, United States Secretary of Homeland Security; and Jeff Sessions, United States Attorney General.

Tab 10

Five Country Ministerial Joint Communique Round Table and Closing Remarks

**Joint Communique Round Table
And Closing Remarks**

Five Country Ministerial Conference

Ottawa, ON, Canada

June 26, 2017

Discussion on Joint Communique

- Over the course of today we have touched on four critical topics for the safety and security of our countries.
- At this time I would like to encourage a short discussion on the joint communique.
- We can use this time to address any concerns that you may still have regarding the wording of the draft communique, which was circulated to your officials in the last few weeks.
- Following our meeting, we will move to adopt the communique in order to show our commitment to addressing the issues and challenges we have been discussing.

Closing Remarks

- Distinguished guests and participants of the 2017 Five Country Ministerial, it has been an honour to meet with, and host, each of you in our nation's capital.
- July 1st will mark one hundred and fifty years since the confederation of Canada.
- In the lead up to the celebrations, Canadians have been reflecting on the ideals and values that led to the founding of this great country; and how our principles of human rights, democracy, and the rule of law have stood the test of time.
- Yet, as we have discussed today, they have become increasingly threatened by those at home and abroad who wish to undermine our freedoms and jeopardize our safety.
- I believe I speak on behalf of all Canadians when I say that we are fortunate to find likeminded friends and partners in the United States, Australia, New Zealand and the United Kingdom, who stand with us against these threats.
- I would like to thank all of you for coming and working together to keep our citizens safe, and to secure our shared values, rights and freedoms.

Five Country Ministerial Joint Communiqué Round Table and Closing Remarks

- Since our previous meeting in February last year, each of our national security and intelligence communities have deterred and prevented countless threats.
- Yet tragically, we have bared witness to acts of terrorism within our own countries. From London to Melbourne, and Orlando to Quebec City, we have collectively grieved and prayed for those who have been lost.
- Protecting our communities from the threat of terrorism is of the utmost importance to the Government of Canada, and these events highlight the significance of following through on the commitments we have made today.
- Our study of radicalization to violence has made clear that the first element of a successful counter-terrorism strategy must be prevention.
- We must continue to engage with diverse communities and local-level organizations on a range of issues to develop trust, and build long-term relationships to counter radicalization before it turns violent.
- We must also work to increase public awareness of the threat, including the role of news sources, social media, and Communication Service Providers, in order to build community resilience and resistance to radicalization.

- However, these meetings have shown that terrorism and violent extremism are not the only threat to our societies.
- Together we have worked to address the security challenges presented by the growing waves of refugees and migrants who reach our shores. While the vast majority of these individuals embark upon new lives and enrich the fabric of our respective nations, the minority of those attempting to exploit these opportunities for nefarious purposes disproportionately endanger our collective well-being.
- The safety of our citizens and the security of our nations must always be our first priority, and it requires that we simultaneously strengthen our borders and support the countries and legitimate organizations that are on the frontlines of these refugee and migrant flows.
- Additionally, by ensuring adequate information sharing between our countries, and establishing a community of experts, we will help guarantee proper vetting processes are in place to overcome new challenges such as social media screening.
- Effective information sharing and cooperation amongst our law enforcement communities will also help to make

efficient use of watch lists, and help to reduce human trafficking, one of the most heinous crimes imaginable.

- In today's world of high speed technology, being able to make vital information available in a timely manner while respecting the rights of our citizens is more necessary and challenging than ever.
- Furthermore, our work here on advancing technological tools and systems has been proactive and necessary to address emerging and future threats in the cyber realm.
- Cyber-crime, hacking and encryption, each pose challenges unique to the 21st century that we must continuously engage with.
- Our work on these issues has been vitally important, and will help us to navigate a challenging security landscape.
- I am truly grateful for this community dedicated towards common goals, and ultimately, the security of our nations.
- Thank you very much for being here, I look forward to following through on the commitments we have made together, and I remain optimistic about our ability to successfully overcome the challenges of this dangerous world.

-

Invitation for Minister Wilson-Raybould to Speak

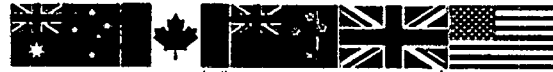
- At this time, I would like to invite the Honourable Jody Wilson-Raybould, Minister of Justice and Attorney General of Canada, to say a few words.

Tab 11

Tab 11A

FOR OFFICIAL USE ONLY

FIVE COUNTRY MINISTERIAL



FCM2017 & FCM/Quintet Joint Meeting: Reception Agenda

| | |
|---------------|--|
| Timing | Action: June 26 |
| 19:30-20:15 | Attendees are served drinks (informal chats), ambient music playing in the main room, Mounties in official uniform |
| 20:15-20:20 | Toast by Canadian host |
| 20:15-21:15 | Dinner: Three Course Meal, gifts are waiting for attendees at the tables (TBC) |
| 21:15-22:00 | Time allotted for bilateral talks, informal meetings, if needed. |
| 22:00 | Conclusion of reception/dinner |

Reception/Dinner Event:

Location:

- Sir John A MacDonald Building
- 144 Wellington St, Ottawa, ON K1A

Expected Guests:

- Between 120-140
- Delegates of the Quintet and FCM
- Include 10 Ministers and Attorneys General, and four ambassador/high commissioners

Notable Guests:

| Canada | The United States | The United Kingdom | Australia | New Zealand |
|--|---|--|---|--|
| The Honorable Prime Minister Justin Trudeau (TBC) | John F. Kelly (Secretary, Department of Justice) | Amber Rudd (Home Secretary) | George Brandis (Attorney General of Australia) | Christopher Finlayson (Attorney General) |
| Hon. Ralph Goodale (Minister of Public Safety) | Jeff Sessions (Attorney General of the U.S.) | Howard Drake (British High Commissioner to Canada) | Peter Dutton (Minister of Immigration) | Michael Woodhouse (Minister of Immigration) |
| Hon. Jody Wilson-Raybould (Attorney General of Canada) | Elizabeth Moore Aubin (United States Chargé d'Affaires) | | Tony Negus (Australian High Commissioner to Canada) | Daniel Mellsop (New Zealand High Commissioner to Canada) |
| Hon. Ahmed Hussen (Minister of Immigration) | | | | |

FOR OFFICIAL USE ONLY

Alcohol:

- Variety of Canadian wines from B.C. will be made available to the guests over the duration of the event

Entertainment:

- Ambient music
- Photograph on-site
- Selfies with Mounties (available at entrance from 19:00-20:15)

Food:

- Dinner will consist of a three-course meal
- There will be a buffet available for additional support staff in a separate room

Gifts:

- We will be providing small gifts celebrating Canadian culture (100ml bottle of maple syrup)

Guest Speaker:

- Prime Minister Justin Trudeau (TBC)

Dress code:

- Business attire

Tab 11B



BIOGRAPHY

Tony Negus

**Australian High Commissioner
to Canada**

The Australian High Commissioner to Canada is His Excellency Mr Tony Negus AO APM. Taking up his appointment in February 2015, Mr Negus previously served in the Australian Federal Police for 32 years and most recently as its Commissioner from 2009-2014.

In 2016 Mr Negus was named in the Australia Day Honours List as an Officer in the Order of Australia (AO). He has also been awarded the Australian Police Medal (APM) in 2005.

Mr Negus has been awarded several international awards including the INTERPOL Medal in 2014 in recognition of his significant contribution to global safety and security, the Indonesian National Police Meritorious Service Star in 2012 and the International Police and Public Safety 9/11 Medal (USA) in 2012.

Mr Negus holds a Masters of Public Policy and Administration from Charles Sturt University, a Graduate Diploma of Executive Leadership from the Australian Institute of Police Management, and has attended a Harvard University leadership program. Mr Negus is married with three children.



BIOGRAPHY

Daniel Mellsop

**New Zealand High
Commissioner to Canada**

Daniel Mellsop was appointed New Zealand High Commissioner to Canada in February 2016. He is concurrently High Commissioner to Jamaica.

Daniel is a career diplomat. During his time in the New Zealand Ministry of Foreign Affairs and Trade he has worked on a wide range of issues, from trade negotiations to counter-terrorism. Previous appointments included postings to the New Zealand embassies in The Hague and Seoul. He also undertook a secondment to the Office of the Minister of Foreign Affairs, Murray McCully.

Prior to taking up his appointment in Ottawa, Daniel was the Head of the International Branch at the Ministry of Defence. The branch is responsible for providing policy advice to the government on international military deployments and other international defence engagements. As a senior official, Daniel was heavily involved in leading bilateral and multilateral defence diplomacy activities.

Daniel attended the University of Waikato in New Zealand where he studied Korean and Economics graduating with a Bachelor of Arts and Master of Management Studies with honours.

Daniel is joined in Ottawa by his partner Jane Hooker and two children. Daniel and his family are passionate about embracing the great Canadian outdoor lifestyle.



BIOGRAPHY

Howard Drake

British High Commissioner to Canada

Howard Drake was appointed British High Commissioner to Canada in June 2013. Prior to taking up his current position, Howard served as Her Majesty's British High Commissioner to Jamaica as well as non-resident British High Commissioner to the Commonwealth of the Bahamas. From 2005 to 2009 Howard served as Her Majesty's Ambassador to Chile.

His career in HM Diplomatic Service has focussed on political and commercial work, including heading the UK's inward investment operation in the US from 1997 to 2002 and earlier political assignments in Singapore and Chile. In London Howard has worked on European Union affairs and counter-proliferation, and served as Assistant Director for Human Resources.

Howard is married to Gill. They have a daughter and a son.



BIOGRAPHY

Elizabeth Moore Aubin

US Chargé d'Affaires

Elizabeth Moore Aubin is serving as the Chargé d'Affaires ad interim in Ottawa, Canada. She began her tenure as the Deputy Chief of Mission in May 2016 and became Chargé d'Affaires on January 18th, 2017 after the departure of Ambassador Bruce Heyman.

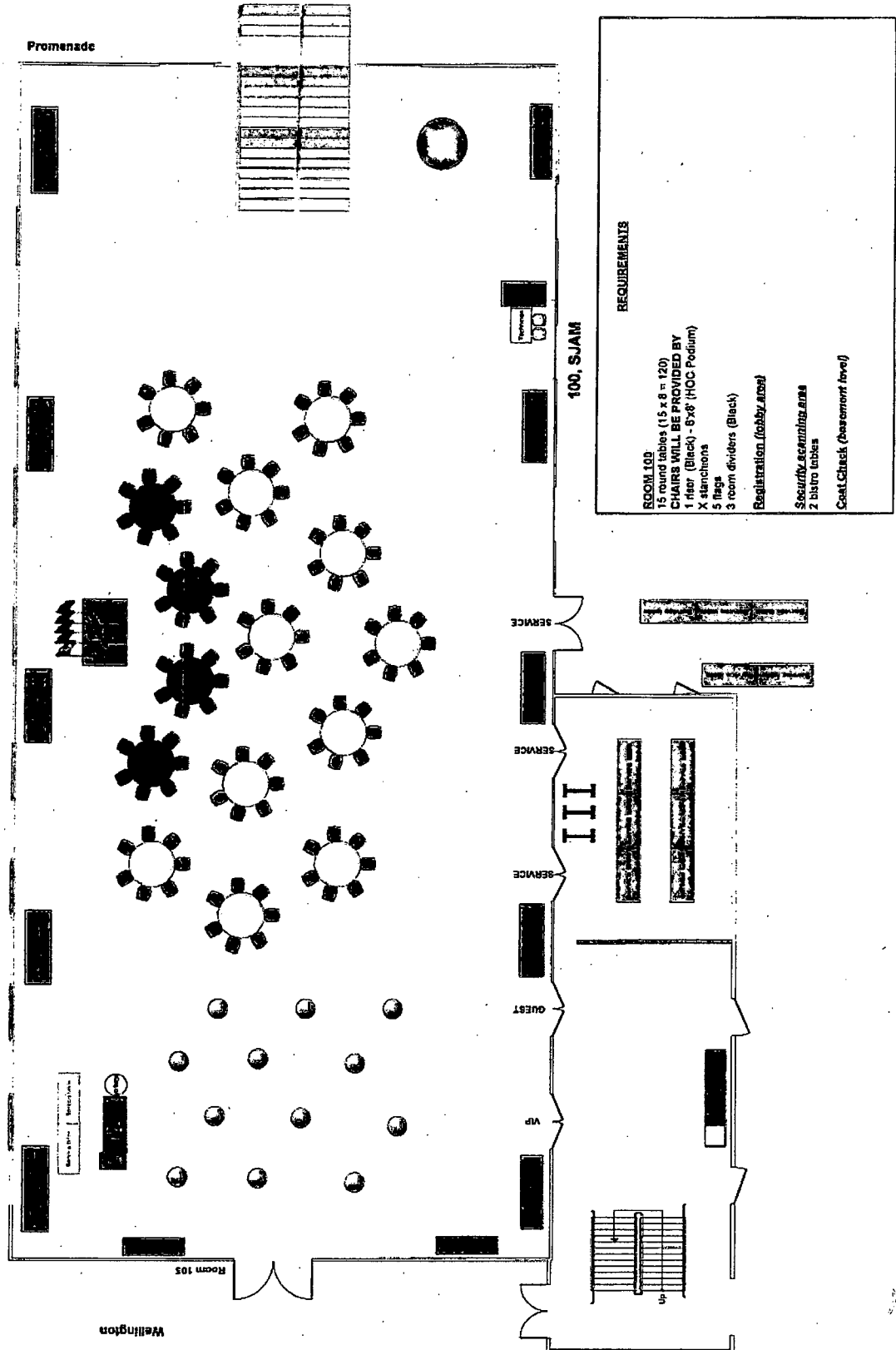
Previously, she was the Executive Director for the Bureau of Western Hemisphere Affairs where she provided policy direction, guidance and planning for the management of 53 diplomatic posts in the Western Hemisphere. From 2011-2014, she served as the Deputy Chief of Mission at the U.S. Embassy in Algiers, winning the Department's Commercial Advocacy Award in 2013.

Elizabeth has served in the State Department as: the Director for Human Resources for the joint Executive Office of the Bureaus of Near Eastern Affairs and South and Central Asian Affairs; a Special Assistant to the Under Secretary for Management where she coordinated macro-management issues for the diplomatic operations in Iraq and Afghanistan; as a Post Management Officer in the Western Hemisphere Affairs Bureau; as well as two tours in the Executive Secretariat; and as a Watch Officer and a Line Officer.

Overseas, she has served as: the Management Counselor for Embassy Tel Aviv; International Resource Management Officer for USNATO in Brussels; Management Officer at the Consulate General in Toronto; and as a General Services Officer at the Consulate General in Hong Kong. Her two entry level tours were as an Economic Officer at Embassy Rome and as a Consular Officer at the Consulate General in Curacao.

Elizabeth holds the rank of Minister-Counselor in the Foreign Service. She speaks French and Italian and has a B.A. in Political Science from Barnard College, 1987. She is married to Daniel J. Aubin.

Tab 11C



Tab 11D

**DRAFT ONLY
FOR INFORMATION
UNCLASSIFIED**

2017-007913

**Talking Points
FCM-Quintet Dinner Toast – Minister Wilson-Raybould
June 26, 2017, Ottawa**

- **Friends and colleagues, new and old.**
- **Welcome to Canada and the eighth meeting of the Quintet of Attorneys General and the fourth meeting of the Five Country Ministerial.**
- **We had a fruitful day of discussions today and I look forward to the meeting of the Quintet tomorrow, but first I hope you will enjoy some Canadian hospitality.**
- **This is a very special time for us in Canada. We have recently celebrated the 35th anniversary of our Charter of Rights and Freedoms – which as you know has inspired bills of rights around the world, including New Zealand. It is also the 35th anniversary of Section 35 of the Constitution Act, 1982, dealing with the rights of Indigenous peoples.**
- **And of course, we are just days away from celebrating the 150th anniversary of our Confederation. You can see all the preparations underway across the street on Parliament Hill for a giant party.**
- **And what an appropriate location for our dinner tonight – this amazing building is named after Sir John A. Macdonald –**



who was not only our first prime minister but also our first Attorney General.

- **This art deco/Beaux-Arts edifice, built in the early 1930s, was for a long time a bank building until it was painstakingly restored and reopened in June 2015. The building is Green Globes certified and earned the highest possible eco-rating for serving as a world leader in energy and environmental performance.**
- **You will find at your places a bottle of Canadian maple syrup in the shape of a maple leaf as a small token of our thanks. It also has on it the Canada 150 logo highlighting our year-long birthday celebrations.**
- **As you may know, both maple syrup and the maple leaf occupy a special place in Canada's history. Since 1965, the maple leaf has of course had a prominent role on our national flag.**
- **I would also note with pride that the wine you are drinking tonight is from my home province of British Columbia.**
- **So when you return home after our meetings tomorrow, I hope you will savour this tasty memory of your visit to Canada.**
- **May I ask you to raise your glasses and join me in a toast to justice.**
- **Enjoy your dinner. Bon appétit!**

Tab 12

FOR OFFICIAL USE ONLY // FIVE EYES USE ONLY

FINAL

Five Country Ministerial – Quintet Meeting
Agreements and Outcomes
February 16-17, 2016

Joint Quintet – Five Country Ministerial Discussions

The Attorneys General and Ministers actively discussed each agenda item and reached a common understanding to:

- Direct officials to explore barriers and limitations to information sharing, both domestically and internationally, with our partner agencies, with consideration for protection of rights. The officials should examine what information sharing can assist the mission of border, immigration and transportation security agencies, including criminal history and watchlist information, while bearing in mind limits that may be appropriate for classification, resource, privacy, legal, and other reasons.
- Advance discussions toward the goal of enhancing cooperation for screening refugees and asylum seekers, including consideration of the principle that the biometric information of refugees and asylum seekers destined for one of the countries should be vetted by all Five Countries, to the extent practicable. Ministers directed their officials to draft Terms of Reference for consideration and further direction.
- Welcome the Canadian Public Safety Minister's offer to provide a report on the Canadian experience of resettling 25,000 Syrian refugees between November 2015 and February 2016.
- Develop a common approach to engage internet service providers and work to share best practices and methods for countering violent extremism, create an exchange program between officials, and enhance analytical cooperation to measure the impact of CVE programs.
- Continue to exchange ideas on how to engage the private sector on encryption, with the aim to coordinate approaches and share views on challenges.
- Direct their officials to work together to identify ways to more effectively share information on best practices, risk methodologies, and patterns of foreign investment transactions across the Five Countries that might implicate national security concerns.
- Meet again jointly to discuss issues of mutual interest and importance.
- Establish an Executive Steering Group to meet semi-annually by Secure Video Teleconference at the Under Secretary/Assistant Secretary level to share a briefing on threats, implement the actions agreed to at the meeting, and direct work between meetings.
- Invite the Immigration Ministers to join in the Five Country Ministerial, recognizing the inherent intersection between security and immigration.

Five Country Ministerial Discussions

For those agenda items specifically discussed among the Five Countries Ministers, the Ministers actively discussed each item and reached a common understanding to:

FOR OFFICIAL USE ONLY // FIVE EYES USE ONLY

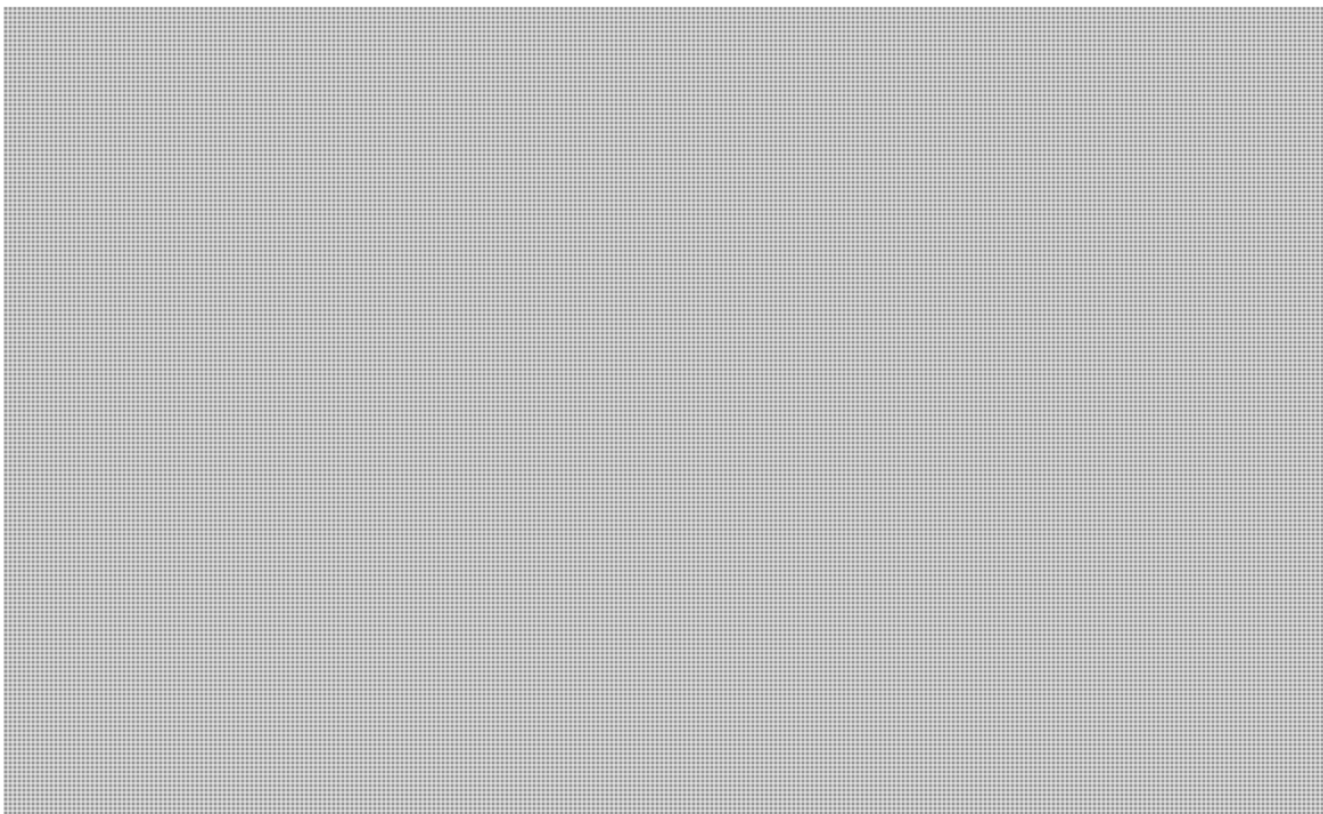
000633

FOR OFFICIAL USE ONLY // FIVE EYES USE ONLY**FIN/**

- Approve and welcome the Five Country Conference Annual Research Taskforce Report recommendations, and direct officials to work toward implementing these recommendations.
- Continue to inform each other of developments to visa requirements and exemption regimes, and noted the value of trusted traveler programs to increase travel facilitation benefits for our citizens, and directed that the FCC continue its efforts to maximize facilitated travel among the five, consistent with security and other requirements.

Quintet Discussions

For those agenda items specifically discussed among the Five Countries Attorneys General, the Attorneys General actively discussed each item and reached a common understanding to:



**Pages 635 to / à 639
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1) - Int'l

**of the Access to Information
de la Loi sur l'accès à l'information**

Tab 13

Five Eyes forums matrix

QUINTET OF ATTORNEYS GENERAL
Attorneys General Forum on legal issues and cooperation
(cybercrime, terrorism, organised crime, prevention, etc)
Quintet Steering Committee calls between annual Quintet

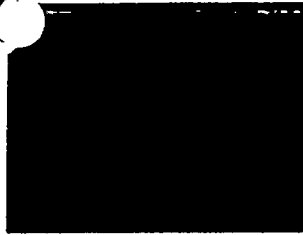
FIVE COUNTRY MINISTERIAL (FCM)
National Security Forum between Ministers
(Border Security-Immigration-Cyber Security-Critical Infrastructure-CVE-Counterterrorism)
Executive Steering Group and Sherpa calls between annual FCM

Foreign Terrorist Fighters Working group

Mutual Legal Assistance Working group

Cybercrime Working group

Countering Violent Extremism Working Group



FIVE COUNTRY MINISTERIAL (FCM)
National Security Forum between Ministers
(Border Security-Immigration-Cyber Security-Critical Infrastructure-CVE-Counterterrorism)
Executive Steering Group and Sherpa calls between annual FCM

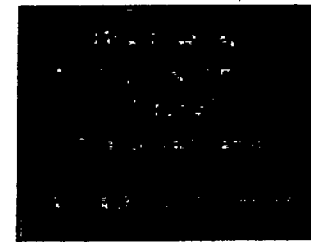
Border 5 (B5)
Commissioner/
President of Agencies
Customs and Border

Five Nations (5N)
Passport Senior management
Passports

Ottawa 5 (O5)
High level executives
Cyber Security Policy

Usual 5 (U5)
Executives & Managers
Cyber Security Operations

Critical 5 (C5)
Executives & Managers
Critical Infrastructure



HINT
Heads of Intelligence

Anti-Fraud Working Group

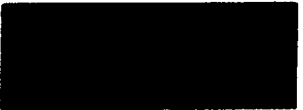
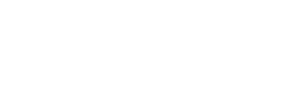


Targeting Working Group

Forecasting and Data Analytics WG



Data Analytics Working Group



Research & Development



Five Eyes forums matrix

| Five Eyes Forum | Mandate/Purpose |
|---|--|
| Five Country Ministerial | To collectively pursue and support policies and initiatives on the most immediate and pressing issues confronting national security and public safety amongst the Five Eyes partners, such as cybersecurity/encryption, foreign investment in critical infrastructure, countering violent extremism, counterterrorism, data exchange initiatives, and border security. |
| Quintet of Attorneys General | To bring together the Attorneys General of the Five Eyes to work jointly to address legal challenges of common interest such as cybercrime, organised crime, terrorism, genocide and innovative approaches to prevention of youth violence, as well as to promote justice and legal cooperation. |
| Migration 5 (M5 - Former FCC) | To discuss and collaboratively advance immigration priorities and shared goals, initiatives of mutual concern |
| Five Country Citizenship Conference (FCCC) | To exchange information and discuss issues as well as different practices related to citizenship and nationality law, regulations, policy and services delivery. |
| Border 5 (B5) | To foster closer collaboration and information sharing among the customs agencies |
| Five Nations (5N) | To leverage collective capabilities, enhance the security, improve service delivery, and maximize operational efficiency of the Five Eyes countries passport systems. |
| Ottawa 5 (O5) | To provide policy guidance to the Usual 5 and to address strategic cyber-related goals and objectives in a collaborative environment among principle-level members of five key allied nations. |
| Usual 5 (U5) | To enhance operational cybersecurity coordination and collaboration and to increase interaction with global cybersecurity information sharing and operational collaboration among the Five Eyes members |
| Critical 5 (C5) | To coordinate and collaborate on critical infrastructure protection and resilience issues of mutual interest |
| Five Eyes Law Enforcement Group (FELEG) | To enhance the collective capability of the Five Eyes to combat transnational crime and to agree on the direction of joint-cooperation to tackle serious and organized crime, through key shared priorities and agreed-upon annual deliverables. |

Tab 14

**Government of Canada Communications Approach
Five Country Ministerial Meeting Quintet of Attorneys General, Ottawa, June 26-27, 2017
Notes**

Objective

- To support the principle of transparency in regards to national security

Considerations

- The Five Country Ministerial will meet on June 26. A joint meeting is planned on that same day between the Five Country Ministerial and the Quintet of Attorney Generals. The Quintet will meet on June 27.
- Given the topics and participation of high-level officials, a high level of media interest is anticipated.
- Security will prevent on-site media opportunities. Communications will balance the commitment to be transparent about national security issues with safety and security considerations.

Tactics

Before the event:

- Public Safety Canada is working on communications approach with domestic (Justice Canada and Immigration, Refugees and Citizenship Canada) and international partners (Australia, New Zealand, the United Kingdom and the United States).
- No communications activities are recommended in advance of the meeting. However, we may have to respond to media enquiries, if received.
- A welcoming news release from Ministers of Public Safety and Justice to inform Canadians that the meeting will be held in Ottawa could also be published on June 23.

During the event:

- Posts on twitter to inform Canadians that the meeting is being held in Ottawa. This will include a family photo for both events.

After the events:

- Policy communiqué will be issued in both English and French.
- A Canada-only news release will be issued June 27th after the conclusion of both meetings domestically to highlight cooperation and issues discussed at the Five Country Ministerial and the Quintet
- Posts on Twitter to promote the News Release
- A media availability by the Canadian Minister of Public Safety may be held at the end of the meetings (TBC)

Updated on June 14, 2017

Tab 15

**Pages 646 to / à 649
are withheld pursuant to sections
sont retenues en vertu des articles**

13(1)(a), 15(1) - Int'l

**of the Access to Information
de la Loi sur l'accès à l'information**

Tab 16

| FIVE COUNTRY MINISTERIAL AND JOINT MEETINGS | | |
|--|---|--|
| CONFERENCE DAY 1: June 26 (CSIS HQ, Ottawa) | | |
| FCM Plenary | | Ministerial Lead |
| 8:00 – 9:30 | SESSION 1: Intelligence Briefing / Counterterrorism (CAN) – Ministerial Introductions (CAN - ALL) – Threat briefing (CAN - Intelligence assessors) – Recent Attacks and Lessons Learned (UK) | GOODALE (CAN) TAB 3 CSIS |
| 9:30 – 10:45 | SESSION 2: Countering Violent Extremism (CAN) – Action plan (CAN) [REDACTED] (UK) / FTF (AUS) | GOODALE (CAN) TAB 4 |
| 10:45-11:00 | <i>Health break</i> | |
| 11:00 – 12:00 | SESSION 3: Refugees & Migration (UK) – Migration Flows/Global context (UK) – Refugees/Screening (CAN-AUS) – Border Technology (CAN) | RUDD (UK) TAB 5 |
| 12:15 – 13:30 | FCM Lunch – Served lunch for Ministers and Attorneys General in Director Boardroom <i>Discussion on Transparency/Accountability (CAN)</i> – Buffet-style lunch for other members of delegation in Lounge area | GOODALE (CAN) TAB 6 |
| FCM/QUINTET JOINT MEETING | | Ministerial Lead |
| 13:45-15:00 | SESSION 4: Security Cooperation & Law Enforcement (US) – Information Sharing: Terrorist Watchlist (US) & Criminal Information (UK) – Modern Slavery/Human Trafficking (UK) | KELLY (US) TAB 7 |
| 15:00 – 15:15 | <i>Health break – Family Photo</i> | |
| 15:15 – 16:30 | SESSION 5: Encryption & Cyber Security (AUS) – Encryption / Engaging with CSPs (AUS) – Cyber security / Response to Critical Cyber Incident (CAN) | BRANDIS (AUS) TAB 8 |
| 16:30 – 17:00 | Conclusion – Communique Agreement (ALL) – Closing Remarks (CAN) | GOODALE (CAN) TAB 9 TAB 10 |
| 17:00 – 18:30 | <i>Bilateral Meetings (CSIS HQ or Fairmont)</i> | |
| 19:30 – 22:00 | Reception and Dinner (Sir John A. Macdonald Building) | |

TAB 2

**Pages 653 to / à 660
are withheld pursuant to sections
sont retenues en vertu des articles**

69(1)(e), 69(1)(g) re (a)

**of the Access to Information
de la Loi sur l'accès à l'information**

TAB 3

**Pages 662 to / à 669
are withheld pursuant to sections
sont retenues en vertu des articles**

69(1)(e), 69(1)(g) re (a)

**of the Access to Information
de la Loi sur l'accès à l'information**

Today's News / Actualités
June 28, 2017 / le 28 juin 2017
8:00 – 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via [InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / CYBERSÉCURITÉ

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

Feds won't confirm possible terror threats targeting Canada Day celebrations

The federal government is trying to calm some fears about the security of Canada Day celebrations, after reports say ISIS has named our country and the United States as potential targets, following the Manchester bombing late last month. In an email statement, the **public safety minister's office** says it doesn't comment on specific threats but adds the government is unwavering in its commitment to protect Canadians and will continue to take appropriate action to counter terrorist threats. Recently RCMP Superintendent Mike O'Beirne also didn't directly answer when asked about any known threats for Canada Day. "Our assessment is continuous, both domestically and internationally and I can tell you constantly in contact with our partners in that regard." He adds officers are preparing for all possible security scenarios. "We've been monitoring all the external, internal pressures and we flex our

[BACK TO TOP / HAUT DE LA PAGE](#)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Five Eyes stress sharing information to battle 'relentless' terrorist plots

Security and justice officials from the Five Eyes alliance say they will explore more timely and detailed information sharing to detect terrorists and extremist fighters. In a joint communique issued today, the partners say Daesh and its affiliates will continue to attack soft targets in public spaces. Public security ministers and attorneys general from Canada, the United States, Britain, Australia and New Zealand gathered in Ottawa for two days of closed-door talks that wrapped up Tuesday. The sessions followed a rash of deadly attacks in Britain that highlighted the international alliance's concerns about the threat of homegrown extremism and the backlash it can provoke. In order to help prevent "sophisticated and relentless plots," the countries affirmed the importance of sharing information among partners on known criminal and terrorist actors. The joint message comes as officials in Ottawa step up security measures in anticipation of tens of thousands of people assembling on Parliament Hill to celebrate Canada's 150th birthday. [Canadian Press](#) (Globe and Mail)

Canada On Alert For ISIS Terrorist Attack This Weekend

As Canadians prepared to celebrate the 150th anniversary of confederation, security forces are poised to prevent any potential terrorist attack. A memo obtained by CTV News reveals that Canada — along with the United States — was named as a terrorist target by ISIS after the Manchester bombing in May. More than 500,000 celebrants are expected to converge on Parliament Hill this Saturday but security at the event will be "unprecedented," according to one source. Police will be fully armed and surveillance cameras are being put into place right now. There will be a barricade placed around the event in order to prevent any vehicles from entering the area. The memo indicates that ISIS has actually told Muslims to avoid markets and public gatherings in Canada because they plan to use "explosives, vehicles and beheadings to kill crusaders." "Given the current threat environment it is increasingly necessary for law enforcement officers to be aware of possible suspicious incidents that may be indicative of pre-attack planning," the memo continues. "The planning cycle of self-directed extremists is becoming increasingly shorter and subsequently more difficult to attack." Despite the memo and the grave warning, sources told CTV News that there is no intelligence report indicating that a specific target will be hit on Canada Day this weekend. In fact, the security threat levels has not been increased from medium, where it has stood since 2014. [Daily Caller](#)

Australia pushes ahead with plans to pressure tech firms on encryption

The Australian government has emerged from two days of talks with its Five Eyes intelligence partners confident in its plans to have technology firms decrypt communications for law enforcement purposes. The government met with representatives of the United States, UK, Canada, and New Zealand in Ottawa earlier this week to discuss how they could access encrypted messages used by criminals. Attorney-General George Brandis first revealed the government's intentions to chase end-to-end encrypted communications providers earlier this month, in response to terrorists' use of the technology. Australia has taken its lead from the UK, which proposed 'technology capability notices' following the Westminster terror attack, which would force communications operators to ensure they are technically able to hand over decrypted data to the government. At the time the Australian government insisted it was not trying to legislate backdoors for government in popular encrypted communications products like Signal and WhatsApp. But it is yet to detail how it expects operators - who don't hold the keys to decrypt user communications - to be able to break encryption, without weakening the security of their products. Today Brandis said the Five Eyes partners had broadly agreed at the Ottawa meeting that being able to decrypt communications used in criminal activities was "very important". He said the parties had concluded that "encryption can severely undermine public safety if it's by impeding lawful access to the content of communications during investigations into serious crimes during terrorism". But the countries had also decided to try and engage with internet service providers and technology companies to secure co-operation through an agreed set of protocols, rather than law changes, he said. He said these protocols would not amount to a specific request for implanted backdoors. [ITNews](#)

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Wednesday, June 28, 2017 1:31 PM
To: Today's News / Actualités (PS/SP)
Subject: CP: Five Eyes stress sharing information to battle 'relentless' terrorist plots

Five Eyes stress sharing information to battle 'relentless' terrorist plots

Canadian Press

Jim Bronskill

2017-06-28, 13:28 ET

OTTAWA - Security and justice officials from the Five Eyes countries plan to explore "more timely and detailed" information sharing to detect terrorists and extremist fighters.

Daesh and its affiliates will continue to attack soft targets in public spaces - underscoring a need for better data exchanges to address the threat, the partners said in a joint communique issued Wednesday.

Attorneys general and ministers for public security and immigration from Canada, the United States, Britain, Australia and New Zealand gathered in Ottawa this week for two days of closed-door talks.

"Throughout these discussions, we affirmed that building public trust within our countries is required to move forward on national security issues," the communique said. "Enhanced safeguards and greater efforts to promote transparency are critical in this respect."

The sessions followed a rash of deadly attacks in Britain that highlighted the international alliance's concerns about the threat of homegrown extremism and the backlash it can provoke.

The meetings also came as police in Ottawa busily stepped up security measures in anticipation of tens of thousands of people gathering Saturday on Parliament Hill to celebrate Canada's 150th birthday.

In order to help prevent "sophisticated and relentless plots," the five countries affirmed the importance of sharing information among partners on known criminal and terrorist actors, the communique said.

Security officials are worried about the widespread availability of encryption tools and applications that can allow extremists to more easily communicate without their phone calls and texts being intercepted.

Civil libertarians argue the right of law-abiding people to converse in private should not be compromised in the name of fighting terrorism by giving authorities the means to crack encryption or build back doors into security programs.

In a statement Sunday, Australian Attorney General George Brandis said his country planned to lead a discussion at the meetings on the terrorist use of cyberspace.

In its Wednesday communique, the alliance said the ability of terrorists and other criminals to shield their electronic activities through encryption can "severely undermine public safety efforts by impeding lawful access to the content of communications."

They agreed to a common approach to engaging with communication service providers to deal with online terrorist activities and propaganda, while "upholding cybersecurity and individual rights and freedoms."

The countries also committed to support a new industry forum led by Google, Facebook, Microsoft and Twitter.

In addition, they plan to:

_ Look at the role of traditional and social media and community voices in fostering - or discouraging - the radicalization of young people;

_ Share ideas on handling the threat posed by terrorist fighters who return from conflicts abroad;

_ Explore the possibility of joint operations to better tackle human trafficking and modern slavery.

Sent to: !INTERNAL; !INTERNAL 2; CSIS Breaking News; RCMP Breaking News

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Thursday, June 29, 2017 8:44 AM
To: Cyber Security / Sécurité cybernétique (PS/SP)
Subject: Cyber Security Media Summary / Revue de presse sur la cybersécurité - 2017-06-29

Cyber Security Media Summary / Revue de presse sur la cybersécurité June 29, 2017 / le 29 juin 2017

TOP STORIES / MANCHETTES

THREATS, VULNERABILITIES AND RESOLUTIONS / MENACES, VULNÉRABILITÉS ET SOLUTIONS

CYBER SURVEILLANCE AND ESPIONNAGE / CYBERSURVEILLANCE ET ESPIONNAGE

CYBER DEFENCE / CYBERDÉFENSE

RESEARCH AND DEVELOPMENT / RECHERCHE ET DÉVELOPPEMENT

OTHER / AUTRES

TOP STORIES / MANCHETTES

Five Eyes to engage with communications industry

Officials from five countries including Canada have agreed to "engagement" with communication-service providers on the use of encryption among terrorists and other criminals - which Canadian law enforcement and government agencies have described as an impediment to investigations. Security and justice officials from Canada, the United States, Britain, Australia and New Zealand - known as the Five Eyes - gathered in Ottawa this week to discuss national-security challenges, including the use of encryption applications such as WhatsApp and Signal by extremists to hide their electronic communications. (...) The Five Eyes did not expand on what it means by "engagement" and what possible shared solutions would be. The alliance is looking at whether security agencies should be able to lawfully access encrypted communications during investigations into serious crimes. Companies in Five Eyes countries are not required by law to hold decryption "keys" that unscramble encrypted communications, such as text messages, and when they do not, it's impossible for them to provide government or law-enforcement agencies with data. For instance, the RCMP were unable to read Islamic State supporter Aaron Driver's encrypted messages with two well-known members of the terrorist group; Mr. Driver was shot dead during a raid led by the Mounties in August, 2016. While Public Safety Minister Ralph Goodale has acknowledged the significant obstacles encryption presents for Canadian law enforcement and national-security agencies, he said the technology is essential for the growth of Canada's digital economy and the safeguarding of cyberssecurity and online privacy. [The Globe and Mail](#), A3

"Dynamic" cyber defence systems to protect Canadian government against latest attacks, says CSE chief

A new cyber attack, which originally was aimed at computers in Ukraine, has spread to systems around the world. The New York Times reports that the attack has hit firms around the globe, "from Maersk, the Danish shipping conglomerate, to Merck, the drug giant in the United States." Greta Bossenmaier, Chief of Canada's Communications Security Establishment has issued this statement in response to the attacks: CSE continues to closely monitor the recent global cyber/ransomware attacks. As we have seen in recent attacks, today's attacks continue to indiscriminately target both organizations and individuals. Our dynamic cyber defence security systems remain ready to defend Government of Canada systems and help protect against future types of similar attacks. Working with Shared Services Canada and our other partners, Government of Canada networks continue to be well placed to defend against these types of attacks. Thanks to this work, there is no indication at this time that Government of Canada systems were negatively impacted, and that any information, personal or otherwise, was compromised. As the situation continues to develop, we remain in close contact with our domestic and international partners to address any developments. In addition, we will ensure all relevant information and guidance that is available to CSE is provided to our partners at Public Safety Canada to relay to the private sector. [Postmedia](#) (Ottawa Citizen)

NATO decides cyber attacks could trigger collective defence clause

Article 5 of the North Atlantic Treaty which states an attack on one NATO member is considered an attack on all, is being extended into the realm of cyber warfare. Speaking to journalists on Wednesday, NATO Secretary General Jens Stoltenberg said the collective defence articles could be invoked in the face of a cyber attack. "We have also decided that a cyber attack can trigger Article 5 and we have also decided -- and we are in the process of establishing -- cyber as a military domain, meaning that we will have land, air, sea, and cyber as military domains," he said. "All of this highlights the advantage of being an alliance of 29 allies because we can work together, strengthen each other, and learn from each other." [ZD Net](#); [Infosecurity Magazine](#)

Hacks Raise Fear Over N.S.A.'s Hold on Cyberweapons

Twice in the past month, National Security Agency cyberweapons stolen from its arsenal have been turned against two very different partners of the United States — Britain and Ukraine. The N.S.A. has kept quiet, not acknowledging its role in developing the weapons. White House officials have deflected many questions, and responded to others by arguing that the focus should be on the attackers themselves, not the manufacturer of their weapons. But the silence is wearing thin for victims of the assaults, as a series of escalating attacks using N.S.A. cyberweapons have hit hospitals, a nuclear site and American businesses. Now there is growing concern that United States intelligence agencies have rushed to create digital weapons that they cannot keep safe from adversaries or disable once they fall into the wrong hands. On Wednesday, the calls for the agency to address its role in the latest attacks grew louder, as victims and technology companies cried foul. Representative Ted Lieu, a California Democrat and a former Air Force officer who serves on the House Judiciary and Foreign Affairs Committees, urged the N.S.A. to help stop the attacks and to stop hoarding knowledge of the computer vulnerabilities upon which these weapons rely. [New York Times](#)

[BACK TO TOP / HAUT DE LA PAGE](#)

THREATS, VULNERABILITIES AND RESOLUTIONS / MENACES, VULNÉRABILITÉS ET SOLUTIONS

Microsoft Releases Feature That Makes Windows 10 Immune to WannaCry, Petya

Windows has been hit twice by ransomware infections in the last couple of months, and thousands of computers ended up compromised after owners failed to properly protect data. While Microsoft has indeed released Windows updates to block these infections, most of the systems that got infected weren't actually running the latest patches, so it was very clear that the company needed to develop a solution that would keep users secure even when zero-day updates are not available. Enter Controlled folder access. This is a new feature that Microsoft is testing right now with help from insiders that is supposed to keep an eye on critical folders and alert users whenever a specific app attempts to make unauthorized notifications... With Windows folders protected by default, Controlled folder access can keep an eye on any folder on your system, and even on network shares and mapped drives, thus ensuring that if ransomware reaches your computer, it cannot make any modifications that would eventually lock down the PC. [Softpedia](#)

Surprise! NotPetya Is a Cyber-Weapon. It's Not Ransomware

The NotPetya ransomware that encrypted and locked thousands of computers across the globe yesterday and today is, in reality, a disk wiper meant to sabotage and destroy computers, and not ransomware. This is the conclusion of two separate reports coming from Comae Technologies and Kaspersky Lab experts. Experts say that NotPetya — also known as Petya, Petna, ExPetr — operates like a ransomware, but clues hidden in its source code reveal that users will never be able to recover their files. This has nothing to do with the fact that a German email provider has shut down the NotPetya operator's email account. Even if victims would be able to get in contact with the NotPetya author, they still have no chance of recovering their files. [Bleeping Computer](#); [ZD Net](#); [Threat Post](#)

Shadow Brokers Threaten to Expose Identity of Former NSA Hacker

The Shadow Brokers have published a new message today, gloating about the damage caused by the NotPetya ransomware, and threatening to expose the real-life identity of an alleged NSA employee, who they say has been mocking the group on Twitter. In their message, the group also boasted about have "many many subscribers" to their monthly data dump service, which they started earlier this month. [Bleeping Computer](#); [Security Affairs](#)

As firms gauge cost, malware under control

The data-scrambling software epidemic that paralyzed computers globally is under control in Ukraine, where it likely originated, officials said Wednesday, as companies and governments around the world counted the cost of a crisis that is disrupting ports, hospitals and factories. In a statement published Wednesday, the Ukrainian Cabinet said that "all strategic assets, including those involved in protecting state security, are working normally." The same couldn't be said for India's largest container port, where one of the terminals was idled by the malicious software, which goes by a variety of names including ExPetr. [Associated Press](#) (Chronicle Herald, B6; London Free Press; Whig Standard; Toronto Sun;

Winnipeg Sun; Ottawa Sun; Edmonton Sun; National Post; Montreal Gazette; Times-Colonist; Windsor Star; Vancouver Sun; Calgary Herald; Star Phoenix; Edmonton Journal; Leader-Post; Chronicle-Journal; Daily Courier; Whitehorse Star); BBC News

Cyberattack: Shipping giant's terminals slowly recovering

Danish shipping giant A.P. Moller-Maersk, one of the global companies hardest hit by a malicious software that froze computers around the globe, said Thursday that most of its terminals are now operational, though some remain crippled. The Copenhagen-based company said that some terminals are "operating slower than usual or with limited functionality." Problems have been reported across the shippers' global business, from Mobile, Alabama, to Mumbai in India. The shipping company is one of a number of major corporations and government agencies — from logistics firm FedEx to Ukraine's banking system — to have been hit by the software epidemic... As companies and governments gauged the cost of the attack, experts were trying to shed light on who launched it and why. The attack has the telltale signs of ransomware, which scrambles a computer's data until a payment is made. But some analysts believe this attack was less aimed at gathering money than at sending a message to Ukraine, where it seems to have originated, and its allies. That hunch was buttressed by the way the malware appears to have been seeded using a rogue update to a piece of Ukrainian accounting software — suggesting an attacker focused on Ukrainian targets. And it comes on the anniversary of the assassination of a senior Ukrainian military intelligence officer and a day before a national holiday celebrating a new constitution signed after the breakup of the Soviet Union. Associated Press (Financial Post; ABC News; Seattle Times); ABC News

Cyberattack: Was it really ransomware, or an attack on Ukraine - or something yet to come?

A day after the latest cyberattack crippled computers internationally, starting in Ukraine, expert opinions vary widely over who was behind it and what the real goal was. On Tuesday morning in Kyiv, Ukraine, a sudden blast brought traffic to a halt near the city's main railway station. When the dust settled, a mangled Mercedes Benz sat smoking in the street. Dead inside the car was a colonel who worked with the country's special operations forces. As Ukrainian officials and news media began to process the grisly execution, the country was overwhelmed by a massive cyberattack. The hackers behind it brought down a range of infrastructure and companies throughout Ukraine... The country's intelligence service, the SBU, almost immediately attributed the cyberattack to the Kremlin. Robert M. Lee, the founder and chief executive of the industrial cybersecurity company Dragos, Inc., however, tells CBC News that the statement was wrong. A world-renowned expert in the cybersecurity of critical infrastructure, Lee said he understands why Ukrainian officials would be quick to blame Russia. Attacks against Ukraine's power grid in 2015 and 2016 were widely attributed to Russia by cybersecurity experts. "Ukraine is understandably hyper-sensitive to the conflict, and there's many there that rightfully feel no one else is taking the attacks against Ukraine seriously," said Lee. The early analysis seemed to indicate that the hack was a relatively straightforward ransomware campaign that started in Ukraine and spread globally. CBC News

Latest cyberattack 'more sophisticated' and spreading, says Europol

The second cyberattack in as many months that struck systems around the world was more sophisticated than the first one and is still spreading, Europol has said. It says companies and governments are being targeted by an updated version of a known virus. Tuesday's attack, believed to have started in Ukraine, brought disruption to major organisations including the Chernobyl radiation monitoring system, European bank BNP Paribas, advertising firm WPP and parts of the Ukrainian government computer system. The Danish owner of the world's largest container shipper Maersk Line said its computer systems were also affected, causing problems with processing orders and delaying cargoes. It came just weeks after the NHS was crippled by a cyberattack. Europol, which helps EU member states fight international crime, said the attack is still ongoing and it is monitoring the spread of the virus. Sky News

Cyberattaque: des milliers d'ordinateurs infectés dans le monde

La cyberattaque mondiale au rançongiciel (ransomware), démarrée en Ukraine et en Russie, semblait contenue mercredi après avoir touché des milliers d'ordinateurs et a rappelé, un mois et demi après WannaCry, la vulnérabilité d'infrastructures critiques. Si l'ampleur des dégâts paraît minime par rapport aux centaines de milliers de victimes de WannaCry début mai, le virus, qui bloque des ordinateurs jusqu'au paiement d'une rançon de 300 \$ en monnaie virtuelle, a affecté les contrôles sur le site de l'accident nucléaire de Tchernobyl, le port de Bombay et des bureaux de multinationales dans le monde entier. Plus de 2000 utilisateurs ont été concernés, essentiellement en Ukraine et en Russie, selon Kaspersky Labs. Ce spécialiste de la sécurité informatique basé en Russie avait auparavant estimé que ce rançongiciel n'était pas une nouvelle version du virus Petya, pourtant désigné par de nombreux autres spécialistes et déjà à l'oeuvre l'année dernière. « Cela semble être une attaque complexe, qui utilise plusieurs vecteurs afin de se propager au moins au sein des réseaux des entreprises visées », a détaillé la société. Le Devoir; Radio-Canada; CTV News

The Latest Ransomware Took Advantage of a Devilishly Clever Trick

Usually, ransomware may be spread via emails or websites. But at least some victims of this latest wave were infected by a software update, according to researchers and law enforcement. Tuesday's global ransomware outbreak may be notable for its size, but there is a second aspect that sets it apart from other attacks: the way in which at least some

victims appear to have been infected. Typically, ransomware may be distributed through spam emails, or dodgy adverts on websites. In this case, some victims were impacted because of a booby-trapped software update from a Ukrainian financial software company, according to researchers and law enforcement. This episode doesn't only showcase a novel attack approach, it also highlights the power that software updates can have over the security of a system more generally. In a blog post published on Tuesday, Microsoft said it had evidence that "a few active infections of the ransomware initially started from the legitimate MEDoc updater process." MEDoc is a company that provides accounting software, such as tools that simplify filing your taxes. [Motherboard](#)

Internet Radio Service 8tracks Hacked, 18 Million Accounts Stolen

Internet radio service 8tracks was hacked earlier this week, and attackers managed to extract no less than 18 million accounts, including usernames, hashed passwords, and email addresses. In a message posted on the company's blog, 8tracks confirms the hack, and says that it all started from an employee's Github account that was not using two-factor authentication. IT admins became aware of the hack once the attackers attempted to change the password of the Github account, they say. 8tracks explains that only users who signed up with email are affected by the hack, while everyone else, including those who are using Google and Facebook accounts to log in, are completely secure. [Softpedia](#)

Vault 7: CIA Malware for Tracking Windows Devices via WiFi Networks

Today, WikiLeaks has published the documentation manual for an alleged CIA tool that can track users of WiFi-capable Windows devices based on the ESS (Extended Service Set) data of nearby WiFi networks. According to the tool's 42-page manual, the tool's name is ELSA. The manual includes the following image to explain to CIA operatives how the tool works. A summary of an ELSA operation is included below the image. [Bleeping Computer](#); [Security Affairs](#)

Linux's systemd vulnerable to DNS server attack

Security experts are warning of a bug that could allow hackers to craft TCP packets that fool Linux's initialization daemon systemd, which could cause systems to crash or make them run malicious code. [ZD Net](#); [Security Affairs](#)

[BACK TO TOP / HAUT DE LA PAGE](#)

CYBER SURVEILLANCE AND ESPIONNAGE / CYBERSURVEILLANCE ET ESPIONNAGE

Australia pushes ahead with plans to pressure tech firms on encryption

The Australian government has emerged from two days of talks with its Five Eyes intelligence partners confident in its plans to have technology firms decrypt communications for law enforcement purposes. The government met with representatives of the United States, UK, Canada, and New Zealand in Ottawa earlier this week to discuss how they could access encrypted messages used by criminals. Attorney-General George Brandis first revealed the government's intentions to chase end-to-end encrypted communications providers earlier this month, in response to terrorists' use of the technology. Australia has taken its lead from the UK, which proposed 'technology capability notices' following the Westminster terror attack, which would force communications operators to ensure they are technically able to hand over decrypted data to the government. At the time the Australian government insisted it was not trying to legislate backdoors for government in popular encrypted communications products like Signal and WhatsApp. But it is yet to detail how it expects operators - who don't hold the keys to decrypt user communications - to be able to break encryption, without weakening the security of their products. Today Brandis said the Five Eyes partners had broadly agreed at the Ottawa meeting that being able to decrypt communications used in criminal activities was "very important". He said the parties had concluded that "encryption can severely undermine public safety if it's by impeding lawful access to the content of communications during investigations into serious crimes during terrorism". But the countries had also decided to try and engage with internet service providers and technology companies to secure co-operation through an agreed set of protocols, rather than law changes, he said. He said these protocols would not amount to a specific request for implanted backdoors. [ITNews](#)

Senate Gets Ready to Ban Kaspersky Products as FBI Interviews Company's US Employees

A draft of the "National Defense Authorization Act for Fiscal Year 2018" — which approves the budget and policies for US defensive projects — outlines a ban on the usage of Kaspersky Lab software products at DOD facilities under the explanation that the Russian antivirus vendor "might be vulnerable to Russian government influence." "[The Committee] prohibits the DOD from using software platforms developed by Kaspersky Lab due to reports that the Moscow-based company might be vulnerable to Russian government influence," the proposed bill reads [page 12], first spotted by Reuters last night. [Bleeping Computer](#)

Russia doesn't rule out retaliation if U.S. bans Kaspersky products

Russia does not rule out retaliatory measures if the United States bans Moscow-based cyber security firm Kaspersky Lab's products, RIA news agency cited Russia's Communications Minister Nikolai Nikiforov as saying on Thursday. On

Wednesday U.S. senators sought to ban Kaspersky Lab's products from use by the military because of fears the company is vulnerable to "Russian government influence". [Reuters](#)

[BACK TO TOP / HAUT DE LA PAGE](#)

CYBER DEFENCE / CYBERDÉFENSE

Cisco launches IoT Threat Defense

Cisco has launched its Internet of Things (IoT) Threat Defense solution in an effort to mitigate and solve common security issues threatening the deployment and operation of IoT devices. According to Cisco Product Marketing Industry Solutions manager Marc Blackmer, many vendors and companies don't see IoT devices as security threats, with Cisco additionally having to combat the stripping out of security mechanisms from IoT devices in order to keep them low cost to ensure profitability. "These devices are new to security, meaning the vendors are new in a lot of cases, so what happens is they tend to think, 'Why would anyone attack this?'," Blackmer explained during Cisco Live Las Vegas. "For us on the security side, we see them as avenues into the network. So whether it's propagating malware, or whether it's a targeted attack, they're just not dealing with it." Announced in March and launched at Cisco Live this week, the IoT Threat Defense suite includes network segmentation through Cisco TrustSec; cloud security using Cisco Umbrella; malware protection via Cisco AMP; a firewall using Cisco's Firepower NGFW; network behaviour analytics through Cisco Stealthwatch; device visibility through Cisco ISE; and remote access through Cisco AnyConnect. [ZD Net](#)

[BACK TO TOP / HAUT DE LA PAGE](#)

RESEARCH AND DEVELOPMENT / RECHERCHE ET DÉVELOPPEMENT

It's Too Late to Stop China From Becoming an AI Superpower

Last Thursday, Texas senior senator John Cornyn stood before an audience of wonks at the Council for Foreign Relations in Washington, DC, and warned that America's openness to investors looking for new ideas in technologies like artificial intelligence was putting it in danger. "Most of what China wants to invest in these days is leading-edge US technology that's a key to our future military capabilities," he said. "Unless the trend line changes, we may one day see some of these technologies incorporated in China-made equipment that can be used against our country in the event, heaven forbid, of a military conflict." Cornyn highlighted China's interest in robotics and artificial intelligence as particularly concerning. His warning—and pledge to introduce legislation that could restrict Chinese investment in technology companies—came the week after Reuters reported, citing unidentified Trump administration officials, that the administration is considering a similar policy, also motivated in part by fears of China gaining access to valuable AI knowledge. However, Cornyn's diagnosis and proposed cure could lead to a result opposite to the intended one. America's military does need to harness machine learning and artificial intelligence to keep up with China and other nations. But restricting China from investing in US technology probably wouldn't make much of a dent in the country's progress—and could make America less competitive. [Wired](#)

How artificial intelligence is taking on ransomware

Twice in the space of six weeks, the world has suffered major attacks of ransomware - malicious software that locks up photos and other files stored on your computer, then demands money to release them. It's clear that the world needs better defences, and fortunately those are starting to emerge, if slowly and in patchwork fashion. When they arrive, we may have artificial intelligence to thank. [Telegram](#), B11

Seek the cloud to avoid a cyberattack: Malware hack heightens global awareness

Malware has yet again disrupted businesses around the world, just weeks after hackers used leaked National Security Administration tools in a global cyberattack called WannaCry. The ultimate target in both cases may be people's sensitive information - a troubling reality that should finally motivate organizations to get serious about security. Tuesday's attack, which continued to spread around the world Wednesday, was more sophisticated than WannaCry, which took advantage of a Windows exploit to infect more than 200,000 computers in 150 countries (and which cost, by one estimate, more than US\$4 billion)... It's worth noting that cloud computing services like Google and Amazon, which control vast amounts of data around the world, have yet to be crippled by a ransomware attack or even suffer a known data breach. Google in particular prevents break-ins across a global workforce by implementing a strict provisioning system, in which every device is presumed to be untrustworthy. [Postmedia](#) (National Post; Ottawa Citizen; Calgary Herald)

[BACK TO TOP / HAUT DE LA PAGE](#)

OTHER / AUTRES

Un premier bac offert en cybersécurité : Polytechnique Montréal s'adapte à la demande croissante pour une formation spécialisée

Alors que les cyberattaques se font plus fréquentes ces dernières années, touchant de nombreuses personnes et sociétés à travers le monde, il devient urgent de former davantage de spécialistes en cybersécurité, estiment des experts. Un baccalauréat dans le domaine fera ainsi son apparition à l'école Polytechnique de Montréal dès cet automne. Intrusion, piratage, usurpation d'identité virtuelle, virus, cheval de Troie : les réseaux informatiques sont la cible de multiples attaques, et la tendance est à la hausse, croit Gervais Ouellet, responsable du programme. La nouvelle vague de cyberattaques qui a paralysé les systèmes informatiques de plusieurs entreprises à travers le monde mardi, en exigeant le paiement d'une rançon, ne peut qu'appuyer son propos. Déjà dotée de trois certificats reliés à la thématique (cyberenquête, cyberfraude et cybersécurité des réseaux informatiques), Polytechnique proposera désormais une formation plus complète à ses étudiants. Ce nouveau diplôme, le seul offert au premier cycle au Québec, pourra être obtenu en cumulant les certificats déjà existants. Les étudiants pourront autrement combiner deux d'entre eux avec le certificat en analyse de la sécurité de l'information et des systèmes à HEC, ou encore ceux en informatique appliquée ou en criminologie de l'Université de Montréal. Devoir, A1/A8

[BACK TO TOP / HAUT DE LA PAGE](#)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille de la sécurité publique. We can be reached at / Vous pouvez communiquer avec nous à l'adresse : PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Sent to: !Cyber Security Media Summary Dist List #1; !Cyber Security Media Summary Dist List #2; !Cyber Security Media Summary Dist List #3; !Cyber Security Media Summary Dist List #4

Daily Media Summary / Revue de presse quotidienne
Canadian Security Intelligence Service / Service canadien du renseignement de sécurité
June 29, 2017 / le 29 juin 2017

CSIS IN THE NEWS / LE SCRS DANS LES NOUVELLES

MINISTER / MINISTRE

SECURITY AND LAW ENFORCEMENT / SÉCURITÉ ET EXÉCUTION DE LA LOI

BORDER ISSUES / ENJEUX FRONTALIERS

CYBER AND TECHNOLOGY / CYBER ET TECHNOLOGIE

MILITARY ISSUES / ENJEUX MILITAIRES

PUBLIC SERVICE / FONCTION PUBLIQUE

LEGISLATION AND POLICIES / LÉGISLATION ET POLITIQUES

OTHER / AUTRES

INTERNATIONAL / INTERNATIONAL

CSIS IN THE NEWS / LE SCRS DANS LES NOUVELLES

The Hostage crisis

It began with what seemed like any other tip called in to the Toronto Star's 24-hour news desk. But the man on the line - his voice steady, at times upset but never once raised - would soon reveal he had made a desperate move. He was "at a breaking point." He needed to be listened to. This is what it would take, he said (...) What unfolded beginning at around 9:30 a.m. Wednesday was a daylight hostage-taking in an Eglinton West massage parlour tucked into an industrial area strip mall. Heavily armed members of Toronto police's Emergency Task Force soon descended on the area (...) Michael Storms, 35, was charged Wednesday with forcible confinement and uttering threats. The man on the phone had told the Star he had converted to Islam when he was 20, and also went by the name Muhammed Islam. The caller said his motivations for the kidnapping were related to years of being surveilled and monitored by the RCMP, and that he was desperate for it to stop. The RCMP did not return a request for comment to the Star by press time (...) On the phone, Michael instructs Cudmore to tell police not to approach. Cudmore attempts to keep the caller calm, reminding him that he's going to help. Cudmore invites Michael to tell him more about "what's going on that's making you feel this way." "It's the police. It's CSIS. OK?" Michael alleged that RCMP surveillance had resulted in him losing his job and not being able to get an apartment. He claims he has been on the national security watchlist for 15 years, being followed and monitored. "I need people to know that I've been targeted because I'm Muslim, right ... They want to tell me that I'm a terrorist, or potential terrorist. I don't support terrorism or any of that stuff," Michael says. Toronto Star, A1 (Wendy Gillis, Victoria Gibson, Ainslie Cruickshank & Alex Mckeen)

How the phone conversation unfolded

When the call came in to the Star newsroom Wednesday morning, reporter Fakiha Baig answered. Here's how the conversation played out. The transcript has been edited for space and privacy considerations. Michael: I've needed help for a long time, OK? And nobody will listen. The only way to do this is to create a situation. A crisis, OK? Which is what I'm doing. So I took a hostage. Are you listening

Union, public safety minister push for action at 'toxic' Edmonton prison

Canada's public safety minister has ordered the federal corrections service to prepare a report on what it's doing to prevent harassment by and of employees - a move that comes as one union is lambasting the response to high-profile harassment issues at Edmonton's maximum-security prison. In an email to CBC News, a spokesperson for Ralph Goodale said that his office wrote directly to the commissioner of the Correctional Service of Canada (CSC) to make the request. "Minister Goodale asked Commissioner [Don] Head to prepare a report on the actions CSC has taken to date to ensure its workplace is free from harassment and sexual violence, its plans moving forward and what challenges it faces in driving progress," Scott Bardsley wrote. It comes after CBC News uncovered explosive allegations that lengthy and sexually explicit conversations on work phones were allegedly the reason why prison guards at the Edmonton Institution missed several calls for help from inmates. Goodale had ordered the comprehensive harassment report from the CSC commissioner this past spring, making the same request to Canada Border Services Agency, the Parole Board of Canada, the RCMP and CSIS. He has asked that those reports be completed by the end of the year. [CBC News](#) (Marion Warnica)

Investissements étrangers: une complaisance préoccupante

Un éditorial note, « Pour la seconde fois en trois mois, le gouvernement Trudeau permet à une entreprise chinoise d'acquérir une entreprise de haute technologie canadienne produisant du matériel militaire. Et dans ce dernier cas, la décision a été prise sans même procéder à un examen en profondeur des risques potentiels pour la sécurité nationale. Cette affaire crée des remous aux Communes et ailleurs depuis que le Globe and Mail a révélé au début du mois de juin que la firme chinoise Hytera Communications prendrait le contrôle de Norsat, une entreprise de Vancouver spécialisée dans la haute technologie de communication pour, entre autres, les satellites et les réseaux sans fil civils et militaires. Cette compagnie compte parmi ses clients l'OTAN et l'armée américaine. Deux anciens patrons du Service canadien du renseignement de sécurité ont dit qu'un examen approfondi de cette transaction s'imposait. Au Congrès américain, on manifeste de fortes inquiétudes. Le Globe écrivait mardi, pour des raisons de sécurité, le département américain de la Défense allait revoir tous ses liens d'affaires avec Norsat. Cela n'a pas ébranlé le premier ministre Justin Trudeau, qui, en conférence de presse le même jour, s'est dit à l'aise avec cette transaction. Il a déclaré que jamais son gouvernement n'approuverait une prise de contrôle comportant des risques pour la sécurité nationale. Il a poursuivi en notant que lors du processus d'examen des investissements étrangers, les « agences de sécurité examinent la transaction, la technologie, les joueurs en présence. Elles consultent nos alliés, y compris les États-Unis, et déterminent s'il faut pousser l'examen plus loin ou non ». Et cela n'aurait pas été jugé nécessaire dans ce cas-ci, dit-il. Voilà qui surprend. Les entreprises chinoises, même celles dites privées, collaborent avec le gouvernement chinois qui, à travers ces acquisitions, a accès à des technologies très prisées. M. Trudeau se veut rassurant, mais on garde l'impression qu'il est surtout prêt à bien des contorsions pour charmer la Chine, avec qui il rêve de conclure un accord de libre-échange. » [Le Devoir](#)

[BACK TO TOP / HAUT DE LA PAGE](#)

MINISTER / MINISTRE

Five Eyes agree to engage with industry on terrorists' use of encryption

Officials from five countries including Canada have agreed to "engagement" with communication-service providers on the use of encryption among terrorists and other criminals - which Canadian law enforcement and government agencies have described as an impediment to investigations. Security and justice officials from Canada, the United States, Britain, Australia and New Zealand - known as the Five Eyes - gathered in Ottawa this week to discuss national-security challenges, including the use of encryption applications such as WhatsApp and Signal by extremists to hide their electronic communications. "Ministers and Attorneys-General also noted that encryption can severely undermine public safety efforts by impeding lawful access to the content of communications during investigations into serious crimes, including terrorism. To address these issues, we committed to develop our engagement with communications and technology companies to explore shared solutions while upholding cybersecurity and individual rights and freedoms," read a joint communiqué released by the Five Eyes on Wednesday. The Five Eyes did not expand on what it means by "engagement" and what possible shared

solutions would be. The alliance is looking at whether security agencies should be able to lawfully access encrypted communications during investigations into serious crimes. Companies in Five Eyes countries are not required by law to hold decryption "keys" that unscramble encrypted communications, such as text messages, and when they do not, it's impossible for them to provide government or law-enforcement agencies with data. For instance, the RCMP were unable to read Islamic State supporter Aaron Driver's encrypted messages with two well-known members of the terrorist group; Mr. Driver was shot dead during a raid led by the Mounties in August, 2016. While Public Safety Minister Ralph Goodale has acknowledged the significant obstacles encryption presents for Canadian law enforcement and national-security agencies, he said the technology is essential for the growth of Canada's digital economy and the safeguarding of cybersecurity and online privacy. On the other hand, British Prime Minister Theresa May and French President Emmanuel Macron recently called for greater access to encrypted communications as a part of their counterterrorism joint action plan. The plan was announced June 13, after a string of terrorist attacks in Britain and France. [Globe and Mail](#) (Michelle Zilio) (2017-06-28)

Feds won't confirm possible terror threats targeting Canada Day celebrations

The federal government is trying to calm some fears about the security of Canada Day celebrations, after reports say ISIS has named our country and the United States as potential targets, following the Manchester bombing late last month. In an email statement, the public safety minister's office says it doesn't comment on specific threats but adds the government is unwavering in its commitment to protect Canadians and will continue to take appropriate action to counter terrorist threats. Recently RCMP Superintendent Mike O'Beirne also didn't directly answer when asked about any known threats for Canada Day. "Our assessment is continuous, both domestically and internationally and I can tell you constantly in contact with our partners in that regard." He adds officers are preparing for all possible security scenarios. "We've been monitoring all the external, internal pressures and we flex our contingency plans in regards to that." There are reports the threat was not made about Canada Day celebrations specifically, but it urges Muslims to avoid public gatherings and threatened to use "explosives, vehicles, [and] beheadings to kill crusaders." However, police in Ottawa and Mounties have said there will be heightened security measures and it will be all hands on deck for the celebration in the nation's capital, which is expecting a crowd of about half a million people. The public safety minister's office stresses police will be involved in celebrations across the country and it's urging Canadians to be vigilant, and stay up to date with the latest security requirements. The terror threat in Canada remains at medium. [News 1130](#) (Cormac MacSweeney) (2017-06-28)

RCMP's Michaud outlines changes he'd like to see after Paulson's retirement

Gilles Michaud knows what he'd like to do with the Royal Canadian Mounted Police. The police officer charged with pursuing the country's most serious criminals has a clear vision of where he'd like to take the force - or, at least, the 4,700 or so uniformed officers he oversees as its deputy commissioner of federal policing. Deputy Commissioner Michaud says he wants to open up new fronts to better tackle growing criminal challenges such as outlaw bikers, criminal hackers, fentanyl smugglers and money launderers. But to do that, he says, he needs people who are not like him. Decades of staffing Canada's federal police force with career Mounties have filled the ranks with generalists who can bring broad policing skills to a range of files, he said in a frank interview with [The Globe and Mail](#). But in an era of increasingly complex and sophisticated crime, the one-time drug cop says that the force lacks much-needed specialists - people with deep investigative skills and expertise who can dig into complicated issues. "Do you need to be a gun-carrying police officer to do financial-crime investigations? Do you need to be a gun-carrying officer to do cybercrime investigations?" Deputy Commissioner Michaud asked rhetorically, suggesting that what the RCMP needs most right now may be accountants, computer programmers and professional managers. "We have lost some of our expertise," he said. (...) There's only one problem with Deputy Commissioner Michaud's vision: He isn't the person who can sign off on big-picture changes at the RCMP. Those decisions rest in the hands of the force's commissioner, a position that's now in transition. With the June 30 retirement of the current Commissioner, Bob Paulson, the RCMP now stands at a crossroads. It's anticipated that the minister in charge of the Mounties, Public Safety Minister Ralph Goodale, will announce that he has hired a former premier and ambassador, Frank McKenna, to put together a panel to recommend a new leader. In a recent radio interview, he hinted that the appointment could shake up the force. "The change in command is an opportunity to examine all dimensions of governance and structure," Mr. Goodale said. [The Globe and Mail](#), A8

BORDER ISSUES / ENJEUX FRONTALIERS

Far-right Soldiers of Odin members 'not afraid to use violence,' intelligence report warns

The emergence of the far-right Soldiers of Odin group in Canada has raised concerns about the potential for "anti-immigrant vigilantism," according to a de-classified intelligence report obtained by Global News. The Canada Border Services Agency Intelligence Bulletin cautioned that the Soldiers of Odin-Canada, or SOO, was "gaining popularity," "rapidly expanding" and "setting up chapters in many provinces." (...) "The group's nature has raised concerns of anti-immigration vigilantism," said the "Protected" report, which was written by the CBSA's Intelligence Analysis Unit in the Prairie Region, where several SOO chapters were based. (...) The intelligence report did not explain why the CBSA had taken an interest in the group. Such bulletins are typically distributed to border officials to alert them to emerging immigration enforcement issues. [Global News](#) (2017-06-28)

[BACK TO TOP / HAUT DE LA PAGE](#)

CYBER AND TECHNOLOGY / CYBER ET TECHNOLOGIE

"Dynamic" cyber defence systems to protect Canadian government against latest attacks, says CSE chief

A new cyber attack, which originally was aimed at computers in Ukraine, has spread to systems around the world. The New York Times reports that the attack has hit firms around the globe, "from Maersk, the Danish shipping conglomerate, to Merck, the drug giant in the United States." Greta Bossenmaier, Chief of Canada's Communications Security Establishment has issued this statement in response to the attacks: CSE continues to closely monitor the recent global cyber/ransomware attacks. As we have seen in recent attacks, today's attacks continue to indiscriminately target both organizations and individuals. Our dynamic cyber defence security systems remain ready to defend Government of Canada systems and help protect against future types of similar attacks. Working with Shared Services Canada and our other partners, Government of Canada networks continue to be well placed to defend against these types of attacks. Thanks to this work, there is no indication at this time that Government of Canada systems were negatively impacted, and that any information, personal or otherwise, was compromised. As the situation continues to develop, we remain in close contact with our domestic and international partners to address any developments. In addition, we will ensure all relevant information and guidance that is available to CSE is provided to our partners at Public Safety Canada to relay to the private sector. [Postmedia](#) (Ottawa Citizen) (2017-06-28)

Australia pushes ahead with plans to pressure tech firms on encryption

The Australian government has emerged from two days of talks with its Five Eyes intelligence partners confident in its plans to have technology firms decrypt communications for law enforcement purposes. The government met with representatives of the United States, UK, Canada, and New Zealand in Ottawa earlier this week to discuss how they could access encrypted messages used by criminals. Attorney-General George Brandis first revealed the government's intentions to chase end-to-end encrypted communications providers earlier this month, in response to terrorists' use of the technology. Australia has taken its lead from the UK, which proposed 'technology capability notices' following the Westminster terror attack, which would force communications operators to ensure they are technically able to hand over decrypted data to the government. At the time the Australian government insisted it was not trying to legislate backdoors for government in popular encrypted communications products like Signal and WhatsApp. But it is yet to detail how it expects operators - who don't hold the keys to decrypt user communications - to be able to break encryption, without weakening the security of their products. Today Brandis said the Five Eyes partners had broadly agreed at the Ottawa meeting that being able to decrypt communications used in criminal activities was "very important". He said the parties had concluded that "encryption can severely undermine public safety if it's by impeding lawful access to the content of communications during investigations into serious crimes during terrorism". But the countries had also decided to try and engage with internet service providers and technology companies to

secure co-operation through an agreed set of protocols, rather than law changes, he said. He said these protocols would not amount to a specific request for implanted backdoors. [ITNews](#) (2017-06-28)

Encryption cracking campaign receives lacklustre support from Five Eyes

Five Eyes nations' ministers and attorney-generals have "committed to develop our engagement with communications and technology companies to explore shared solutions" around the encrypted content of communications sent by criminals. This will be done while "upholding cybersecurity and individual rights and freedoms" a joint communique issued following two days of talks in Ottawa, Canada noted. Despite being a key topic for the Australian government in recent weeks – spoken about by Prime Minister Malcolm Turnbull in his security statement to the House of Representative earlier this month, and in numerous TV and radio interviews by Brandis – it appears cracking encryption may be less of a priority for the other Five Eyes member nations (the US, UK, New Zealand and Canada). It was mentioned in just two sentences in the official communique, coming at the very end of the description of topics discussed. Speaking on ABC's RN Breakfast on Wednesday, Brandis said the nations had agreed to "engage with ISPs and device makers to ensure that we secure from them the greatest possible level of cooperation" but denied this amounted to forcing them to build backdoors into their products. "What we need is to develop, and what we'll be asking the device makers and the ISPs to agree to, is a series of protocols as to the circumstances to which they will be able to provide voluntary assistance to law enforcement," he said. "We're not specifically asking them to do that [build in backdoors] and it's not as simple as that," he added. Brandis' reassurances around backdoors echoes those made by Prime Minister Malcolm Turnbull earlier this month. [Computerworld Australia](#) (2017-06-28)

Five Eyes network tackles encryption

Australia has taken a lead role at international security talks over unlocking secret communications between potential terrorists. The controversial move to access encrypted messaging was the top priority issue at the meeting with Australia's FiveEyes intelligence partners v the US, the UK, Canada and New Zealand. Fran Kelly spoke to Attorney General George Brandis who is in Ottawa for the talks. "Encryption can severely undermine public safety if it's by impeding lawful access to the content of communications during investigations into serious crimes during terrorism," said Attorney General Brandis. "What we decided to do ... was to engage with ISPs and device makers to ensure that we secure from them the greatest possible level of cooperation." "What we need to develop ... is a series of protocols as to the circumstances to which they will be able to provide voluntary assistance to law enforcement," he said. [ABC.net.au](#) (2017-06-28)

Five-eyes nations want comms providers to bust crypto for them

This week's five-eyes meeting has issued its communique, promising to get the tech sector to solve the problems of online terrorism and encrypted communications. As is the way of political communiques, there's a carefully-crafted lack of detail (sufficient, for example, for plausible deniability) about what exactly is planned. The communique explains the five countries need to "deal with the relentless threats of terrorism, violent extremism, cyber-attacks, and international instability, while retaining our deep commitment to the shared values of democracy, human rights and the rule of law". The relevant ministers of Australia, New Zealand, Canada, the United Kingdom and the USA pledged their support for the recently-announced "Global Internet Forum to Counter Terrorism" (Google, Facebook, Microsoft and Twitter). About encryption, the HTTPS-hosted communique says it can "severely undermine public safety efforts by impeding lawful access to the content of communications during investigations into serious crimes, including terrorism." [The Register](#)

As firms gauge cost, malware under control

The data-scrambling software epidemic that paralyzed computers globally is under control in Ukraine, where it likely originated, officials said Wednesday, as companies and governments around the world counted the cost of a crisis that is disrupting ports, hospitals and factories. In a statement published Wednesday, the Ukrainian Cabinet said that "all strategic assets, including those involved in protecting state security, are working normally." The same couldn't be said for India's largest container port, where one of the terminals was idled by the malicious software, which goes by a variety of names including ExPetr. [Associated Press](#) (Chronicle Herald, B6; London Free Press; Whig Standard; Toronto Sun; Winnipeg Sun; Ottawa Sun; Edmonton Sun; National Post; Montreal Gazette; Times-Colonist; Windsor

Today's News / Actualités
July 4, 2017 / le 4 juillet 2017
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through [Newsdesk](#) / Les Actualités peut également être accédée via [InfoMédia](#)

MINISTER / MINISTRE

TOP STORIES / MANCHETTES

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

LAW ENFORCEMENT / APPLICATION DE LA LOI

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS |
ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET
ASSASSINÉES

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRES

INTERNATIONAL

SOCIAL MEDIA / MÉDIAS SOCIAUX

MINISTER / MINISTRE

Canada Will Reportedly Apologize to Omar Khadr For His Mistreatment At Guantanamo Bay

Omar Khadr, one of the youngest people to have been detained at Guantanamo Bay, will reportedly get an official apology from the Canadian government and \$10 million in compensation over his mistreatment. According to the Globe and Mail, Khadr's apology is expected later this week. The government confirmed to BuzzFeed Canada that "there is an on-going court process on this case" but declined to provide further details. ***"Settlement processes are always strictly confidential by nature,"*** Scott Bardsley, press secretary for Minister of Public Safety Ralph Goodale, said in an email. ***"Accordingly, the Government is not in a position to provide any comment one way or another."*** [Buzzfeed News](#)

Designer drug smuggling posing “greatest challenge” to Canadian border agency: CBSA document

Designer and new psychoactive drugs which can produce effects similar to cocaine, marijuana, ecstasy and other drugs have emerged as the substances posing “the greatest challenge” to Canadian border officials, and are a “significant danger to public health,” according to a Canada Border Services Agency document. Despite a small number of seizures, the drugs are of particular concern because they comprise “the most rapidly evolving” drug smuggling market, says a briefing note sent to CBSA officers by its Intelligence Operations and Analysis Division in June 2016, obtained by Global News through an access to information request. (In 2015, “new psychoactive substances” or NPS — a category that encompasses narcotic and psychotropic drugs not included in international conventions before 1971 — comprised only seven per cent of 2,400 CBSA seizures of “other controlled drugs,” the vast majority of which were prescription drugs.) [Global News](#)

Court mulls drugs sentence

Ronald Learning is going to spend more time in prison but how much time is up in the air. Already serving a nine-year sentence in Saskatchewan for acting as a courier in a major drug trafficking operation, the 34-year-old Vernon man is before the BC Supreme Court for sentencing on 21 other drug-related convictions. The convicted man was brought into a courtroom Tuesday in handcuffs and wearing red prison garb. “When would the clock start ticking on these offenses?” asked Justice G.P. Weatherill during a sentencing hearing in Vernon. Crown Counsel Jeremy Guild has asked for a seven-to-nine year sentence for convictions on charges that include possession of restricted handguns, prohibited ammunition, false identification and various illicit drugs for the purpose of trafficking. On Jan. 8, 2015, a large quantity of Thai heroin was found by Canada Border Services Agency staff at Vancouver International Airport when they x-rayed a box and found the drugs hidden in two lamps. RCMP kept the box of 363.6 grams of heroin under surveillance. Four days later, Learning was arrested in Vernon when he tried to pick it up. [Castanet](#)

[BACK TO TOP / HAUT DE LA PAGE](#)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Global coalition demands “Five Eyes” protect encryption

CJFE had joined 83 organizations and individuals from Australia, Canada, New Zealand, the United Kingdom, and the United States to send letters to our respective governments insisting that government officials defend strong encryption. The letter comes on the heels of a meeting of the “Five Eyes” ministerial meeting in Ottawa on June 26 and 27... According to a joint communique issued after the meeting encryption and access to data was discussed. The communique stated that “encryption can severely undermine public safety efforts by impeding lawful access to the content of communications during investigations into serious crimes, including terrorism.” In the letter organized by Access Now, CIPPIC, and researchers from Citizen Lab, 83 groups and individuals from the so-called “Five Eyes” countries wrote “we call on you to respect the right to use and develop strong encryption.” Signatories also urged the members of the ministerial meeting to commit to allowing public participating in any future discussions. [CJFE](#)

[BACK TO TOP / HAUT DE LA PAGE](#)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Former Mountie sues RCMP for 'constructive dismissal' following PTSD diagnosis

A former Alberta Mountie has filed a civil suit against the RCMP, arguing she was forced out of her job after returning from treatment for post-traumatic stress disorder. Laura Lee Kelly, formerly the commander of an Edmonton-area RCMP detachment, filed a statement of claim with Court of Queen's Bench in June,

Daily Media Summary / Revue de presse quotidienne
Canadian Security Intelligence Service / Service canadien du renseignement de sécurité
July 5, 2017 / le 5 juillet 2017

CSIS IN THE NEWS / LE SCRS DANS LES NOUVELLES

MINISTER / MINISTRE

SECURITY AND LAW ENFORCEMENT / SÉCURITÉ ET EXÉCUTION DE LA LOI

BORDER ISSUES / ENJEUX FRONTALIERS

CYBER AND TECHNOLOGY / CYBER ET TECHNOLOGIE

MILITARY ISSUES / ENJEUX MILITAIRES

PUBLIC SERVICE / FONCTION PUBLIQUE

LEGISLATION AND POLICIES / LÉGISLATION ET POLITIQUES

OTHER / AUTRES

INTERNATIONAL / INTERNATIONAL

CSIS IN THE NEWS / LE SCRS DANS LES NOUVELLES

Des excuses et 10 millions pour Omar Khadr

Le gouvernement Trudeau offrira des excuses et une compensation d'au moins 10 millions de dollars à l'enfant-soldat Omar Khadr pour les abus dont il a souffert lorsqu'il était emprisonné pour terrorisme à la prison militaire américaine de Guantánamo, ont appris le Globe and Mail et le Toronto Star. La Cour suprême du Canada a reconnu en 2010 que les agents du Service canadien du renseignement de sécurité (SCRS) avaient violé les droits d'Omar Khadr lorsqu'ils l'ont interrogé à la base de Guantánamo, alors que l'adolescent croyait qu'ils étaient venus pour l'aider. Selon la Cour, le gouvernement du Canada a violé la Charte canadienne des droits et libertés et a privé des principes fondamentaux de la justice un individu qui n'était à l'époque qu'un enfant. Ainsi, Ottawa présentera finalement des excuses officielles à M. Khadr cette semaine et lui offrira une compensation de 10 millions, a rapporté le Globe and Mail, qui a obtenu l'information auprès d'une source au sein du gouvernement. Selon le Toronto Star, M. Khadr recevra plus de 10 millions. La Presse (Audrey Ruel-Manseau) (2017-07-04)

A chronological look a Khadr's legal saga

A look at the long legal odyssey of Canadian-born Omar Khadr... February 2003: Investigators from the RCMP and Canadian Security Intelligence Service interview Khadr at Guantanamo. Canadian Press (Red Deer Advocate, A8, Edmonton Sun)

Khadr, Arar and the fragile rule of law

An editorial states, "Reasonable people can debate many things about the apology and \$10.5-million settlement that the government of Canada is giving Omar Khadr. How much is a life worth? How much are you owed for being tortured? How much should Ottawa pay Mr. Khadr for the decade he spent in American custody, and the physical, psychological and legal abuse he suffered while a guest of Uncle Sam - given that Canada had little more than a walk-on part in the affair? Maybe \$10.5-million is too much. Then again, maybe if the Trudeau government hadn't settled, a judge would have awarded even

A Montreal man accused of stabbing a police officer in the neck at Bishop International Airport in Flint, Mich., last month is back in court Wednesday. Amor Ftouhi, a 49-year-old native of Tunisia, is charged with committing violence at an airport on June 21 when he allegedly pulled out a long knife with a serrated edge and attacked Lt. Jeff Neville. He was denied bail when he made a brief court appearance in Flint last week. Authorities in both Canada and the U.S. treated the attack as a terrorist incident. The FBI investigated in Michigan while police in Montreal swarmed Ftouhi's St-Michel neighbourhood. Ftouhi is expected in court for his preliminary hearing around 1:30 p.m. [CBC News](#)

Ottawa won't stop victims of terror from suing Iran in Canada

After coming into office on a pledge of warming to Iran, Canada has apparently abandoned plans to make nice with the theocracy. In so doing, the Trudeau government is giving the green light to a flurry of lawsuits against the Iranian regime. The Canadian government opted last month to continue listing Iran as a state supportive of terrorism, which will continue to keep relationships between Ottawa and Tehran virtually non-existent. Being included on the list is an unenviable position for a foreign state, as those listed on it — currently just Iran and Syria — do not enjoy immunity when it comes to terrorism-related crimes. Normally, under international law, the courts of one state cannot allow legal action against another nation. The decision to keep Iran on that list was announced on Friday ahead of the Canada Day long weekend. The government must review the list every two years. [VICE News](#) (2017-07-04)

[BACK TO TOP / HAUT DE LA PAGE](#)

BORDER ISSUES / ENJEUX FRONTALIERS

NIL

[BACK TO TOP / HAUT DE LA PAGE](#)

CYBER AND TECHNOLOGY / CYBER ET TECHNOLOGIE

Global coalition demands "Five Eyes" protect encryption

CJFE had joined 83 organizations and individuals from Australia, Canada, New Zealand, the United Kingdom, and the United States to send letters to our respective governments insisting that government officials defend strong encryption. The letter comes on the heels of a meeting of the "Five Eyes" ministerial meeting in Ottawa on June 26 and 27... According to a joint communique issued after the meeting encryption and access to data was discussed. The communique stated that "encryption can severely undermine public safety efforts by impeding lawful access to the content of communications during investigations into serious crimes, including terrorism." In the letter organized by Access Now, CIPPIC, and researchers from Citizen Lab, 83 groups and individuals from the so-called "Five Eyes" countries wrote "we call on you to respect the right to use and develop strong encryption." Signatories also urged the members of the ministerial meeting to commit to allowing public participating in any future discussions. [CJFE](#) (2017-07-04)

Ukraine: We prevented second cyberattack

Ukrainian Interior Minister Arsen Avakov says that authorities have avoided a second cyberattack. The announcement suggests that the effort to wreak electronic havoc across Ukraine is ongoing. Ukraine is still trying to find its feet after scores or even hundreds of businesses and government agencies were hit by an explosion of data-scrambling software on June 27. Avakov said in a statement posted to his Facebook page that what he described as the second stage of that malware attack had been timed to hit its peak at 4 p.m. Ukraine time on Tuesday. Avakov said that, like the first attack, Tuesday's originated from the Ukrainian tax firm M.E. Doc. [Associated Press](#) (National Post)

Ukrainian police seize software company's servers

Ukraine's national cybercrime unit seized servers belonging to a small company at the centre of a global outbreak of malicious software after "new activity" was detected there, the service said in a statement

COMDO / COMDO (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Wednesday, July 05, 2017 8:37 AM
To: Cyber Security / Sécurité cybernétique (PS/SP)
Subject: Cyber Security Media Summary / Revue de presse sur la cybersécurité - 2017-07-05

Cyber Security Media Summary / Revue de presse sur la cybersécurité July 5, 2017 / le 5 juillet 2017

TOP STORIES / MANCHETTES

THREATS, VULNERABILITIES AND RESOLUTIONS / MENACES, VULNÉRABILITÉS ET SOLUTIONS

CYBER SURVEILLANCE AND ESPIONNAGE / CYBERSURVEILLANCE ET ESPIONNAGE

CYBER DEFENCE / CYBERDÉFENSE

RESEARCH AND DEVELOPMENT / RECHERCHE ET DÉVELOPPEMENT

OTHER / AUTRES

TOP STORIES / MANCHETTES

Global coalition demands “Five Eyes” protect encryption

CJFE had joined 83 organizations and individuals from Australia, Canada, New Zealand, the United Kingdom, and the United States to send letters to our respective governments insisting that government officials defend strong encryption. The letter comes on the heels of a meeting of the “Five Eyes” ministerial meeting in Ottawa on June 26 and 27... According to a joint communique issued after the meeting encryption and access to data was discussed. The communique stated that “encryption can severely undermine public safety efforts by impeding lawful access to the content of communications during investigations into serious crimes, including terrorism.” In the letter organized by Access Now, CIPPIC, and researchers from Citizen Lab, 83 groups and individuals from the so-called “Five Eyes” countries wrote “we call on you to respect the right to use and develop strong encryption.” Signatories also urged the members of the ministerial meeting to commit to allowing public participating in any future discussions. [CJFE](#)

Ukraine: We prevented second cyberattack

Ukrainian Interior Minister Arsen Avakov says that authorities have avoided a second cyberattack. The announcement suggests that the effort to wreak electronic havoc across Ukraine is ongoing. Ukraine is still trying to find its feet after scores or even hundreds of businesses and government agencies were hit by an explosion of data-scrambling software on June 27. Avakov said in a statement posted to his Facebook page that what he described as the second stage of that malware attack had been timed to hit its peak at 4 p.m. Ukraine time on Tuesday. Avakov said that, like the first attack, Tuesday's originated from the Ukrainian tax firm M.E. Doc. [Associated Press](#) (National Post)

Ukrainian police seize software company's servers

Ukraine's national cybercrime unit seized servers belonging to a small company at the centre of a global outbreak of malicious software after "new activity" was detected there, the service said in a statement early Wednesday. The announcement raised the possibility that the hackers behind last week's wide-ranging cyberattack were still seeking to sow chaos. Tax software firm M.E. Doc was raided to "immediately stop the uncontrolled proliferation" of malware. In a series of messages, Cyberpolice spokeswoman Yulia Kvitko suggested that M.E. Doc had sent or was preparing to send a new update and added that swift action had prevented any further damage. [Associated Press](#) (National Post; Chronicle Journal); [Bleeping Computer](#); [Infosecurity Magazine](#); [Softpedia](#); [Gizmodo](#)

[BACK TO TOP / HAUT DE LA PAGE](#)

THREATS, VULNERABILITIES AND RESOLUTIONS / MENACES, VULNÉRABILITÉS ET SOLUTIONS

NotPetya Group Moves All Their Bitcoin, Posts Proposition on the Dark Web

The person or group behind the NotPetya ransomware has made its first move since the outbreak that took place eight days ago. The first to spot movement from the group was a Twitter bot that was designed to tweet out transactions associated with the Bitcoin wallet used by the NotPetya ransomware (1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx). Around 21:30 UTC, the NotPetya group sent two payments — of around \$285 and \$300 — to the Bitcoin wallets associated with the PasteBin and DeepPaste text sharing services. Half an hour later, the group moved the remainder of their Bitcoin funds to a new account, located at 1Ftixp78FjTWFi3ssJjBw5NqKf5ZPQjXBb. The transferred sum was 3.96298755, which amounts to over \$10,000, the total sum made by the group from their operation last week... At the same time when the group was making these financial transactions, they also appear to have posted two messages online, on PasteBin and DeepPost. Both messages featured the same text, reading: "Send me 100 Bitcoins and you will get my private key to decrypt any harddisk (except boot disks)." [Bleeping Computer](#); [Motherboard](#)

South Korea's Largest Ethereum Exchange Was Hacked

Losses may be upwards of \$1,000,000 USD. South Korea is a leader in the ethereum cryptocurrency; a full 20 percent of global ether trades are exchanged for South Korea's currency, the won. Now, all the attention appears to have attracted hackers. Last week, customer information and allegedly "billions" of won were stolen from South Korea's largest exchange for buying and selling ether as well as its more popular and established cousin bitcoin. South Korea-based Bithumb is the fourth largest cryptocurrency exchange in the world by volume, and the second largest ethereum exchange behind China's OKCoin. English-language details are scarce right now, but the government-funded Yonhap News reported that Bithumb contacted South Korea's cyber crime watchdog on Friday after it learned of the hack. According to Yonhap, a Bithumb employee's home computer was hacked and information on 30,000 customers was stolen, although no passwords were compromised, according to the exchange. Yonhap also reports that South Korean officials are now investigating the hack. [Motherboard](#); [Bleeping Computer](#); [Help Net Security](#); [Beta News](#)

Vulnerabilities in Pre-Installed Software expose Dell Systems to hack

According to experts from Talos, security vulnerabilities in pre-installed software expose Dell systems to code execution attacks. Security vulnerabilities in pre-installed software expose Dell systems to code execution attacks. Hackers can exploit the flaws to disable security mechanisms, escalate privileges and execute arbitrary code within the context of the application user. According to the experts from CISCO Talos, the vulnerable pre-installed software is the Dell Precision Optimizer application service and the Invincea-X and Invincea Dell Protected Workspace. [Security Affairs](#); [Softpedia](#)

[BACK TO TOP / HAUT DE LA PAGE](#)

CYBER SURVEILLANCE AND ESPIONNAGE / CYBERSURVEILLANCE ET ESPIONNAGE

NZ Airport Travelers Forced to Surrender Device Passwords, Data Copied by Govt

New Zealand airport customs agents force thousands of travelers every year to hand over the passwords for their devices, in some cases inspecting files and even copying the data for the government. Though this sounds like a severe privacy violation, the so-called digital strip search is performed without a court order as the customs agents claim to adhere to the country's privacy act, which allows them to perform searches on people perceived as possible threats to national security. Data obtained by New Zealand's 1 news channel reveals that agents can perform a quick or a much more extensive search, with one passenger explaining that he had to spend no less than 5 hours until all his data was analyzed. In some cases, the customs officers can create backups of travelers' data and then pass it along to the government and law enforcement for closer inspection. The digital strip search has been performed on more than 1,350 people since 2015, and most of them were New Zealanders. 296 people were based in New Zealand, while 269 of the travelers who were forced to surrender their passwords were Chinese.

Intelligence Investigations Customs general manager Jamie Bamford says that customs agents have the necessary means to crack the encryption of devices protected with a password if owners do not agree to unlock them themselves. [Softpedia](#)

Security researchers Crack 1024-bit RSA Encryption in GnuPG Crypto Library

Experts have devised a side-channel attack on RSA secret keys that allowed to crack 1024-bit RSA Encryption in GnuPG Crypto Library. Security researchers have found a critical vulnerability, tracked as CVE-2017-7526, in a Gnu Privacy Guard (aka (GnuPG or GPG) cryptographic library that allowed them cracking RSA-1024 and extract the RSA key to decrypt data. The research team was composed of experts from several universities, including Technical University of Eindhoven, the University of Illinois, the University of Pennsylvania, the University of Maryland, and the University of Adelaide. GnuPG is popular open source encryption software currently used by many operating systems, including Linux, Windows, and macOS X. [Security Affairs](#); [Bleeping Computer](#)

Importance of AI, data in law enforcement suggests growing tension with privacy

Artificial intelligence (AI) and machine learning play an important role in helping law enforcement deal with increasing threats, but the need then for access to data is likely to further drive concerns about privacy. Closer collaboration between the private and public sectors as well as citizens also would be essential, according to delegates at Interpol World 2017 in Singapore this week. The rise of urbanisation, globalisation, and online connectivity had unleashed tremendous amount of data that was never before available, Anselm Lopez, director of strategic relations directorate, international cooperation and partnerships division at Singapore's Ministry of Home Affairs. He also is part of Interpol's Asia executive committee. Lopez noted that data had become a critical element in decision making for law enforcement, as it had for enterprises, and these agencies would have to adapt or be rendered irrelevant. He said the data could be used and analysed to combat crime and threats, including terrorism, incident response, and cybercrime. Failure to do so efficiently, especially amid the deluge of data available, could lead to law enforcement missing out on critical details and making decisions that were not supported by sound analysis, and possibly leading to loss of lives or losses. [ZD Net](#)

Russia's Eugene Kaspersky battles viruses and deep suspicions from U.S. intelligence officials

The chief executive of Russia's Kaspersky Lab says he's ready to have his company's source code examined by U.S. government officials to help dispel long-lingering suspicions about his company's ties to the Kremlin. In an interview with The Associated Press at his Moscow headquarters, Eugene Kaspersky said Saturday that he's also ready to move part of his research work to the U.S. to help counter rumours that he said were first started more than two decades ago out of professional jealousy. "If the United States needs, we can disclose the source code," he said, adding that he was ready to testify before U.S. lawmakers as well. "Anything I can do to prove that we don't behave maliciously I will do it." Kaspersky, a mathematical engineer who attended a KGB-sponsored school and once worked for Russia's Ministry of Defence, has long been eyed suspiciously by his competitors, particularly as his anti-virus products became popular in the U.S. market. Some speculate that Kaspersky, an engaging speaker and a fixture of the conference circuit, kept his Soviet-era intelligence connections. Others say it's unlikely that his company could operate independently in Russia, where the economy is dominated by state-owned companies and the power of spy agencies has expanded dramatically under President Vladimir Putin. [Associated Press](#) (Toronto Star)

[BACK TO TOP / HAUT DE LA PAGE](#)

CYBER DEFENCE / CYBERDÉFENSE

NIL

[BACK TO TOP / HAUT DE LA PAGE](#)

RESEARCH AND DEVELOPMENT / RECHERCHE ET DÉVELOPPEMENT

NIL

[BACK TO TOP / HAUT DE LA PAGE](#)

OTHER / AUTRES

Darknet 101: Your guide to the badlands of the internet

Hacked login details, cybersecurity exploits for hire, guns, drugs and ammo -- if there's something shady going on online, chances are it's happening on the darknet. But for those of us used to opening Chrome or Safari to get online, the darknet is an entirely different beast. How does it work? How is it different to the "surface web"? And what do you need to know before you wade in? [CNET](#)

[BACK TO TOP / HAUT DE LA PAGE](#)

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille de la sécurité publique. We can be reached at / Vous pouvez communiquer avec nous à l'adresse : PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

*Sent to: !Cyber Security Media Summary Dist List #1; !Cyber Security Media Summary Dist List #2; !Cyber Security Media
Summary Dist List #3; !Cyber Security Media Summary Dist List #4*

SECRET //CABINET CONFIDENCE

[REDACTED]

From: [REDACTED]
Sent: September-27-17 2:22 PM
To: [REDACTED]
Cc: Beecher, Sophie; [REDACTED]
Subject: [REDACTED]

CLASSIFICATION:SECRET //CABINET CONFIDENCE

Hi [REDACTED]

[REDACTED]

[REDACTED]

Policy Analyst
Intelligence Policy Division
Public Safety Canada

[REDACTED]

SECRET //CABINET CONFIDENCE

 (unclass)

SECRET //CABINET CONFIDENCE

Lauzon, Adam (PS/SP)

From: Lauzon, Adam (PS/SP)
Sent: Tuesday, October 17, 2017 4:27 PM
To: Digiacomo, Daniela (PS/SP)
Cc: Glazer, Julie (PS/SP)
Subject: Lawful Access

Hi Daniela,

We understand that following IPC, the ADM was asked to do some follow-ups regarding the lawful access item going on Dec 11.

Can you confirm with us when those updates have been completed?

Thanks very much,

Adam

Adam Lauzon

Cabinet Briefing Analyst | Analyste d'information du Cabinet
Public Safety Canada / Sécurité publique Canada
Tel.: (613) 991-2902
adam.lauzon@canada.ca



SECRET / Confidence of the Queen's Privy Council

s.69(1)(g) re (a)

s.69(1)(g) re (e)

Minister's Briefing Brefpage du ministre

Monday, December 4, 2017 - 11:00 a.m. to 12:00 p.m. / Le lundi 4 décembre 2017 - 11h00 à 12h00

Room 501-S, Centre Block / Pièce 501-S, Édifice du Centre

AGENDA / ORDRE DU JOUR

| ITEM / POINT | SUBJECT / SUJET | PARTICIPANTS | DURATION / DURÉE |
|-----------------|-----------------|---|-------------------------------------|
| 1 | [REDACTED] | <p>LEAD / RESPONSABLE</p> <p>Kathy Thompson <i>Assistant Deputy Minister, CSCCB</i></p> <p>Mark Potter <i>Director General of Research, Intergovernmental Affairs & Horizontal Policy Directorate, CSCCB</i></p> <p>John Ossowski <i>President, CBSA</i></p> <p>Robert Mundie <i>A/Vice-President, CBSA</i></p> | <p>11:00 11:30 (30 min)</p> |
| 2 | [REDACTED] | <p>LEAD / RESPONSABLE</p> <p>Monik Beauregard <i>Senior Assistant Deputy Minister, NCSB</i></p> <p>John Davies <i>Director General, National Security Policy Directorate, NCSB</i></p> <p>OTHERS / AUTRES</p> <p>Francois Bidal <i>Acting Deputy Commissioner, RCMP</i></p> <p>Jeff Adams <i>Acting Assistant Commissioner, Technical Operations, RCMP</i></p> <p>Geoffrey Crampton <i>Assistant Director, Operations Enablement, CSIS</i></p> | <p>11:30 12:00 (30 min)</p> |

TAB 1

**Pages 698 to / à 709
are withheld pursuant to sections
sont retenues en vertu des articles**

69(1)(e), 69(1)(g) re (a)

**of the Access to Information
de la Loi sur l'accès à l'information**

TAB 2

**Pages 711 to / à 738
are withheld pursuant to sections
sont retenues en vertu des articles**

69(1)(d), 69(1)(e), 69(1)(g) re (a)

**of the Access to Information
de la Loi sur l'accès à l'information**

**Pages 739 to / à 743
are withheld pursuant to section
sont retenues en vertu de l'article**

69(1)(g) re (a)

**of the Access to Information
de la Loi sur l'accès à l'information**

**Pages 744 to / à 756
are withheld pursuant to sections
sont retenues en vertu des articles**

69(1)(e), 69(1)(g) re (a)

**of the Access to Information
de la Loi sur l'accès à l'information**

**Pages 757 to / à 954
are withheld pursuant to section
sont retenues en vertu de l'article**

69(1)(a)

**of the Access to Information
de la Loi sur l'accès à l'information**

SECU AND ETHI RECOMMENDATIONS

SECU RECOMMENDATIONS

| Recommendation | Addressed? | Context | Reasoning |
|--|-------------------------|---|---|
| <p>1. That the <i>Department of Public safety and Emergency Preparedness Act</i> be amended to require the publication of the Public Report on Terrorist Threat to Canada, and specifically include 1) performance indicators, 2), data on information sharing as it relates to the Security of Canada Information Sharing Act, and 3) the obligation that it be annually tabled in Parliament.</p> | <p>PARTIALLY</p> | <p>There is concern that Canada's current national security regime lacks sufficient transparency and accountability. Information sharing conducted under the authority of SCISA has been identified as a concern.</p> | <p>Consulted with NSOD, and this recommendation will not be addressed.</p> |

SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|-------------------|--|--|
| <p>2. That building upon past experience, the Government of Canada increase funding for long-term research as well as the development of professional expertise, both within government and outside government, to understand and address new and evolving threats to national security.</p> | <p>YES</p> | | <p>The Government is committed to ensuring that our continuing efforts in the area of countering radicalization to violence are informed by extensive new research and input from a wide range of stakeholders. As part of its role as a centre of excellence, an Office for community outreach and countering radicalization to violence (the Office) will both develop its own in-house expertise to help produce and mobilize a greater evidence base, and support efforts led by other organizations and initiatives.</p> <p>Similar to the Office, a range of departments and agencies are actively involved as leads or lead partners in major initiatives for long-term research and professional development, to address a broader range of new and evolving threats. Examples include the Academic Outreach Program at the Canadian Security Intelligence Service, the SERENE-RISC Smart Cybersecurity Network supported by the Networks of Centres of Excellence Canada federal funding program, and ongoing investments by CSSP to partner with lead agencies, responsible for national security on long-term research and development to address current and emerging security threats. Such initiatives bring together experts and practitioners from within and outside government, aim to address both current and emerging threats, and will continue to have a central role to play in the development and applications of knowledge.</p> |
|--|-------------------|--|--|

SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|------------|--|---|
| <p>3. That Public Safety Canada develop a community-based strategy for the prevention of radicalization to violence based on research data and focusing on best local practices. It should include programs for the empowering of youth and women, inclusion of marginalized persons and groups, and broad community and educational activities.</p> | <p>YES</p> | | <p>The Government of Canada announced \$35 million over five years, and \$10 million per year ongoing to create the Office. As a centre of excellence, the Office will provide national leadership on Canada's response to radicalization to violence, coordinate talent and expertise, provide support to municipal, community and grassroots efforts, and enhance the evidence base on this issue. Its goal is to support the prevention of radicalization to violence of all kinds, regardless of where it originates.</p> <p>The Office will be engaging broadly across the country in 2017 to advance a national strategy on countering radicalization to violence (CRV) that is representative of diverse Canadian views. To this end, the Office will actively engage with Canada's diverse communities, experts, academia, key sectors (e.g., first responders, education, police, social services, health services, private sector) and various groups (e.g. women, youth, faith-based)</p> <p>As part of its role as a centre of excellence, the Office will both develop its own in-house expertise to help produce and mobilize a greater evidence base, and support efforts led by other organizations and initiatives. The latter will include collaboration with other government agencies as they continue building evidence-based CRV tools, as well as with initiatives funded elsewhere in the federal government, such as through Defence Research and Develop Canada's Canadian Safety and Security Program (CSSP), and the Social Sciences and Humanities Council of Canada (SSHRC). A notable example of research supported by both CSSP and SSHRC is the wide range of studies led by the Canadian Network for Research on Terrorism, Security, and Society, a group with which the Office is already collaborating. In addition, several ministries at the Provincial and Territorial level are also investing in CRV research, with recent calls for proposals in both Quebec and Ontario, and the Office will work to complement such efforts in developing and sharing expertise.</p> |
|--|------------|--|---|

SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|-------------------|--|--|
| <p>4. That counter-radicalization programs continue to include and expand efforts to stop groups that promote radicalization from gaining a foothold to spread their message of violence, or the precursors to violence.</p> | <p>YES</p> | | <p>To Champion national CRV efforts, a Special Advisor will be appointed in the near future to promote and coordinate Canadian CRV efforts domestically and internationally; engage with stakeholders and partners to foster trust and build relationships; and advise the Minister of Public Safety and Emergency Preparedness and the Office on CRV issues. The position will be supported by the Office and will receive advice from a new CRV Expert Committee, made of appointed experts in the field. Moving forward, I can assure you that our government is committed to creating a CRV framework that benefits all Canadians, regardless of religion or ideology.</p> <p>A significant portion of the funding for the Office will be allocated to a new grants and contributions program, the <i>Community Resilience Fund (CRF)</i>, to support domestic programming and research initiatives on this issue.</p> <p>Current priority areas for the CRF include: supporting local intervention initiatives that aim to redirect individuals at risk off the path of radicalization to violence; performance measurement and evaluation tools built to gauge program effectiveness in Canada; action-oriented research, in areas such as developing better ways to assess pathways into violent extremism, in support of frontline practitioners; and, youth engagement and support for the development of credible alternative narratives that reflect local context.</p> |
|--|-------------------|--|--|

s.21(1)(a)

SECU AND ETHI RECOMMENDATIONS

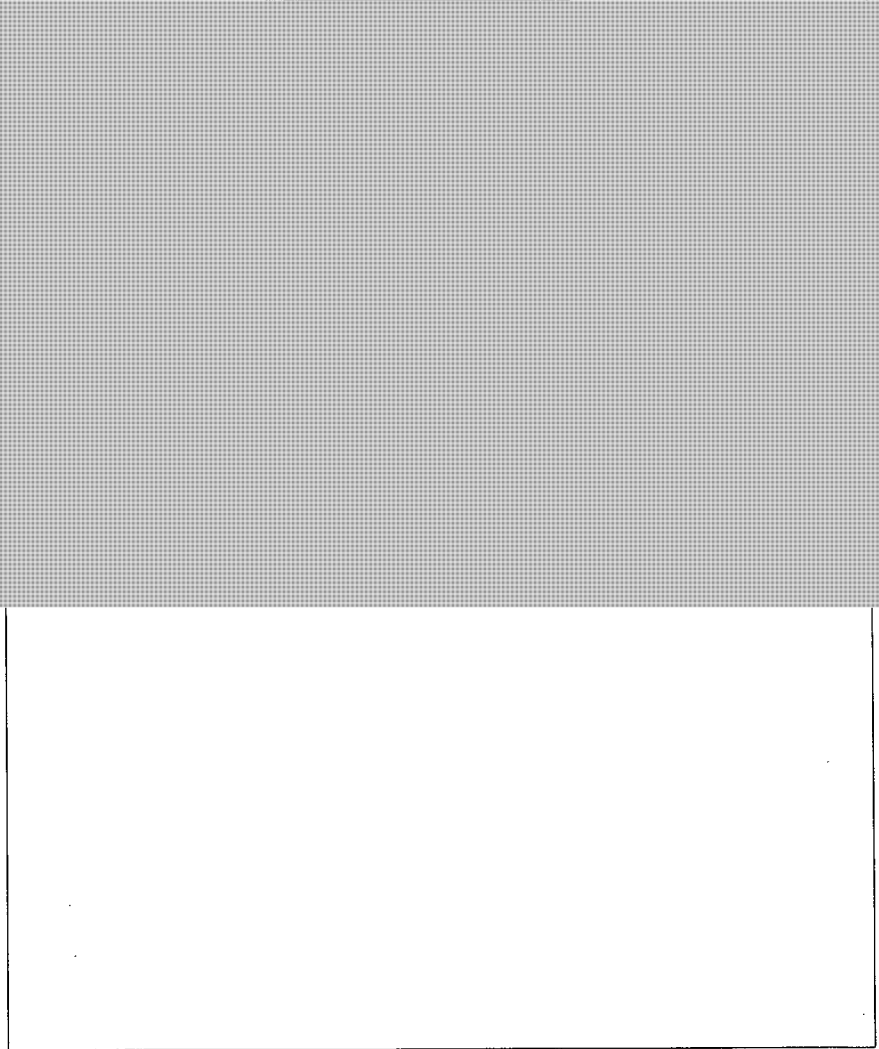
| | | | |
|--|-----------------------------------|---|--|
| <p>5. That the Government of Canada increase its contribution to and promote the Communities at Risk: Security Infrastructure Program to help communities at risk of hate-motivated crimes improve their security infrastructure.</p> | <p>YES</p> | | <p>As of December 1st, 2016, the Government of Canada has streamlined the submission process for the Communities at Risk: Security Infrastructure Program (SIP) to implement two annual calls for proposal cycles, enhance flexibility and accessibility to the program. In Budget 2017, new funding of \$5.0 million over five years has been allocated, starting in 2017-18, in support of SIP.</p> |
| <p>6. That the Government of Canada recognize that establishing a national security and intelligence committee of parliamentarians is a first step toward increasing the transparency and accountability of the security agencies and that other mechanisms must be considered in order to be considered in order to restore Canadians' trust in those agencies.</p> | <p>YES</p> | <p>Designated review mechanisms/bodies are seen as the most direct way of ensuring accountability for and organization as they are able to maintain a critical distance from the activities being reviewed.</p> <p>This is not a silver-bullet approach, but needs to be seen as a part of creating a comprehensive accountability regime that is heavily integrated with existing review bodies.</p> | |
| <p>7. That the Government of Canada create an independent and external review body for the operations of the Canada Border Service Agency.</p> | <p>PARTIALLY ADDRESSED</p> | <p>CBSA does not have a review body while other agencies (RCMP, CSIS, CSE) do. Since CBSA has law enforcement and national security functions, many of its activities are not disclosed publicly.</p> | |

SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|--|--|--|
| <p>8. That the Government of Canada establish statutory gateways among all national public safety and national security review bodies in order to provide for the appropriate exchange of information, referral of investigations, conduct of joint investigations and coordination in the preparation of reports.</p> | <p>YES, THROUGH ALTERNATE MEANS</p> | <p>Stakeholders have argued that the current siloed approach can hamper investigations as review bodies can't follow the information/investigation from one agency to another. Agencies can conduct joint investigations whereas review bodies can't do joint reviews.</p> | |
| <p>9. That the Government of Canada increase the funding of all public safety and national security review bodies to enable them to carry out their mandates effectively, matching the increase in activities of the agencies they oversee and to ensure the protection of Canadians' rights and freedoms.</p> | <p>YES</p> | <p>Increased activities and scope of agencies means review bodies should have a commensurate increase in resources to maintain their ability to review these activities. (No direct reference to funding in report)</p> | |

s.21(1)(a)

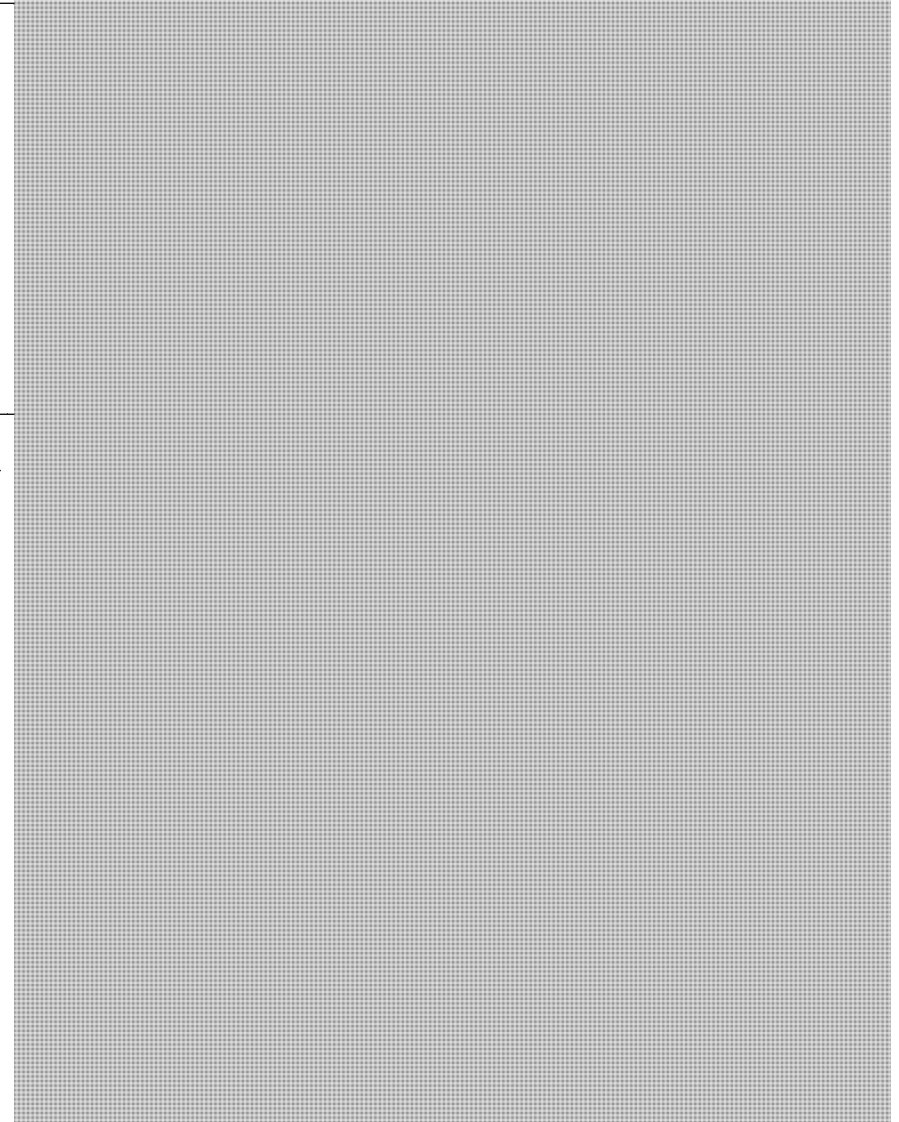
SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|--|---|--|
| <p>10. That the Government of Canada establish a national security review office as the integrated review body for the bodies inside the government that have a national security mandate that are currently without a review body and that the national security review office act as a coordinating committee for the existing national security review bodies. The national security review office should have the following mandate:</p> <p>1) to ensure that the statutory gateways among the independent review bodies operate effectively,</p> <p>2) to take steps to avoid duplicate reviews,</p> <p>3) to provide a centralized intake mechanism for complaints regarding the national security activities of federal entities,</p> <p>4) to report on accountability issues relating to practices and trends in the area of national security in Canada, including the effects of those practices and trends on human rights and freedoms,</p> <p>5) to conduct public information programs,</p> <p>6) to initiate discussion for co-operative review with independent review bodies for provincial and municipal police forces involved in national security activities.</p> | <p>YES, THROUGH ALTERNATE MEANS</p> | <p>Centralizing the coordination of independent review will create a more efficient process. Classified information sharing can be facilitated and carried out properly. The National Security Advisor's (NSA) role could be enhanced to allow a more centralized process of coordination among review bodies. (Following recommendations of the Air India Inquiry)</p> |  |
|--|--|---|--|

s.21(1)(a)

SECU AND ETHI RECOMMENDATIONS

| | | |
|---|-----------------------------------|---|
| <p>11. That the reference to the Canadian Charter of Rights and Freedoms in section 12.1(3) of the Canadian Security Intelligence Service Act be repealed in order to remove the ability to violate the Charter.</p> | <p>YES</p> | <p>Currently, CSIS may undertake threat reduction activities that contravene the <i>Charter</i> currently by applying for a warrant from the Federal Court.</p> <p>No formal definition of a disruption activity in Canada (or other Five Eyes countries), leading to broad interpretation.</p> <p>Some stakeholders believe CSIS should be stripped of threat disruption powers.</p> |
| <p>12. That before the Canadian Security Intelligence Service engage in disruptive powers, the agency exhaust all other non-disruptive means of reducing threats.</p> | <p>PARTIALLY ADDRESSED</p> | <p>There are concerns that the threat disruption powers of CSIS are too broad, and that this may facilitate their possible misuse or overlap with law enforcement functions. The separation of intelligence gathering with law enforcement functions was a key reason for CSIS being created.</p> |



SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|--|---|--|
| <p>13. That the Government of Canada ensure that section 12.1 of the Canadian Security Intelligence Service Act (CSIS Act) requires that all disruption activities that violate Canadian law necessitate a warrant and that the Minister's approval be obtained prior to the activity under section 21.1 of the CSIS Act.</p> | <p>YES, THROUGH ALTERNATIVE MEANS</p> | <p>There currently is no requirement to seek a warrant for disruption activities that do not violate the <i>Charter</i>. Stakeholders argue that CSIS should not have the ability to break Canadian law as they are able carry out their mandates without doing so.</p> | |
| <p>14. That the Canadian Security Intelligence Service Act be amended in order to include a quarterly report on disruption activities for the Committee of Parliamentarians.</p> | <p>YES, THROUGH ALTERNATIVE MEANS</p> | <p>There is a general concern that CSIS and other national security institutions require further accountability and transparency. Threat disruption activities have been identified as a particular concern due to their secrecy and lack of accountability measures.</p> | |

s.21(1)(a)

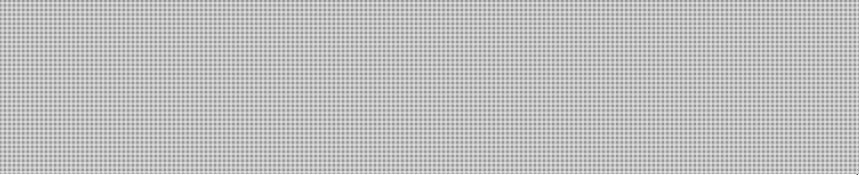
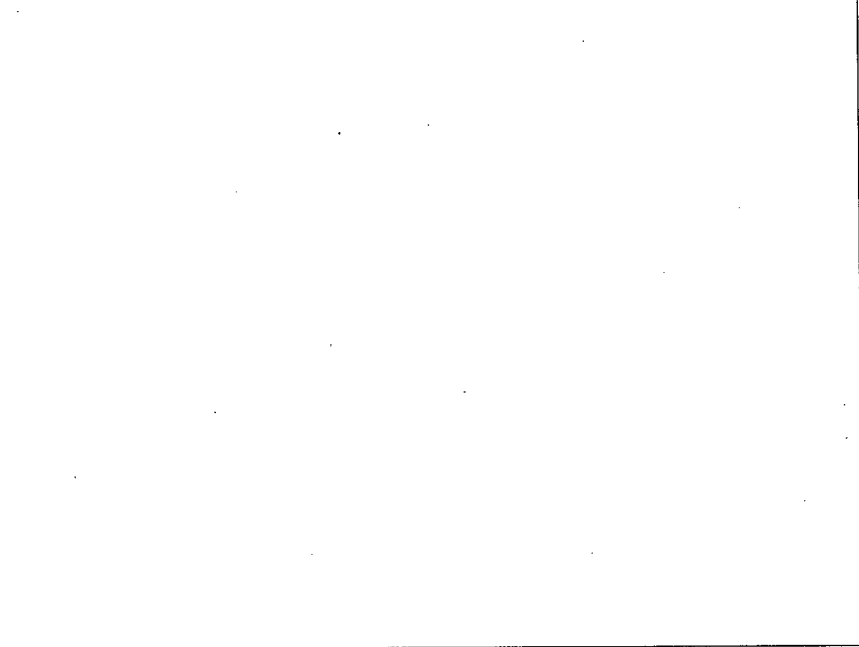

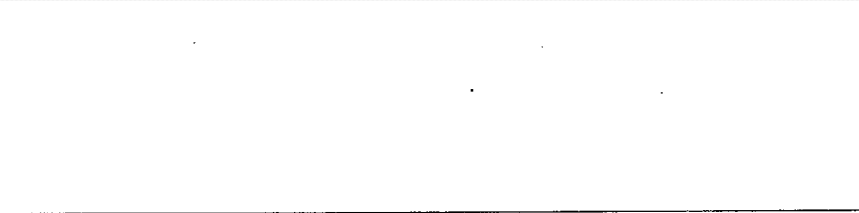
SECU AND ETHI RECOMMENDATIONS

| | | | |
|---|--|--|--|
| <p>15. That the Government of Canada ensure that the Canadian Security Intelligence Service respect the traditional distinction between intelligence gathering and police disruptive operations by working in concert with the Royal Canadian Mounted Police and other police forces to assist in their investigations and the exercise of their disruptive powers, and not duplicate such investigations or powers.</p> | <p>YES, THROUGH ALTERNATIVE MEANS</p> | <p>There is some concern that CSIS threat disruption may overlap with police operations, consuming resources and leading to duplication of activities.</p> <p>However, as CSIS tends to be one of the first agencies to acquire intelligence about an attack, they may be seen as the best placed to approach a disruptive activity.</p> | |
| <p>16. That the Government of Canada restrict preventive detention to only exceptional, narrowly defined circumstances, and ensure conditions of those detained comply with Canadian and international standards on detention and due process.</p> | | | <p>Criminal Code file— under JUS portfolio</p> |
| <p>17. That the Government of Canada study other measures that could be used instead of preventive detention.</p> | | | <p>Criminal Code file— under JUS portfolio</p> |

SECU AND ETHI RECOMMENDATIONS

| | | | |
|---|--|--|--|
| <p>18. That sections 83.3(2) and 83.3(4) of the Criminal Code be amended in order to remove the wording “may be” and “is likely to” applicable to recognizance with conditions and to replace them with the “balance of probabilities” concept.</p> | | | <p>Criminal Code file— under JUS portfolio</p> |
| <p>19. That section 83.221 of the Criminal Code be amended in order to clarify the concept of “terrorism offences in general” and to consider replacing it with “terrorism offences”, as defined in section 2 of the Criminal Code. Furthermore, the Government of Canada should consider applicable defences modeled after those in section 319(3) of the Criminal Code that prohibit the wilful promotion of hatred and contain a number of truth and fair comment defences.</p> | | | <p>Criminal Code file— under JUS portfolio</p> |
| <p>20. That the Government of Canada ensure no Canadian is restricted from the legitimate exercise of their right to freedom of expression and freedom of association, and that it remove any provisions in current legislation that may be in contravention to the Charter of Rights and Freedoms or restrict the legitimate exercise of rights, particularly those of journalists, protesters, non-governmental organizations and environmental and Indigenous activists.</p> | | | <p>Criminal Code file— under JUS portfolio</p> |
| <p>21. That the definition of “terrorist propaganda” in section 83.222(8) of the Criminal Code be amended in order to be limited to material that counsels the commission of a terrorist offence or that instructs the commission of a terrorist offence.</p> | | | <p>Criminal Code file— under JUS portfolio</p> |

SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|--|---|---|
| <p>22. That the scope of activities subject to information sharing under the Security of Canada Information Sharing Act be narrowed so as to be consistent with all other national security legislation.</p> | <p>YES, THROUGH ALTERNATIVE MEANS</p> | <p>The definition of “activity that undermines the security of Canada” identifies which national security-compromising activities fall within the scope of the SCISA and accompanying scope of departmental responsibilities that information can be shared for.</p> <p>“Activity that undermines the security of Canada” is currently defined as any activity that undermines Canada’s sovereignty, security, or territorial integrity or the lives or the security of the people of Canada”. This core part of the definition has been referred to as the “chapeau” of the definition.</p> <p>The illustrative examples in the definition are activities that <u>could</u> be activities that undermine the security of Canada <u>if</u> the specific instance of the example meets the chapeau threshold (i.e., it undermines “Canada’s sovereignty, security, or territorial integrity or the lives or the security of the people of Canada”.</p> |   |
| <p>23. That the Government of Canada change the definition of an “activity that undermines the security of Canada” and revise the list of activities enumerated in section 2 of the Security of Canada Information Sharing Act in order to ensure that basic civil liberties such as freedom of expression, freedom of association and freedom of peaceful assembly are upheld.</p> | <p>YES, THROUGH ALTERNATIVE MEANS</p> | <p>Section 2 of SCISA defines what activities are within the scope of the SCISA by providing a list of illustrative examples of activities that could be covered by the core portion component of the definition. It has been criticized as being too broad in scope and does not clearly indicate that advocacy, protest, dissent and artistic expression are excluded from the list of activities for which information could be shared.</p> |   |

s.21(1)(a)

SECU AND ETHI RECOMMENDATIONS


| | | | |
|--|--|---|--|
| <p>24. That the Government of Canada ensure that protections guaranteed under the Privacy Act are not abrogated by the Security of Canada Information Sharing Act, thus ensuring Canadians' privacy is protected.</p> | <p>YES, THROUGH ALTERNATIVE MEANS</p> | <p>The nonderogation clause in section 8 stipulates that nothing in the Act limits or affects any authority to disclose information under another Act of Parliament or a provincial statute; however, the use and further disclosure of information are not governed by the information sharing framework of the SCISA. SCISA also says that if you have lawful authority for the culling of information, you have an exemption to the Privacy Act.</p> | |
| <p>25. That the proposed Committee of Parliamentarians conduct an immediate review of the operational evaluation of the information exchange process included in the Security of Canada Information Sharing Act.</p> | <p>N/A</p> | <p>SCISA permits a Government of Canada institution to disclose information "in respect of activities that undermine the security of Canada." The definition of those activities is broad, and the conflict between the Privacy Act and SCISA will need to be monitored. The SCISA provisions had been used approximately 50 times in the first six months after SCISA came into force, and only 3 of 17 recipient institutions are subject to independent external review.</p> | |

SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|--|--|--|
| <p>26. That the Security of Canada Information Sharing Act be amended in order to adopt a model of dual thresholds, one threshold of relevance for the disclosing institutions and a threshold of necessity and proportionality for the recipient institutions currently numbered at 17.</p> | <p>YES, THROUGH ALTERNATE MEANS</p> | <p>The Privacy Commissioner recommended dual thresholds, one for the disclosing institutions, and another for the 17 recipient institutions. The committee found that the 17 recipient departments should be responsible for selectively receiving and retaining only information that meets the higher threshold of necessity and proportionality (subject to any further limits imposed by their enabling laws), and under a positive legal obligation to return or destroy information that does not.</p> | |
| <p>27. That the Government of Canada create an office of the national security compliance commissioner to review all national security information sharing activity between and among government departments and agencies, including Canadian Security Intelligence Service and the Royal Canadian Mounted Police, to ensure compliance with the Charter of Rights and Freedoms and all Canadian law.</p> | <p>PARTIALLY ADDRESSED</p> | <p>Although SIRC said that CSIS has established a very rigorous structure in order to meet its obligations in terms of mistreatment, witnesses fear that such information sharing – without implementing a rigorous review system for all institutions – would result in new cases of abuse (similar to Maher Arar). One stakeholder recommended that the government create an office of the National Security Advisor to review all national security activity, and to ensure proper information sharing from government agencies to CSIS and the RCMP.</p> | |

s.21(1)(a)

SECU AND ETHI RECOMMENDATIONS

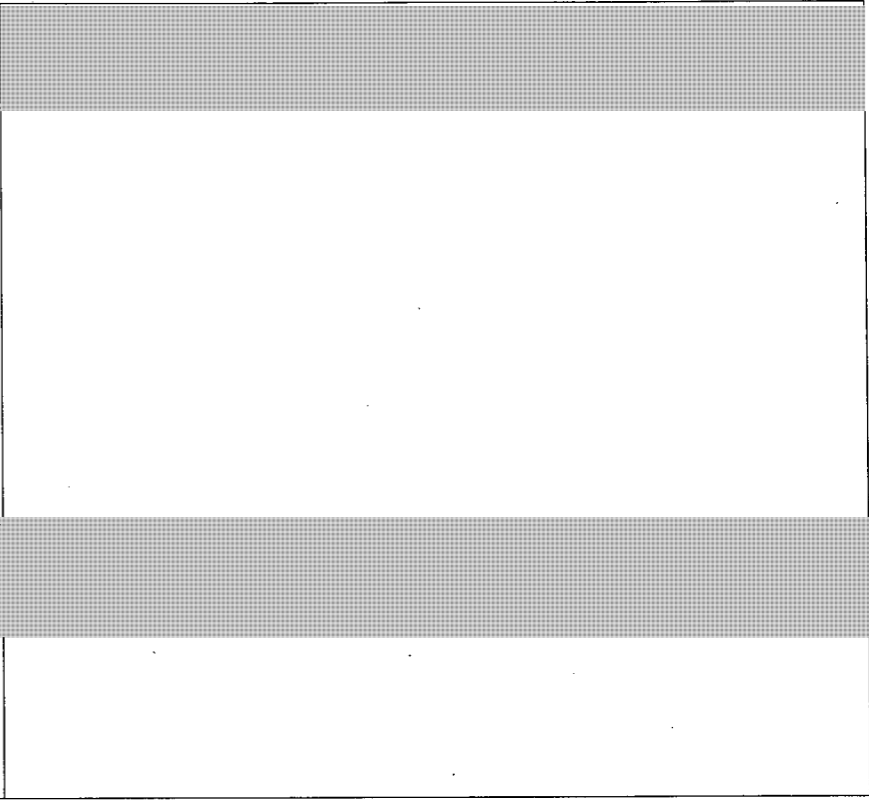
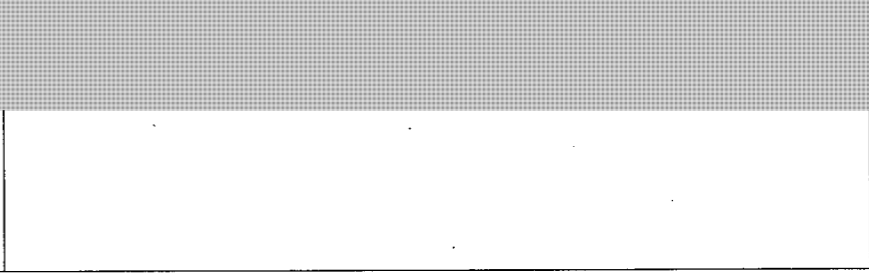
| | | | |
|---|-------------------|---|---|
| <p>28. That the Minister of Public Safety and Emergency Preparedness review the ministerial directives concerning torture to ensure that they are consistent with international law.</p> | <p>YES</p> | <p>One stakeholder recommended to the Committee that “ministerial directions on intelligence sharing and torture, which presently allow intelligence to be shared with other governments, even if it may lead to torture and which similarly allow intelligence to be received even if it may have been obtained under torture” should be withdrawn or reformed.</p> <p>Noted that “when democratic countries start to undermine this principle, it also opens the door to many other countries that are less particular in this regard.”</p> |  |
| <p>29. That sections 38 to 38.16 of the Canada Evidence Act be amended in order to repeal the two-court system for criminal cases and enable trial judges to review secret information and decide on matters of confidentiality.</p> | | | <p>Intel and evidence—under JUS portfolio</p> |
| <p>30. That the Canada Evidence Act be amended in order to allow the court to appoint, upon request or automatically, special advocates, with the necessary security clearance, who will be given access to confidential government information and will be tasked with protecting the interests of the accused and of the public in disclosure proceedings.</p> | | | <p>Intel and evidence—under JUS portfolio</p> |

s.21(1)(a)

SECU AND ETHI RECOMMENDATIONS

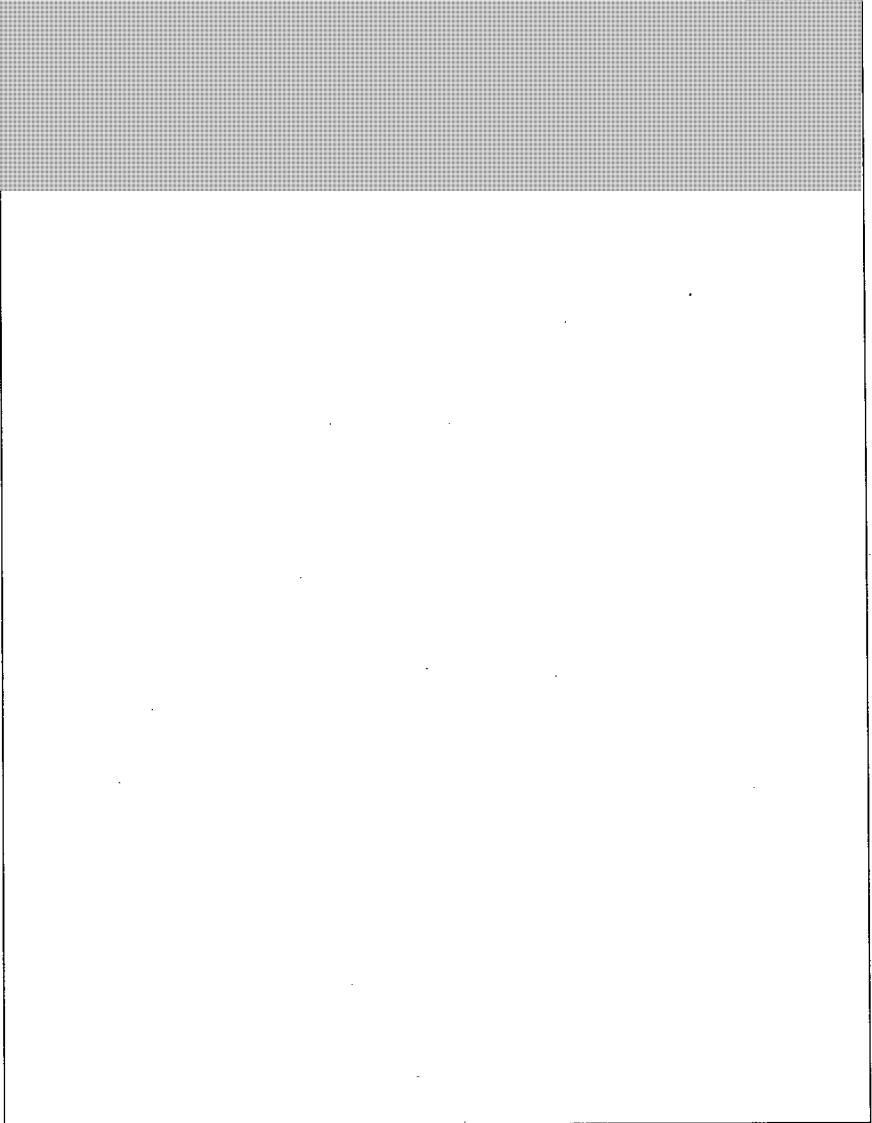
| | | | |
|--|---|---|--|
| <p>31. That sections 83(1) and 85.4(1) of the Immigration and Refugee Protection Act be amended in order to give special advocates full access to complete security certificate files.</p> | <p>NO</p> | <p>For security certificates, the ATA, 2015 allows a Federal Court judge to exempt the Minister of Public Safety from having to provide the special advocate with information that does not enable the individual to be reasonably informed of the case made by the Minister when the certificate is not based on this information and this information is not filed with the Federal Court. This may impact rights guaranteed under Section 7 of the <i>Charter</i>.</p> | |
| <p>32. That the Secure Air Travel Act be amended in order to allow an individual who has been denied air travel to confirm with the Passenger Protect Inquiries Office that they themselves are or are not on the Canadian Specified Persons List, and that they do or do not share a name with an individual on the Canadian list.</p> | <p>PARTIALLY ADDRESSED OR YES, THROUGH ALTERNATE MEANS</p> | <p>As a result of false name matches (also known as “false positives”) some individuals can be delayed in obtaining a boarding pass. The extent of the intrusion on liberty and security resulting from the operation of the Secure Air Travel Act appeal provisions is central to the consideration of whether the new provisions would engage section 7 of the <i>Charter</i>.</p> | |

SECU AND ETHI RECOMMENDATIONS







| | | | |
|--|-------------------|--|---|
| <p>33. That the Department of Public Safety and Emergency Preparedness Act be amended to provide that Public Safety Canada's annual report to Parliament include the number of individuals on the Specified Persons List.</p> | <p>NO</p> | <p>Recommendation was made by an academic stakeholder regarding a need for "fairness, openness and transparency of the appeal process." Individuals are not notified when they are put on the list and there needs to be a meaningful way to appeal. Another academic said "The federal government can tell the people on the no fly list that their problems are not the result of Canada's list. The government cannot necessarily tell people which list is being used, but they could be told that the ban is not due to the passenger protect program."</p> |  |
| <p>34. That the Government of Canada enhance the operations of the Passenger Protect Program in order to prevent false positive matches with individuals with the same or similar names.</p> | <p>YES</p> | <p>False positive matches are a concern, particularly when it comes to children who may be falsely matched with an individual on the SATA list. Individuals are not notified when they are listed. An effective system for eliminating these false positives would help ease some concerns about PPP.</p> |  |

s.21(1)(a)

SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|-----------------------------------|--|--|
| <p>35. That the Government of Canada create an expeditious redress system to assist travelers erroneously identified as a person on the Specified Persons List (known as "false positives") and that it continue to work with foreign governments in order to assist Canadians whose names appear on these governments' lists.</p> | <p>PARTIALLY ADDRESSED</p> | <p>Under SATA, a listed person may apply to the Minister of Public Safety to have their name removed from the list within 60 days after being denied transportation. The individual must be afforded a reasonable opportunity to make representations. The Minister must then decide whether reasonable grounds to maintain the applicant's name on the list continue to exist and, without delay, give the applicant notice of any decision (but not the reasons for it). If the Minister does not make a decision within 90 days, or within any further period that is agreed on by the Minister and the applicant, the Minister is deemed to have denied it.</p> <p>SATA affords a listed person the right to appeal to the Federal Court in respect of a ministerial decision to add or retain the person's name on the list. Ultimately, the judge may base a decision on information or other evidence even if a summary of that information or other evidence has not been provided to the appellant.</p> <p>The SATA does not allow for special advocates. Witnesses noted that there must be a meaningful way to appeal, and one that there would need to be "the possibility of eradicating a completely mistaken record."</p> |  |
|--|-----------------------------------|--|--|

SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|-------------------|--|---|
| <p>36. That the Secure Air Travel Act be amended in order to require the Minister of Public Safety to respond to an administrative recourse under the Act within 90 days. If the Minister does not respond within the prescribed time period, the individual will be automatically removed from the Specified Persons List.</p> | <p>YES</p> | <p>The redress system for listed individuals is in need of review. Currently, if the Minister does not respond within 90 days the individual automatically remains on the list.</p> <p>Reversing this so that the individual is de-listed if there is no response within 90 days would create more accountability over the PPP.</p> |   |
| <p>37. That the Secure Air Travel Act be amended in order to provide for the nomination of a special advocate to protect the interest of individuals who have appealed to have their name removed from Specified Persons List.</p> | <p>NO</p> | <p>Special Advocates have been used in other contexts where classified information is used as evidence in court proceedings, to protect the interests of the accused. For example, detention reviews held under IRPA Division 9. There is concern that under PPP, an individual is being denied <i>Charter</i> rights without due process.</p> |   |
| <p>38. That the Government of Canada ensure effective safeguards in the Passenger Protect Program against any unfair infringements on individuals' legitimate right to liberty, freedom of movement, privacy and protections from discrimination on the basis of national or ethnic origin, religion, sexual orientation, or any other characteristic protected by law.</p> | <p>YES</p> | <p>Stakeholders have raised concerns about the effects that a no-fly list can have on members of their communities. Those individuals are denied <i>Charter</i> rights, such as the rights to mobility and due process, without adequate safeguards or systems for redress.</p> |   |

s.21(1)(a)

SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|-------------------|---|--|
| <p>39. That at this time, and following the Supreme Court of Canada's decision in R. v. Spencer, no changes to the lawful access regime for subscriber information and encrypted information be made, but that the House of Commons Standing Committee on Public Safety and National Security continue to study such rapidly evolving technological issues related to cyber security.</p> | <p>NO</p> | <p>The Committee heard significant concerns from stakeholders about the privacy impact of potential basic subscriber information (BSI) and encryption legislation.</p> <p>Investigators are facing operational challenges due to legal gaps around access to basic subscriber information and rapidly evolving technologies, such as encryption. Further examination of these issues by SECU could assist in developing potential measures to address current challenges.</p> | |
| <p>40. That the Communications Security Establishment, in acting upon the requests of other national security agencies regarding the surveillance of private communications and the gathering and retention of metadata, work only with appropriate warrants from the agencies making such requests.</p> | <p>YES</p> | | |

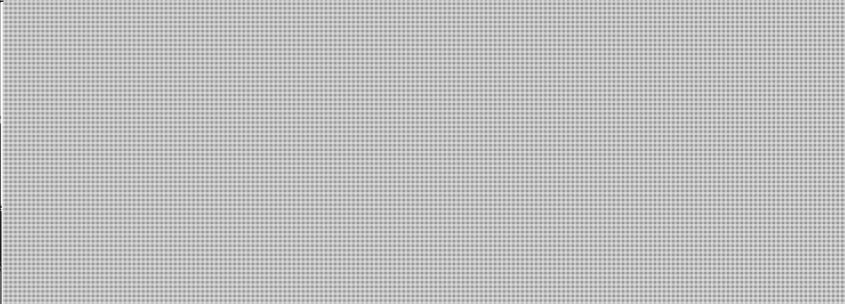
SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|--|--|---|
| <p>41. That cyber security strategies need to adopt a whole of government approach, such as the GCHQ (UK Government Communications Headquarters) approach.</p> | | | <p>The Government of Canada recently completed a Cyber Security Review as a means of taking stock of the existing measures to protect Canadians and Canadian critical infrastructure from cyber threats. The review was an opportunity to examine evolving threats in cyberspace as well as to understand and explore the ways that cyber security has become a driver of economic prosperity.</p> <p>As part of this review, the Government initiated a public consultation process that sought the views of Canadians, the private sector, academia, and other informed stakeholders on cyber security. A range of comments were submitted, including ways in which the government can best serve the needs of the private sector and Canadians.</p> <p>In addition to these consultations, an examination of the current cyber security strategies of international partners was conducted, in order to identify lessons learned and common practices. Internal discussions on important policy issues, operational issues and how government should better organize itself to deliver on its cyber security mandate also took place. Results of the external consultations and the various internal discussions will inform how Government should position itself to delivery policy and programs that will best support a cyber security strategy that is tailored to the needs of our nation.</p> |
|--|--|--|---|

s.21(1)(a)

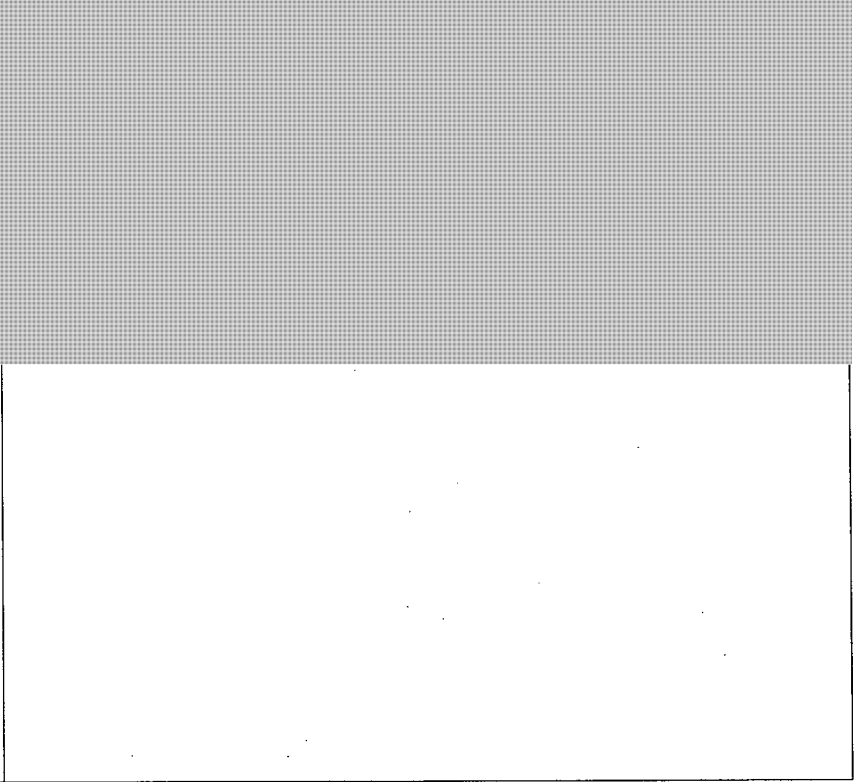
SECU AND ETHI RECOMMENDATIONS

ETHI RECOMMENDATIONS

| Recommendation | Addressed? | Context | Reasoning |
|---|---|---|---|
| <p>1. That the Government of Canada further study which recipient institutions should be, listed in Scheduled 3 to SCISA to insure that only institutions directly relevant to Canada's national security framework are listed.</p> | <p>YES (THROUGH NON- LEGISLATIVE MEASURES)</p> | <p>Concerns have been raised that the list of designated recipient institutions, consisting of 17 departments and agencies, some with unapparent national security responsibilities and jurisdictions, is too extensive.</p> <p>All listed institutions have a national security jurisdiction or responsibility and submitted an application outlining such, which was approved by the Privy Council Office, Machinery of Government Secretariat.</p> |  |
| <p>2. That the government of Canada amended Schedule 3 to SCISA to list not only the names of potential recipient institutions and their designated heads, but also specific sections of the statutes administered or implemented by those institutions that may conceivably relate to national security concerns.</p> | <p>YES</p> | <p>See above</p> | <p>See above</p> |

s.21(1)(a)

SECU AND ETHI RECOMMENDATIONS

| | | | |
|---|--|--|---|
| <p>3. That the Government of Canada repeal the definition of 'activity that undermines the security of Canada' in section 2 of the SCISA and replace it with a narrower definition such as the definition of 'threats to the security of Canada' in the Canadian Intelligence Security Act.</p> | <p>YES, THROUGH ALTERNATIVE MEANS</p> | <p>The definition of "activity that undermines the security of Canada" identifies which national security-compromising activities fall within the scope of the SCISA and accompanying scope of departmental responsibilities that information can be shared for.</p> <p>"Activity that undermines the security of Canada" is currently defined as any activity that undermines Canada's sovereignty, security, or territorial integrity or the lives or the security of the people of Canada". This core part of the definition has been referred to as the "chapeau" of the definition.</p> <p>The illustrative examples in the definition are activities that <u>could</u> be activities that undermine the security of Canada <u>if</u> the specific instance of the example meets the chapeau threshold (i.e., it undermines "Canada's sovereignty, security, or territorial integrity or the lives or the security of the people of Canada").</p> |  |
|---|--|--|---|


s.21(1)(a)

SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|--|--|--|
| <p>4. That the Government of Canada amend subsection 5(1) of SCISA so that any sharing of information under the Act would have to meet the standard of necessity and proportionality.</p> | <p>YES, THROUGH ALTERNATIVE MEANS</p> | <p>Concerns have been raised that the threshold of “relevant” in the SCISA is too low of a standard for disclosure, given the sensitivity of the information being shared.</p> | |
| <p>5. That the Government of Canada amend SCISA: a. To clarify the Privacy Act takes precedence over SCISA b. to stipulate that the Privacy Act continues to apply to all personal information disclosed pursuant to SCISA</p> | <p>YES, THROUGH ALTERNATIVE MEANS</p> | <p>The SCISA does not explicitly state that the statutory restrictions or prohibitions outlined in the <i>Privacy Act</i> continue to apply regardless of the SCISA’s existence.</p> | |

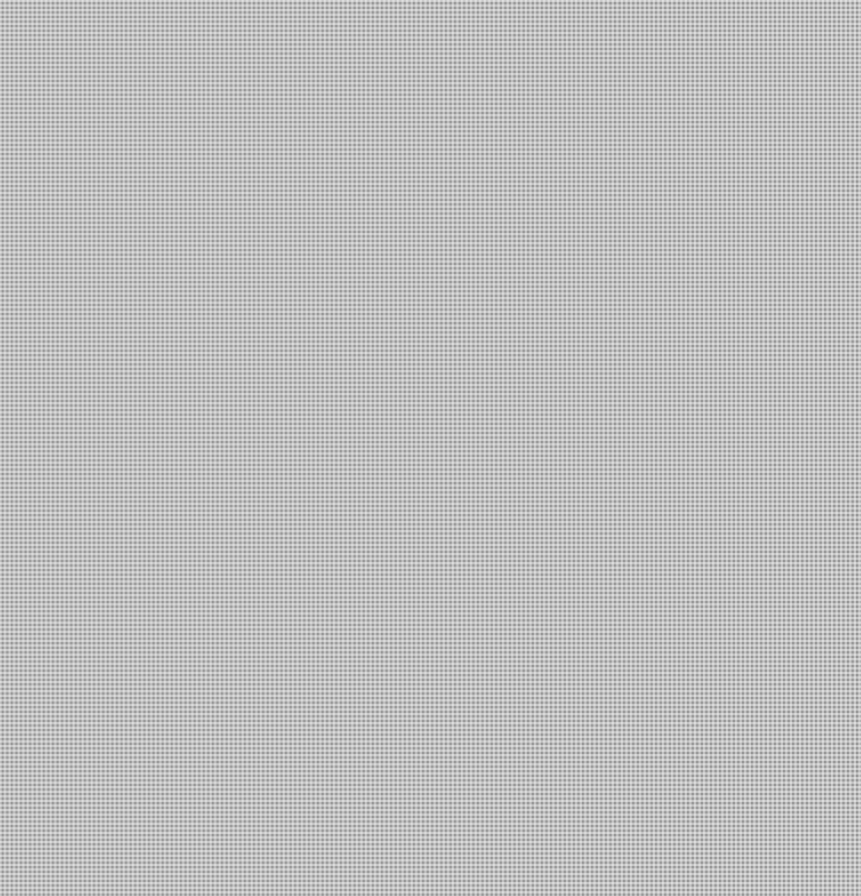
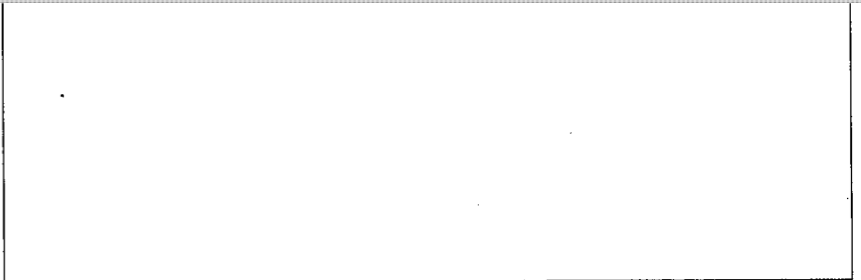
s.21(1)(a)

SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|--|---|---|
| <p>6. That the Government of Canada amend section 5 of SCISA to clearly stipulate that the recipient institution must respect its mandate and current legislative and collection powers.</p> | <p>YES, PARTIALLY ADDRESSED</p> | <p>Similar to above, the SCISA does not explicitly state that existing statutory requirements or authorities are to be upheld during the information sharing process.</p> |  |
|--|--|---|---|

s.21(1)(a)

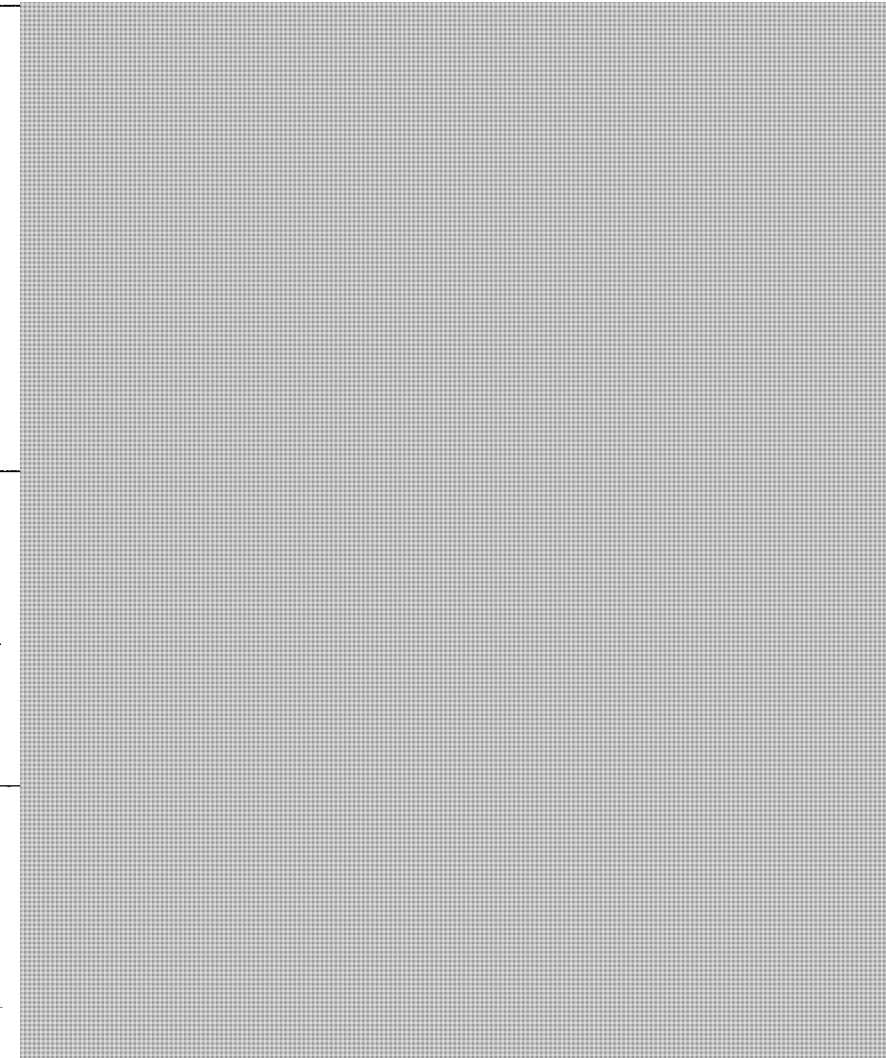
SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|--|--|---|
| <p>7. The Government of Canada strengthen the oversight of information sharing by GoC institutions, by considering the following options:</p> <p>a) establish a super-agency top provide expert oversight that would review all information-sharing activities by federal national security institutions;</p> <p>b) establishing new oversight bodies, where there are existing gaps, such as the CBSA, capable of cooperating to review information sharing between federal institutions pursuant to SCISA.</p> <p>c) conferring new powers upon the Security Intelligence Review Committee, the Office of the Communications Security Establishment Commissioner, the Civilian Review and Complaints Commission for the RCMP, and the Privacy Commissioner that would enable them to:</p> <p>i. oversee information sharing among the 14 GoC institutions listed in Schedule 3 to SCISA as well as their use of information; and</p> <p>ii. cooperate with other agencies and conduct joint investigations;</p> <p>d) establishing a parliamentary review mechanism that, on a complementary basis with one or several other expert oversight agencies, would review the information-sharing activities of federal national security institutions;</p> | <p>YES, THROUGH ALTERNATIVE MEANS</p> | <p>The SCISA does not address oversight or review of disclosures, however, through other amendments related to former Bill C-51, oversight and review may be address under Bill C-22 or other current proposals regarding review bodies.</p> |   |
|--|--|--|---|

s.21(1)(a)

SECU AND ETHI RECOMMENDATIONS

| | | |
|---|--|--|
| <p>8. That the Government of Canada amend the SCISA to impose on federal institutions and on the recipient institutions listed in Schedule 3 in order to report on any use of subsequent sharing of information to them under the Act.</p> | <p>YES, THROUGH ALTERNATIVE MEANS</p> | <p>The SCISA does not require federal institutions to report or keep records on information exchanges (either disclosure or collection) under the SCISA.</p> |
| <p>9. That the Government of Canada amend SCISA in order that the guiding principles listed in section 4 become legal obligations.</p> | <p>NO</p> | <p>There is no binding provision in SCISA to protect the privacy of Canadians, suggested a number of privacy safeguards, focusing on information reliability, information sharing-agreements, privacy impact assessments (PIAs), and the retention and deletion of personal info. Current guidelines are not binding, suggest implementing mechanisms to enforce them.</p> |
| <p>10. That the Government of Canada amend SCISA by creating a legal obligation to ensure the reliability of any shared information.</p> | <p>YES, THROUGH ALTERNATIVE MEANS</p> | <p>Neither reliability nor accuracy of the information being disclosed is addressed through the existing provisions of the SCISA or as part of the threshold for disclosure.</p> |



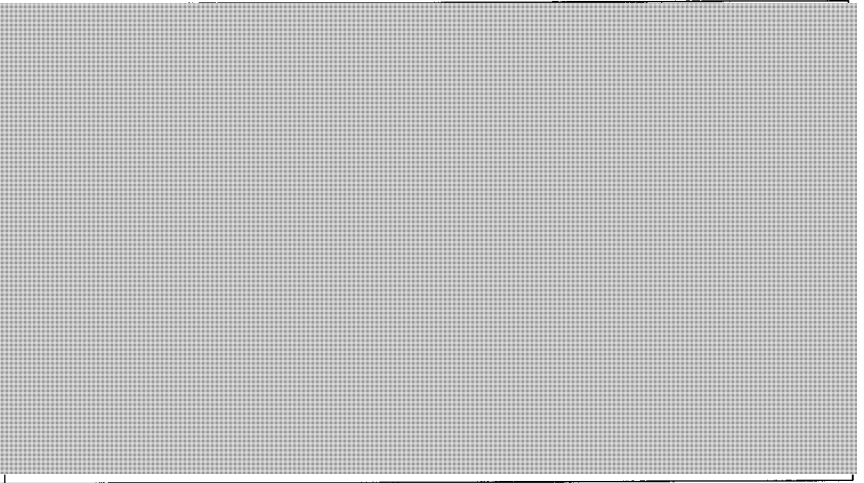
s.21(1)(a)

SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|--|---|--|
| <p>11. The Government of Canada amend section 10 of SCISA to confer upon the Governor in Council the power to make regulations concerning the correction and deletion of information and that the Governor in Council make regulations regarding the correction, deletion and retention of information.</p> | <p>YES PARTIALLY ADDRESSED</p> | <p>Similar to reporting, the SCISA does not address further aspects of the information sharing process, such as correction, deletion or retention of information.</p> | |
| <p>12. That the Government of Canada amend SCISA so as to:</p> <p>a) Make is a duty for the recipient institutions to enter into information sharing arrangements with disclosing institutions.</p> <p>b) Conform upon the Privacy Commissioner of Canada the power to review and comment on all existing or future information sharing arrangements.</p> | <p>NO, ALTERNATIVE SOLUTION</p> | <p>Given the sensitivity of the information being shared, additional rigour around the information sharing process is being requested since the SCISA only addresses disclosure and no other aspect of the information sharing process. There is no requirement to track, record or report on any disclosure current, which has been identified as a source of concern.</p> | |
| <p>13. That the government of Canada amend section 9 of the SCISA to make it clear and unequivocal that:</p> <p>a) Only employees acting in good faith in the performance of their duties are immune from civil proceedings; and</p> <p>b) The Crown remains liable for the actions of its employees</p> | <p>YES, THROUGH ALTERNATIVE MEANS</p> | <p>Clarify that should information not be shared in good faith, the Crown would be liable for the actions of its employees.</p> | |

s.21(1)(a)

SECU AND ETHI RECOMMENDATIONS

| | | | |
|--|------------------|--|---|
| <p>14. That the Government of Canada implement recommendation 10 made by the Commission of Inquiry into the Air India tragedy by CSIS Act to require CSIS to report information that may be used in an investigation or prosecution of an offence either to the relevant policing or prosecutorial authorities or to the national security advisor.</p> | <p>NO</p> | <p>Concern that SCISA fails to implement a key recommendation of Commission on Air India Flight 182, the consequences when not enough information is shared, 'intelligence to evidence' conundrum.</p> |  |
|--|------------------|--|---|

ETHI Recommendations



BUILDING A **SAFE AND RESILIENT CANADA**

- 1 That the Government of Canada further study which recipient institutions should be listed in Schedule 3 to the SCISA to ensure that only institutions directly relevant to Canada's national security framework are listed.
- 2 That the Government of Canada amend Schedule 3 to the SCISA to list not only the name of potential recipient institutions and their designated heads, but also the specific sections of the statutes administered or implemented by those institutions that may conceivably relate to national security concern.
- 3 That the Government of Canada repeal the definition of "activity that undermines the security of Canada" in section 2 of SCISA and replace it with a narrower definition such as the definition of "threats to the security of Canada" in the *CSIS Act*.
- 4 That the Government of Canada amend subsection 5(1) of SCISA so that any sharing of information under the Act would have to meet the standard of necessity and proportionality.
- 5 That the Government of Canada amend SCISA:
 - To clarify that the *Privacy Act* takes precedence over SCISA.
 - To stipulate that the *Privacy Act* continues to apply to all personal information disclosed pursuant to the SCISA.
- 6 That the Government of Canada amend section 5 of the SCISA to clearly stipulate that the recipient institution must respect its mandate and current legislative and collection powers.

Legend:

Red = not addressed

Non-red = partially or fully addressed, or alternative solution



ETHI Recommendations

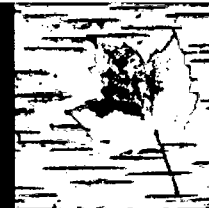


BUILDING A **SAFE AND RESILIENT CANADA**

- 7 That the Government of Canada strengthen the oversight of information sharing by Government of Canada institutions, by considering the following options:
 - Establishing a super-agency to provide expert oversight that would review all information-sharing activities by federal security institutions.
 - Establishing new oversight bodies, where there are existing gaps, such as the Canada Border Services Agency, capable of cooperating to review information sharing between federal institutions pursuant to SCISA.
 - Conferring new powers upon the Security Intelligence Review Committee, the Office of the Communications Security Establishment Commissioner, the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police, and the Privacy Commissioner of Canada that would enable them to:
 - Oversee information sharing among the 14 Government of Canada institutions listed in Schedule 3 to the SCISA as well as their use of information; and
 - Cooperate with other agencies and conduct joint investigations;
 - Establishing a parliamentary review mechanism that, on a complementary basis with one or several other expert oversight agencies, would review the information-sharing activities of federal national security institutions.
 - Conferring upon the Privacy Commission of Canada the role of overseeing the information sharing of the 14 Government of Canada institutions listed in Schedule 3 to the SCISA as well as their use of information, and that the Privacy Commissioner report his or her findings to Parliament
- 8 That the Government of Canada amend SCISA to impose on federal institutions and on the recipient institutions listed in Schedule 3 of the Act a legal duty to keep records in order to report on any use or subsequent sharing of information provided to them under the Act.
- 9 That the Government of Canada amend SCISA in order that the guiding principles listing in section 4 become legal obligations.
- 10 That the Government of Canada amend SCISA by creating a legal obligation to ensure the reliability of any shared information.



ETHI Recommendations



BUILDING A **SAFE AND RESILIENT CANADA**

- 11 That the Government of Canada amend section 10 of SCISA to confer upon the Governor in Council the power to make regulations concerning the correction and deletion of information and that the Governor in Council make regulations regarding the correction, deletion and retention of information.
- 12 That the Government of Canada amend the SCISA so as to:
 - Make it a duty for recipient institutions to enter into information-sharing arrangements with disclosing institutions; and,
 - Confer upon the Privacy Commissioner of Canada the power to review and comment on all existing or future information-sharing arrangements.
- 13 That the Government of Canada amend section 9 of the SCISA to make it clear and unequivocal that:
 - Only employees acting in good faith in the performance of their duties are immune from civil proceedings; and
 - The Crown remains liable for the actions of its employees.
- 14 That the Government of Canada implement recommendation 10 by the Commission of Inquiry into the Air India tragedy by amending the *CS/S Act* to require CSIS to report information that may be used in an investigation or prosecution of an offence either to the relevant policing or prosecutorial authorities or to that national security advisor.



SECU Recommendations



BUILDING A **SAFE AND RESILIENT CANADA**

- 1 That the *Department of Public Safety and Emergency Preparedness Act* be amended to require the publication of the Public Report on the Terrorist Threat to Canada, and specifically include: 1) performance indicators, 2) data information sharing as it related to the *Security of Canada Information Sharing Act* (SCISA), and 3) the obligation that it be annually tabled in Parliament.
- 2 That the Government of Canada increase funding for long-term research as well as the development of professional expertise, both within government and outside government, to understand and address new and evolving threats to national security.
- 3 That Public Safety develop a community-based strategy for the prevention of radicalization to violence based on research data and focusing on best local practices. It should include programs for the empowering of youth and women, inclusion of marginalized persons and groups, and broad community educational activities.
- 4 That counter-radicalization programs continue and expand efforts to stop groups that promote radicalization from gaining a foothold to spread their message of violence, or the precursors to violence.
- 5 That the Government of Canada increase its contribution to and promote the Communities at Risk: Security Infrastructure Program to help communities at risk of hate-motivated crimes improve their security infrastructure.
- 6 That the Government of Canada recognize that establishing a national security intelligence committee of parliamentarians is a first step toward increasing the transparency and accountability of security agencies and that other mechanisms must be considered in order to restore Canadians' trust in those agencies.
- 7 That the Government of Canada create an independent and external review body for the operations of the Canada Border Service Agency.
- 8 That the Government of Canada establish statutory gateways among all national public safety and national security review bodies in order to provide for the appropriate exchange of information, referral of investigations, conduct of joint investigations and coordination in the preparation of reports.



SECU Recommendations



BUILDING A **SAFE AND RESILIENT CANADA**

- 9 That the Government of Canada increase funding of all public safety and national security review bodies to enable them to carry out their mandates effectively, matching the increase in activities of the agencies they oversee and to ensure the protection of Canadians' rights and freedoms.
- 10 That the Government of Canada establish a national security review office as the integrated review body for the bodies inside the government that have a national security mandate that are currently without a review body and that the national security review office act as a coordinating committee for the existing national security review bodies. That national security review office should have the following mandate:
 - To ensure that the statutory review gateways among the independent review bodies operate effectively;
 - To take steps to avoid duplicative reviews;
 - To provide a centralized intake mechanism for complaints regarding the national security activities of federal entities;
 - To report on accountability issues relating to practices and trends in the area of national security in Canada, including the effects of those practices and trends on human rights and freedoms;
 - To conduct formal public information programs;
 - To initiate discussion for co-operative review with independent review bodies for provincial and municipal police forces involved in national security activities.
- 11 That the reference to the *Canadian Charter of Rights and Freedoms* in section 12.1(3) of the *CSIS Act* be repealed in order to remove the ability to violate the *Charter*.
- 12 That before the CSIS engage in disruptive powers, the agency exhaust all other non-disruptive means of reducing threats.
- 13 That the Government of Canada ensure section 12.1 of the *CSIS Act* requires that all disruption activities that violate Canadian law necessitate a warrant and that the Minister's approval be obtained prior to the activity under section 21.1 of the *CSIS Act*.
- 14 That the *CSIS Act* be amended in order to include a quarterly report in disruption activities for the Committee of Parliamentarians.



SECU Recommendations



BUILDING A **SAFE AND RESILIENT CANADA**

- 15 That the Government of Canada ensure that CSIS respects the traditional distinction between intelligence gathering and police disruptive operations by working in concert with the RCMP and other police forces to assist in their investigations and the exercise of their disruptive powers, and no duplicate such investigations or powers.
- 16 That the Government of Canada restrict preventative detention to only exceptional, narrowly defined circumstances, and ensure conditions of those detained comply with Canadian and international standards on detention and due process.
- 17 That the Government of Canada study other measures that could be used instead of preventive detention.
- 18 That sections 83.3(2) and 83.3(4) of the *Criminal Code* be amended in order to remove the wording “may be” and “is likely to” applicable to recognizance with conditions and to replace them with the “balance of probabilities” concept.
- 19 That section 83.221 of the *Criminal Code* be amended in order to clarify the concept of “terrorism offences in general” and to consider replacing it with “terrorism offences”, as defined in section 2 of the *Criminal Code*. Furthermore, the Government of Canada should consider applicable defences modeled after those in section 319(3) of the *Criminal Code* that prohibit the wilful promotion of hatred and contain a number truth and fair comment defences.
- 20 That the Government of Canada ensure no Canadian is restricted from the legitimate exercise of their right to freedom of expression and freedom of association, and that it remove any provisions in current legislation that may be in contravention to the *Charter of Rights and Freedoms* or restrict the legitimate exercise of rights, particularly those of journalists, protesters, non-governmental organizations and environmental and Indigenous activists.
- 21 That the definition of “terrorist propaganda” in section 83.222(8) of the *Criminal Code* be amended in order to be limited to material that counsels the commission of a terrorist offence or that instructs the commission of a terrorist offence.



SECU Recommendations



BUILDING A **SAFE AND RESILIENT CANADA**

- 22 That the scope of activities subject to information sharing under the SCISA be narrowed so as to be consistent with all other national security legislation.
- 23 That the Government of Canada change the definition of "activity that undermines the security of Canada" and revise the list of activities enumerated in section 2 of the SCISA in order to ensure that basic civil liberties such as freedom of expression, freedom of association and freedom of peaceful assembly are upheld.
- 24 That the Government of Canada ensure that protections guaranteed under the *Privacy Act* are not abrogated by the SCISA, thus ensuring Canadians' privacy is protected.
- 25 That the proposed Committee of Parliamentarians conduct an immediate review of the operational evaluation of the information exchange process included in the SCISA.
- 26 That the SCISA be amended in order to adopt a model of dual thresholds, one threshold of relevance for the disclosing institutions and a threshold of necessity and proportionality for the recipient institutions currently numbered at 17.
- 27 That the Government of Canada create an office of the national security compliance commissioner to review all national security information sharing activity between and among government departments and agencies, including CSIS and the RCMP, to ensure compliance with the *Charter of Rights and Freedoms* and all Canadian law.
- 28 That the Minister of Public Safety and Emergency Preparedness review the ministerial directives concerning torture to ensure that they are consistent with international law.
- 29 That sections 38 to 38.16 of the *Canada Evidence Act* be amended in order to repeal the two-court system for criminal cases and enable trial judges to review secret information and decide on matters of confidentiality.



SECU Recommendations



BUILDING A **SAFE AND RESILIENT CANADA**

- 30 That the *Canada Evidence Act* be amended in order to allow the court to appoint, upon request, or automatically, special advocates, with the necessary security clearance, who will be given access to confidential government information and will be tasked with protecting the interests of the accused and of the public in disclosure proceedings.
- 31 That sections 81(1) and 85.4(1) of the *Immigration and Refugee Protection Act* be amended in order to give special advocates full access to complete security certificate files.
- 32 That the *Secure Air Travel Act* be amended in order to allow an individual who has been denied air travel to confirm with the Passenger Protect Inquiries Office that they themselves are or are not on the Canadian Specified Persons List, and that they do or do not share a name with an individual on the Canadian list.
- 33 That the *Department of Public Safety and Emergency Preparedness Act* be amended to provide that Public Safety Canada's annual report to Parliament include the number of individuals on the Specified Persons List.
- 34 That the Government of Canada enhance the operations of the Passenger Protect Program in order to prevent false positive matches with individuals with the same or similar names.
- 35 That the Government of Canada create an expeditious redress system to assist travelers erroneously identified as a person on the Specified Persons List (known as "false positives") and that it continue to work with foreign government in order to assist Canadians whose names appear on these governments' lists.
- 36 That the *Secure Air Travel Act* be amended in order to require the Minister of Public Safety to respond to an administrative recourse under the Act with 90 days. If the Minister does not respond within the prescribed time period, the individual will be automatically removed from the Specified Persons List.
- 37 That the *Secure Air Travel Act* be amended in order to provide for the nomination of a special advocate to protect the interest of individuals who have appealed to have their name removed from the Specified Persons List.



SECU Recommendations



BUILDING A **SAFE AND RESILIENT CANADA**

- 38 That the Government of Canada ensure effective safeguards in the Passenger Protection Program against any unfair infringements on individuals' legitimate right to liberty, freedom of movement, privacy and protections from discrimination on the basis of national or ethnic origin, religion, sexual orientation, or any other characteristic protected by law.
- 39 That at this time, and following the Supreme Court of Canada's decision in *R. v. Spencer*, no changes in the lawful access regime for subscriber information and encrypted information be made, but that the House of Commons Standing Committee on Public Safety and National Security continue to study such rapidly evolving technological issues related to cyber security.
- 40 That the Communications Security Establishment, in acting upon the requests of other national security agencies regarding the surveillance of private communications and the gathering and retention of metadata, work only with appropriate warrants from the agencies making such requests.
- 41 That cyber security strategies need to adopt a whole of government approach, such as the GCHQ (UK Government Communications Headquarters) approach.



Our Security, Our Rights

National Security Green Paper, 2016

Background Document



This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.



Government
of Canada

Gouvernement
du Canada

Canada

© Her Majesty the Queen in Right of Canada, 2016

Cat. No.: PS4-204/2016E-PDF
ISBN: 978-0-660-06306-5

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Our Security, Our Rights: National Security Green Paper, 2016

BACKGROUND DOCUMENT

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

CONTENTS

| | |
|---|----|
| Introduction | 5 |
| Accountability | 9 |
| Prevention..... | 15 |
| Threat Reduction | 21 |
| Domestic National Security Information Sharing..... | 26 |
| The Passenger Protect Program | 33 |
| <i>Criminal Code</i> Terrorism Measures..... | 38 |
| Procedures for Listing Terrorist Entities | 47 |
| Terrorist Financing | 51 |
| Investigative Capabilities in a Digital World | 55 |
| Intelligence and Evidence | 65 |
| Conclusion | 72 |
| Annex – Diagram of Scenario Characters..... | 73 |

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

INTRODUCTION

Setting the Scene

Canada has long dealt with terrorism threats from a diverse set of groups. Some threats resulted in tragic terrorist attacks. For example, a terrorist bomb exploded aboard Air India Flight 182 in 1985, killing 329 passengers and crew. In a related incident, a second bomb exploded at Narita airport in Japan, killing two more individuals. This remains the worst terrorist attack in Canadian history.

Following the September 11, 2001 attacks in the United States (U.S.), Canada enacted the *Anti-terrorism Act*. The Act recognized the unique nature of terrorism and created offences addressing specific aspects of terrorism. These offences included contributing to the activities of a terrorist group, instructing someone to carry out a terrorist activity, and harbouring a terrorist.

Since 2001, threats to Canadian and international security have continued to evolve. Groups inspired by al-Qaida have emerged in many parts of the world. In early 2014, one of these groups, al-Qaida in Iraq, severed ties with al-Qaida and emerged anew as the Islamic State of Iraq and the Levant (ISIL). What has been referred to as ISIL will be referred to as Daesh in this document. Since the start of the Syrian conflict in 2011, many Canadians have travelled to Syria and Iraq to join Daesh's predecessor and then Daesh itself. Daesh's declaration of a "caliphate" led to even more of these "extremist travellers" from Canada joining Daesh abroad. Some later returned to Canada, leaving trained and connected terrorist actors in our presence. The return of travellers can result in the presence of trained and connected terrorist actors within Canada.

Extremist narratives have also inspired some Canadians to plot and pursue attacks. Sometimes their targets are domestic, such as the 2014 attacks in Ottawa and Saint-Jean-sur-Richelieu. Other times, their targets are outside Canada, such as the Algerian gas plant attacked by terrorists, including two Canadians, in 2013.

The Minister of Public Safety and Emergency Preparedness recently released the *2016 Public Report on the Terrorist Threat to Canada*. The Report noted that the principal terrorist threat to Canada remains that posed by violent extremists who could be inspired to carry out an attack within Canada. Violent extremist ideologies espoused by terrorist groups like Daesh and al-Qaida continue to appeal to certain individuals in Canada.

Both the threat of terrorism and the counter-terrorism tools we use to respond have evolved over the years. However, there has been one constant imperative from the Government of Canada's perspective. That is to ensure that any actions by the Government respect Canadian values, including the rights and freedoms guaranteed by the *Charter*, as well as equality and multiculturalism.

National security institutions in Canada are professional, responsible and effective in the work they do. They work within a well-defined set of legal authorities and respect Canadian law. Their core

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

duty is to keep Canadians safe—and they do so daily. National security institutions in Canada are subject to measures that make them accountable. These accountability measures ensure that these institutions are acting within the law and are being effective. Accountability for national security institutions is, therefore, an important part of any discussion on national security, as it offers protections and safeguards.

The Government is aware that its actions in security matters can impact rights. In protecting national security, the Government must find an appropriate balance between the actions it takes to keep Canadians safe and the impact of those actions on the rights we cherish. The question is: what is an appropriate and reasonable impact?

The Canadian public, stakeholders, experts and those in government institutions will have a variety of views on what constitutes an appropriate balance. Canadians rightly expect strong justifications to limits their rights. This means that we must look at measures to protect national security to see whether they are effective, if there are potential alternatives and if they have properly taken into account the rights they affect.

Human Rights

Canada is founded upon the rule of law, of which the Constitution is the “supreme law.” This means that all laws enacted by Parliament and all actions taken by the Government of Canada must be consistent with the Constitution, which includes the *Charter*. The *Charter* reflects our basic values and guarantees our fundamental rights and freedoms, including freedom of expression and association, and the rights to equality, privacy, and the presumption of innocence. The purpose of the *Charter* is to ensure that we are governed in accordance with our basic values. Any laws of Parliament and actions of government that are inconsistent with the *Charter* are unconstitutional and can be declared so by the courts.

The rights and freedoms guaranteed in the *Charter* are not absolute. They can be limited in accordance with the law, if justifiable. Justifiable limitations are generally those that pursue important objectives and that impact rights or freedoms as little as reasonably possible in the circumstances. Also, limitations are only justifiable if, overall, the benefits from these limitations outweigh the harm to the right.

This concern for balance is acutely important in the national security context, where *Charter* rights and freedoms regularly come into play. Measures to protect national security are aimed at fulfilling the Government's primary mandate, which is to safeguard the people, institutions and values of Canada. Preserving national security includes protecting what defines Canada, including democracy, multiculturalism, and respect for the rule of law and fundamental rights and freedoms.

The *Charter* establishes a minimum standard of conduct by governments in Canada. Governments are free to produce legislation or policies, or carry out activities, that give greater protection to rights

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

and freedoms than the *Charter* requires. In some cases, the appropriate balance between national security concerns and *Charter* rights may result in greater protection. The Government is interested in the views of Canadians about when it may be appropriate in national security matters to give greater protection to rights and freedoms than that required by the *Charter*.

Privacy

In recent years, many countries have experienced high-profile public controversies about privacy impacts of national security activities.

It is difficult to hold an informed public debate about whether privacy impacts are appropriate. In part, this is because revealing some details about national security operations can undermine their effectiveness.

That said, effective and sustainable anti-terrorism measures should reflect a robust democratic consensus, at least at the level of principles. In matters involving privacy in particular, it might not be enough to achieve that consensus if anti-terrorism activities merely satisfy the minimum constitutional and legal standards. The Government is interested in the views of Canadians to help determine where the consensus lies.

Consultation Process

How best to respond to terrorism while protecting rights and freedoms is a highly complex issue. As the Government examines possible changes to Canada's counter-terrorism framework, it is asking Canadians to become active partners in finding an appropriate balance between security and rights. These consultations will help the Government develop more informed policies in this complex area.

Each chapter of this background document provides information on applicable laws, issues, challenges and potential impacts on rights in the counter-terrorism context. It contains hypothetical scenarios to better illustrate the concepts being presented.

All Canadians are invited to respond online at Canada.ca/national-security-consultation to the issues raised in the Green Paper and this background document. Responses will be accepted until December 1, 2016.

The Government will consider the responses and use them to help develop any new laws and policies. The Government will also keep Canadians up to date on the progress of consultations.

Hypothetical scenarios will be presented throughout this document to illustrate issues. The roles of the characters used in these scenarios are set out in the Annex.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Our main scenario starts as follows...

Mr. A is a charismatic speaker who holds weekly meetings in a local community centre. He has strong views on social and political issues. He invites individuals with similar interests to attend. Some of these individuals have become friends with each other, and with Mr. A. They are also his most devoted followers.

Mr. A believes that things in Canada need to change. He is looking for people who are willing to get involved and make this happen. Over time, his calls for political and social change start taking on a more violent tone.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

ACCOUNTABILITY

Some government agencies have unique intelligence collection and enforcement powers to protect national security. They must exercise these powers according to specific laws and in a manner consistent with the *Charter*. These powers are potentially intrusive, and can impact rights and freedoms. For this reason, these powers must be exercised with great care.

Much work of these agencies occurs in secret. This is because the public disclosure of sensitive information could harm national security by putting investigations, sources of information and investigative techniques at risk. As a result, effective accountability mechanisms are key to maintaining the public's trust in these agencies. Accountability mechanisms provide assurance that agencies act responsibly, strictly within the law and with respect for Canadians' rights and freedoms.

Ministerial Oversight

The Minister of Public Safety and Emergency Preparedness and the Minister of National Defence have important responsibilities with regard to the national security and intelligence agencies in their respective portfolios.

The Minister of Public Safety and Emergency Preparedness is responsible for three national security agencies: the Canada Border Services Agency (CBSA), CSIS and the Royal Canadian Mounted Police (RCMP). The Minister is also responsible for Public Safety Canada.

The Minister of National Defence is responsible for the Communications Security Establishment (CSE), the Department of National Defence (DND) and the Canadian Armed Forces (CAF).

The Ministers are accountable to Parliament for the activities of their respective agencies.

If the activities of CSE or of CSIS employees are believed to have contravened the law, the minister responsible for the relevant agency is engaged and the Attorney General of Canada is informed.¹

Ministers can issue formal directions that establish guidelines on the conduct and management of operations, although the principle of police independence limits direct ministerial involvement in day-to-day law enforcement operations. Ministerial Directions (MDs) may also specify reporting requirements and procedures for obtaining approval for agency activities.

A number of MDs are currently in effect for the CBSA, CSE, CSIS and the RCMP. For example, in 2015, CSIS was issued wide-ranging new MD on operations and accountability. The RCMP is also

¹ In the case of CSE, it is the CSE Commissioner who informs the Minister and Attorney General of Canada. Reports to the Attorney General of Canada about CSIS employees must also be provided to the Security Intelligence Review Committee.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

subject to several MDs that provide guidance on aspects of national security investigations related to sensitive sectors, accountability, and cooperation. MDs on information sharing with foreign entities have also been issued to the CBSA, CSE, CSIS and the RCMP. These MDs established a consistent process for deciding whether to share information with foreign entities where there may be a risk of mistreatment stemming from the sharing of information, in accordance with Canada's laws and legal obligations.

The Judiciary

Courts are involved in national security matters in several ways. Judges decide whether to issue warrants for CSIS and law enforcement agencies to use intrusive powers when investigating threats. Judges ensure that agencies meet the legal requirements to obtain warrants and that the warrants comply with the *Charter*. Judges also have the discretion to include in warrants any terms and conditions that are advisable in the public interest. For example, a judge might limit how long a government institution can keep the information it obtains.

More generally, judges decide whether activities leading to an individual's arrest and criminal prosecution are justifiable and proper. For example, judges examine whether investigators respected constitutional rights during investigations and whether evidence was properly collected and should be admitted at trial. Judges also have the authority to provide remedies to citizens who show law enforcement misconduct.

The Federal Court may also hear applications for judicial review of administrative decisions made by the Government in national security matters. Judicial review is a process by which the courts ensure that government decisions were fair and complied with the law. For example, the Court could review decisions made under national security programs such as the Passenger Protect Program.

Independent Review

Canada has a long-standing system of independent, non-partisan bodies reviewing the activities of certain agencies that deal with national security matters. Review bodies operate at arm's-length from government. Their main task is to ensure that national security and intelligence agencies comply with the law and MDs.

At present, there are three such bodies:

- the Civilian Review and Complaints Commission (CRCC), responsible for reviewing RCMP activities;
- the Security Intelligence Review Committee (SIRC), responsible for reviewing CSIS activities; and

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

- the Office of the Communications Security Establishment Commissioner (OCSEC), responsible for reviewing CSE activities.

Governor-in-Council (Cabinet) appointees head the CRCC and SIRC. The Governor-in-Council appoints a supernumerary judge or retired judge of a superior court to head OCSEC. Each review body has an independent research staff and legal counsel to help it.

All three review bodies have a mandate to review the activities of, and hear complaints against, the particular agency for which they are responsible. They have access to information held by the agency. Each review body produces a public report every year summarizing its activities, including findings and recommendations from reviews and complaints.

The authority of these three review bodies does not extend beyond the specific agency for which each review body is responsible. As a result, review bodies do not share classified information with each other or conduct joint reviews of national security and intelligence activities.

Parliament

Parliament has several roles in national security matters. It holds ministers to account for the actions of the institutions for which they are responsible. Parliament reviews, refines and enacts proposed legislation on national security matters. This process often involves calling witnesses to provide expert evidence about the issues raised by the proposed legislation.

Some laws contain provisions requiring a review of the law after a set period. For example, the Government has made a commitment to require a review of the ATA, 2015 after three years. Some laws might also require that a provision expires on a set date unless renewed. Other laws may require an annual report about the use of a particular provision.

House of Commons and Senate committees can also examine national security policy issues and conduct studies of government activities and existing legislation.

Normally, however, parliamentarians do not see classified information. This limits their ability to examine national security issues in depth. To resolve this, the Government has tabled a Bill C-22, the *National Security and Intelligence Committee of Parliamentarians Act*² to create a national security and intelligence committee of parliamentarians with broad access to classified information. The committee would examine how institutions are working together to keep Canadians safe from national security threats. It would also seek to ensure that institutions comply with Canada's laws and respect fundamental values, the democratic nature of our open society and the rights and freedoms of Canadians.

² Bill C-22 can be accessed at:

<http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=8375614>

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Agents of Parliament

Certain agents of Parliament scrutinize the national security activities of all federal institutions in relation to their specific mandates. For example, the Privacy Commissioner of Canada can examine their handling of personal information. The Privacy Commissioner also has a mandate to review the operations of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) every two years. The Information Commissioner of Canada investigates complaints about the Government's handling of access to information requests. The Auditor General (AG) can conduct "value-for-money" audits of national security programs.³

Commissions of Inquiry

Commissions of inquiry provide another means to keep government institutions accountable. Commissions of inquiry are "established by the Governor in Council (Cabinet) to fully and impartially investigate issues of national importance."⁴ Within the last decade, the O'Connor, Iacobucci and Major Commissions⁵ each reported on the activities of various national security institutions. Many, but not all, of their recommendations have been implemented. For example, Commissioner O'Connor made a number of detailed recommendations for changes to the framework for national security accountability in Canada that have not been implemented.

³ For example, in spring 2013, the AG reported on its audit of government spending on the Public Security and Anti-Terrorism Initiative; in fall 2012, the AG reported on the Government's efforts to protect Canadian critical infrastructure against cyber threats; and in March 2009, the AG reported on intelligence and information sharing in relation to national security.

⁴ Privy Council Office, Commissions of Inquiry.

⁵ Specifically, the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (report released September 18, 2006); the Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin (report released 22 October 2008); and the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (report released 17 June 2010).

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

What are other countries doing?

Some of our closest allies, including Australia and the United Kingdom (UK), share democratic traditions and institutions. As such, their experiences ensuring the accountability of national security and intelligence services are useful to consider when reflecting on Canada's own accountability mechanisms.

For instance, both Australia and the UK have parliamentary committees with access to classified information dedicated to national security. Indeed, the UK's Intelligence and Security Committee can, with the government's consent, review specific national security operations.

Australia and the UK also take different approaches to independent review of national security activities. In the UK, a number of different commissioners concentrate on a specific aspect of national security and intelligence across a range of agencies. These include:

- The Interception of Communications Commissioner ensures the propriety of communications interception activities;
- The Intelligence Service Commissioner's Office and the Office of Surveillance Commissioners review covert surveillance activities other than communications intercepts; and
- The Investigatory Powers Tribunal hears complaints and can authorize compensation and other redress.

The UK's system may change shortly, however; the *Investigatory Powers Bill*, currently before the UK Parliament, would consolidate the current bodies into a single Investigatory Powers Commission, and would also establish Judicial Commissioners charged with approving warrants.

Australia, for its part, has long had a consolidated model. There, the Inspector General of Intelligence and Security reviews all key intelligence and security agencies for compliance with the law, ministerial directives, and in regard to human rights.

In addition to its commissions and tribunals, the UK's Independent Reviewer of Terrorism Legislation provides expert commentary on proposed legislation, and reviews the use of powers granted by certain key pieces of existing legislation. In carrying out these duties, the Reviewer – who is appointed from outside of government – has access to classified information. Australia has a similar mechanism, the Independent National Security Legislation Monitor, which reviews, on an ongoing basis, national security and counter-terrorism legislation.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

What do you think?

Should existing review bodies – CRCC, OCSEC and SIRC – have greater capacity to review and investigate complaints against their respective agencies?

Should the existing review bodies be permitted to collaborate on reviews?

Should the Government introduce independent review mechanisms of other departments and agencies that have national security responsibilities, such as the CBSA?

The proposed committee of parliamentarians will have a broad mandate to examine the national security and intelligence activities of all departments and agencies. In addition to this, is there a need for an independent review body to look at national security activities across government, as Commissioner O'Connor recommended?

The Government has made a commitment to require a statutory review of the ATA, 2015 after three years. Are other measures needed to increase parliamentary accountability for this legislation?

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

PREVENTION

A new phrase has appeared in the Canadian lexicon: radicalization to violence. Radicalization to violence is a process where people take up an ideological position that moves them towards extremism and ultimately, terrorist activity.

Semantics are important here. It is not a crime to be a radical. Throughout history, change has been brought about by individuals whose radical ideas have inspired new ways of thinking. What is a crime is terrorism – violence committed in the name of radical ideologies or beliefs. As a Government, as a society, we are obliged to respond to criminal violence, whatever form it takes.

When someone decides to use violence to reach a political, ideological or religious goal, they have “radicalized to violence.” This is where terrorism takes root. This person may be formally linked to a terrorist group, inspired by a terrorist group, or radicalized to violence through their own beliefs. The question is, how does radicalization to violence begin? And, more important, what can be done to prevent it?

What Plays a Role?

We know that specific “narratives” drive radicalization to violence. These narratives reduce an individual's understanding of global events to a few simplistic propositions. Radicalization is also a social process occurring within networks and communities, both virtual and physical. People can be influenced by friends, mentors and other individuals in their lives.

Associating with others ascribing to violent radical ideologies can influence individuals to move further down the path of radicalization to violence. For example, it is no accident that many people who become extremist travellers – individuals who go abroad to join or contribute to terrorist groups – know others like them who have gone abroad. Some extremist travellers who return to Canada have the experience to plan and carry out terrorist attacks at home, as well as the credibility to recruit, encourage, mentor and facilitate the actions of aspiring terrorists.

The Internet also plays an important role in radicalization to violence. Terrorist groups use websites, chat rooms and social media as key propaganda and recruitment tools. For example, in the conflict in Iraq and Syria, some individuals and groups regularly post content and video clips on social media. These online posts boast of battlefield victories and seek to justify terrorist attacks and recruit young people from around the globe to join the fight.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Consider a scenario...

Mr. B is 17 years old and in his final year of high school. He was born and raised in a large suburban area. His neighbours think he is polite and he has no criminal record. Several months ago, a friend encouraged Mr. B to attend weekly discussion group meetings hosted by Mr. A. His charisma, moving speeches about global politics and self-confidence immediately drew in Mr. B. Over time, Mr. A's extremist views and promotion of violence began to resonate with Mr. B.

Between weekly meetings, Mr. B now spends much of his time on the family computer, watching violent videos that Mr. A has posted online. Some friends have noticed changes in Mr. B's behaviour and that he spends more time alone than before. Some teachers have noticed that he is less engaged in the classroom and intolerant of the views of his peers during class discussions. His association with Mr. A worries Mr. B's parents, but their attempts to talk to him about it have failed. They want to know what they can do and where they can go for help to prevent their son from becoming fully committed to a violent radical ideology.

What Can be Done?

All levels of government, communities and other stakeholders must work together to steer at-risk individuals away from radicalization to violence. They also need to give at-risk individuals the support they need to choose an alternative path that reflects Canadian values of peace and acceptance.

Law enforcement organizations play an important role. They seek to support individuals at risk of radicalization to violence and respond if individuals progress to criminal activities. The RCMP train law enforcement officers and front-line personnel to recognize early warning signs and lead interventions to divert individuals from the path of radicalization to violence. As well, Correctional Services Canada conducts tailored interventions for inmates who have radicalized to violence or who are at risk of doing so.

Family members, friends and others close to at-risk individuals can also play a key role in countering radicalization to violence. They are often aware of the individual's beliefs and intentions. Individuals who are early on in the process of radicalization may have many questions and doubts. At this early stage, it may be possible to steer individuals away from radicalization to violence. For this reason, it is essential to support local communities to address this issue.

National Leadership

The Government is also exploring new ideas and innovative approaches to counter radicalization to violence. Budget 2016 announced \$35 million over five years, with \$10 million per year ongoing, to create an Office of the community outreach and counter-radicalization coordinator. The Office will

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

lead Canada's response to radicalization to violence, coordinate federal, provincial, territorial and international initiatives, and support community outreach and research. The material immediately below describes in greater detail what the Office could do.

Work with Communities

The most effective way to prevent radicalization to violence often lies within communities. It involves working with local leaders to develop early intervention programs. A key focus for the new Office is to reach out to Canadians and build constructive relationships with communities across Canada, raise general awareness about threats and means to address them, and maintain a continual dialogue with those communities.

Engaging with Canadians will help identify priorities for the Office and inform the development of a national strategy to counter radicalization to violence. The Office is seeking to support programs that focus on individuals at risk of radicalization to violence. These programs can include community capacity-building, mentorship, multi-agency interventions and training and support for those involved in front-line intervention work (such as youth workers, corrections and parole officers, social service providers, faith leaders and mental health practitioners).

The City of Montreal is also working in this area. It has established a Centre for the Prevention of Radicalization Leading to Violence. The Centre brings together partners from various sectors, including health and social services, public safety and education. The goal is to develop expertise, define areas of prevention and intervention, and empower communities to address radicalization to violence. The Office can incorporate lessons learned from Montreal's experience into future programming.

Engage Youth and Women

Radicalization to violence in Canada affects young people disproportionately. Engaging with youth is therefore important in addressing this issue. Early in the process of radicalization they may have many questions and doubts. They turn to the guidance that is available. At this early stage, tailored outreach has the potential to steer at-risk youth away from radicalization to violence. The Office is looking to start a positive conversation with young people, raise their awareness about the dangers of becoming radicalized to violence, and empower them to respond to the issue.

Women can play a key role in this area. Research has shown that the involvement of women – in different capacities and roles, in both the private and public spheres – is essential to effective prevention efforts. As gatekeepers to their communities, they are often well-positioned to serve as credible, resonant voices against violent radical ideologies. The Office can support local initiatives that engage, inform and empower women to better identify and address violent radicalization in their families and communities. The Office can also develop and share tools, resources and information to support women – and men – in responding to this issue.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Promote Alternative Narratives

Terrorist groups often aim to influence potential recruits by promoting and spreading certain messages. Promoting positive, alternative narratives is one way to counter such messages.

The Office is looking for ways to support credible voices and empower community actors—particularly youth and women—to develop programs, messaging or other tools that reflect local realities. These measures can be used to challenge violent radical narratives and promote critical thinking. For example, terrorist groups use the Internet and social media to spread violent radical ideologies and messaging quickly and broadly. The Office can support programs that harness these tools for positive uses.

Foster Research

Research is a key element in countering radicalization to violence. It can inform policy development, improve the design of programs and tools, and help identify appropriate and effective ways to counter radicalization to violence. The Government is looking to engage with academics, think tanks and others to determine research priorities, identify best practices and lessons learned and develop effective tools to measure the success of programs.

Through the Kanishka Project⁶, the Government has invested in research about radicalization to violence and has identified a number of best practices. There is more to learn, and the demand for that information and research is great. Support for action-oriented research is important. Such research produces guides, tools and other resources to assist the public, as well as mechanisms to evaluate programs and measure their success. Evaluation tools will help develop more effective programs to counter radicalization to violence. Knowing what works will also inform policies and priorities, and can contribute to the success of Canada's overall approach to the issue.

What are other countries doing?

Countering radicalization to violence is a priority for the international community. The United Nations emphasized the importance of prevention efforts in United Nations Security Council Resolution 2178, which was unanimously adopted in September 2014. Also, in January 2016, the United Nations Secretary-General released a Plan of Action to Prevent Violent Extremism, which encourages countries to develop national strategies for addressing radicalization to violence. Canada strongly supports this initiative.

⁶ <http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/r-nd-flight-182/knshk/index-en.aspx>

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Like Canada, other countries have begun to develop policies and programs to respond to this issue. Working with communities, engaging youth and women, promoting alternative narratives, and conducting research are also key areas of focus for our international partners.

Examples

Community engagement is a cornerstone of a number of countries' national strategies to counter radicalization to violence. For example, to enhance social cohesion and harmony, Singapore's Community Engagement Programme brings together Singaporeans from different communities – from religious groups, to unions, to educational institutions, to the media – to strengthen inter-communal bonds, build partnerships and enhance social resilience. Also, to better inform citizens on radicalization to violence, Australia has created a website called Living Safe Together as a central online location where people can read about how Australia addresses this issue, seek information and advice on radicalization to violence, and access other resources. The Office could develop similar initiatives that are tailored to the Canadian experience.

Some countries have also explored programs focusing on youth. For example, in Sweden, there is a youth centre called “Fryshust” that promotes confidence, responsibility, and understanding to enable young people to develop their innate abilities and find their way in society. Also, in Denmark, an organization called “My House” aims to pair individuals at risk of radicalization to violence with mentors that face similar challenges and come from similar backgrounds, but that can show an alternative, positive path to explore.

Finally, engaging women in prevention efforts is an important element of some countries' approaches to this issue. For example, in the UK, “Project Shanaz” was developed in 2011 to understand the perception women have of activities related to the country's national strategy to counter radicalization to violence. This project led to the establishment of the Shanaz Network, an independent body of 50 women community leaders that contributes to the development of policies and strategies related to radicalization to violence. A similar model in Canada could help inform the development of a new strategy to counter radicalization to violence.

What do you think?

The Government would like your views about what shape a national strategy to counter radicalization to violence should take. In particular, it is looking to identify policy, research and program priorities for the Office of the community outreach and counter-radicalization coordinator. What should the priorities be for the national strategy?

What should the role of the Government be in efforts to counter radicalization to violence?

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Research and experience has shown that working with communities is the most effective way to prevent radicalization to violence. How can the Government best work with communities? How can tensions between security concerns and prevention efforts be managed?

Efforts to counter radicalization to violence cannot be “one size fits all.” Different communities have different needs and priorities. How can the Office identify and address these particular needs? What should be the priorities in funding efforts to counter radicalization to violence?

Radicalization to violence is a complex, evolving issue. It is important for research to keep pace. Which areas of research should receive priority? What further research do you think is necessary?

What information and other tools do you need to help you prevent and respond to radicalization to violence in your community?

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

THREAT REDUCTION

Since its creation in 1984, CSIS has collected information and intelligence on threats to the security of Canada, at home and abroad.⁷ CSIS uses the information to advise other institutions of government, such as law enforcement, about these threats. These institutions then in turn act on the information.

The ATA, 2015 amended the *Canadian Security Intelligence Service Act (CSIS Act)* to authorize CSIS to reduce threats to the security of Canada. CSIS can now do more than share information. It can also take direct action against threats to reduce the danger they pose. Threat reduction (also called disruption) seeks to prevent or discourage people who pose a threat from carrying out their plans.

The threats facing Canada have evolved significantly in recent years. In part, this flows from the trend away from complex terrorist operations towards loosely organized small-scale attacks, the growing use of the Internet and mobile communications, and the ease with which people can move about the globe. These changes have made it harder for security agencies to prevent attacks.

The RCMP have long had a crime prevention mandate. This allows them to act pre-emptively to prevent threats from materializing. However, there are differences in the roles and responsibilities of CSIS and the RCMP. These include different priorities, different approaches, access to different information and a different international presence. For these reasons, during the development of the ATA, 2015, it was felt that there were situations where CSIS was best placed to take timely action to reduce threats. Even before the debate about the ATA, 2015, a threat reduction mandate for CSIS was being discussed. A 2010 report by SIRC recommended that CSIS seek guidance and direction on the issue of threat reduction. In 2011, the Senate Special Committee on Anti-terrorism also considered threat reduction and issued recommendations.

The CSIS threat reduction mandate does not give it law enforcement powers. For instance, CSIS cannot arrest individuals. CSIS continues to work in consultation with the RCMP and other law enforcement agencies.

The Threat Reduction Mandate

For some threat reduction measures CSIS requires a warrant from the Federal Court. Whether a warrant is needed hinges on whether the proposed actions by CSIS would affect *Charter* rights or would, without a warrant, be against the law.

⁷ "Threats to the security of Canada" are defined in section 2 of the *CSIS Act*, and encompass terrorism (or more precisely "acts of serious violence... for the purpose of achieving a political, religious or ideological objective"), espionage and sabotage, foreign-influenced activities that are clandestine, deceptive, or threaten a person, as well as domestic subversion aimed at the overthrow by violence of the constitutional order of government. Lawful advocacy, protest and dissent are excluded, unless carried out in conjunction with any of the activities referred to above.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Consider a scenario where a warrant is not needed...

Mr. C, a Canadian citizen, attends Mr. A's weekly meetings. He has even voiced support for terrorist activity in Canada in response to terrorist propaganda encouraging attacks in the West. Mr. C is seeking employment as a guard for a firm that provides security at major concerts and other events. CSIS approaches the firm and provides information about Mr. C. Once aware of Mr. C's support for terrorist activity, the firm launches an investigation and decides to restrict Mr. C's work. As a result, Mr. C does not gain privileged access to major events where he could pose a security threat.

Consider a scenario where a warrant is needed...

Mr. D, an associate of Mr. A, is promoting extremism on his personal website by posting videos supporting a terrorist group. His website is hosted outside Canada and also includes how-to guides for making bombs and suicide vests. CSIS obtains a threat reduction warrant from the Federal Court allowing it to modify the website's how-to guides. CSIS replaces some of the terrorism-related details with misinformation that will make the devices fail. Mr. D and his followers do not notice the changes. As a result, their effective support to terrorism has been limited.

The table below sets out the differences between threat reduction measures by CSIS that require a warrant and those that do not.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

| | No warrant required | Warrant required |
|----------|--|---|
| Examples | <ul style="list-style-type: none"> - Interviews - Asking friends to intervene - Reporting extremist content to social media providers | <ul style="list-style-type: none"> - Disrupting financial transactions - Interfering with terrorist communications - Manipulating goods intended for terrorist use |



| | | |
|--|---|---|
| Procedure CSIS must follow to take threat reduction measures | <ul style="list-style-type: none"> - CSIS must have reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada - CSIS must demonstrate that the proposed measure is reasonable and proportional in the circumstances - CSIS must obtain internal approval, perform a risk assessment, and consult law enforcement and other agencies as appropriate | <ul style="list-style-type: none"> - CSIS must have reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada - CSIS must demonstrate that the proposed measure is reasonable and proportional in the circumstances - CSIS must obtain internal approval, perform a risk assessment, and consult law enforcement and other agencies as appropriate - CSIS must obtain approval from the Minister of Public Safety and Emergency Preparedness for a warrant application - The Federal Court then reviews the warrant application and decides whether to issue the warrant |
|--|---|---|

Threat reduction measures that would cause death or bodily harm, violate a person's sexual integrity or interfere in the course of justice are prohibited.⁸

⁸ See *CSIS Act*, section 12.2.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Potential Impacts on *Charter* Rights

Threat reduction measures may affect Canadians' *Charter* rights and freedoms, depending on the circumstances of the measure.

CSIS must obtain a warrant from the Federal Court before it can take threat reduction measures that would affect rights protected under the *Charter*. The *Charter* recognizes that rights and freedoms are not absolute and that at times they may justifiably be limited. A warrant shows that the Court has determined in advance that the proposed threat reduction measures are reasonable and proportional in the circumstances.

Warrants have long been used to balance government objectives and *Charter* rights. Since 1984, CSIS has sought warrants from the Federal Court to collect intelligence using techniques that limit privacy rights protected by section 8 of the *Charter*. Police wiretaps and search warrants work in a similar way. Threat reduction warrants are a departure from previous warrant regimes. They can limit additional *Charter* rights, not just privacy rights under section 8.

What are other countries doing?

Intelligence and security services in many of Canada's allies have the mandate to reduce threats to national security and a range of threat reduction powers. There is no standard approach to threat reduction, however, as each country has a unique system of government, making direct comparisons difficult. In some countries, responsibility for national security and intelligence is divided between foreign and domestic services. In others, responsibility is divided between intelligence and law enforcement. In the U.S., for example, there are distinct domestic and international agencies. Domestically, the FBI has both intelligence and law enforcement responsibilities.

Nonetheless, various allied intelligence and security services have the authority to take direct action against threats, domestically and/or abroad, subject to various limitations. In the UK, for instance, the Security Service (also known as MI5) has legal authority to take action to protect national security, including against the threat of terrorism. The Australian Secret Intelligence Service has a broad mandate to undertake "other activities", including threat reduction measures outside of Australia. French authorities can also disrupt threats to France and French interests abroad.

Internationally, the means by which threat reduction activity is legally authorized takes various forms. Canada's framework requires court warrants for measures that would affect *Charter* rights. In other countries, senior members of the executive branch authorize intrusive threat reduction measures.

In the current international environment, the threat reduction mandate allows CSIS to contribute to a broader range of allied operations against terrorism and other shared threats than was previously the case.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

What do you think?

The Government wants to know what you think about CSIS's new threat reduction mandate:

CSIS's threat reduction mandate was the subject of extensive public debate during the passage of Bill C-51, which became the ATA, 2015. Given the nature of the threats facing Canada, what scope should CSIS have to reduce these threats?

Are the safeguards around CSIS's threat reduction powers sufficient to ensure that CSIS uses them responsibly and effectively? If current safeguards are not sufficient, what additional safeguards are needed?

The Government has committed to ensuring that all CSIS activities comply with the *Charter*. Should subsection 12.1(3) of the *CSIS Act*⁹ be amended to make it clear that CSIS warrants can never violate the *Charter*? What alternatives might the Government consider?

⁹ Subsection 12.1(3) of the Act states that CSIS "shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms* or will be contrary to other Canadian law, unless [CSIS] is authorized to take them by a warrant . . ."

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

DOMESTIC NATIONAL SECURITY INFORMATION SHARING

National security institutions need information to detect, analyze, investigate and prevent threats. It often takes multiple pieces of information to provide a complete threat picture, and today's national security threats can evolve rapidly, heightening the need for timely and complete information.

Yet information needed for national security purposes can be held in different places by various institutions of government. Because of this, the sharing of information is an important part of national security work today. The report of the Air India inquiry¹⁰ stressed this point. The report of the O'Connor inquiry¹¹ also mentioned the importance of information sharing for investigations and prevention of national security threats, but also highlighted the need for caution with respect to the content of the information and its use by the recipient.

Federal institutions with national security responsibilities can collect information to carry out lawful duties and responsibilities. This collection may be authorized by an Act of Parliament, the common law or the Crown Prerogative. Even institutions that do not have a national security mandate (such as the Department of Fisheries and Oceans) sometimes hold information that could be important for national security institutions. Non-national security institutions must be able to disclose that information to institutions that have a mandate to act on it.

Government institutions must follow certain rules when sharing information, especially information about individuals. These rules are important to protect privacy rights. However, their complexity can sometimes make it difficult to know whether a given institution is permitted to share information. This can prevent information from getting to the right institution in time.

The *Privacy Act*

The *Privacy Act* protects individuals' personal information by regulating how federal government institutions collect, use, retain and disclose it. The Act limits the collection of personal information by government institutions to that which relates directly to their work. It also limits when this information can be used and disclosed without the consent of the individual to whom it relates.

The *Privacy Act* recognizes that personal information may be disclosed without consent in some situations, including those involving national security. The main exceptions to the rule preventing disclosure without consent are as follows:

1. "Consistent use": One federal institution may share information with another institution for the purpose for which the information was collected or for a use consistent with that purpose (for an example, see the scenario below).
2. "Investigative bodies": Some institutions are listed as "investigative bodies" in the Act (for example, the RCMP and CSIS). An investigative body can ask another federal institution to provide it with personal information to assist it in carrying out its activities. However, the

¹⁰ Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

¹¹ Commission of Inquiry into the Actions of Officials in Relation to Maher Arar.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

other institution must be asked first. It cannot decide on its own to proactively share personal information with an investigative body.

3. "Public interest": The head of a federal institution may disclose personal information if the head determines that the public interest benefit in disclosure clearly outweighs any invasion of privacy. In the national security context, communicating what the benefit is to a non-national security institution to obtain disclosure may not be possible (for example because of operational sensitivities). This makes it difficult for the head of the non-national security institution to decide whether to disclose personal information in the public interest.
4. "Lawful authority": the *Privacy Act* permits disclosure of personal information where another Act of Parliament authorizes it.

Consider a scenario...

A foreign national, Ms. E, sends an application for permanent resident status to Immigration, Refugees and Citizenship Canada (IRCC). This application contains the personal information that the Government needs to process her request to become a permanent resident and to determine whether she is admissible to Canada under the *Immigration and Refugee Protection Act*. To assess her application for security concerns, IRCC discloses some of Ms. E's personal information to CSIS, which has a security screening mandate under the immigration program. This type of sharing between IRCC and CSIS is an example of sharing that takes place under the "consistent use" exception of the *Privacy Act*.

The Security of Canada Information Sharing Act

Objective

The ATA, 2015 enacted the *Security of Canada Information Sharing Act* (SCISA) to facilitate national security information sharing. The SCISA creates an explicit disclosure authority, which provides greater certainty about when institutions can share information for national security reasons. Because it is an Act of Parliament that authorizes disclosure, it satisfies the "lawful authority" exception under the *Privacy Act*, as explained above.

What the SCISA Does

The SCISA authorizes all federal institutions to disclose information (including information about individuals) related to "activities that undermine the security of Canada." "Activity that undermines the security of Canada" is defined as any activity that "undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada" (section 2 of the SCISA). This concept covers a broad range of national security-related activities and is intended to provide flexibility to accommodate new forms of threats that may arise. The SCISA includes examples of these activities that may be covered by this concept.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Information may be disclosed to 17 federal institutions listed in the SCISA (referred to as “recipients” throughout this document).¹² To be disclosed, the information must be *relevant*¹³ to the recipient’s lawful national security jurisdiction or responsibilities.

Consider a scenario...

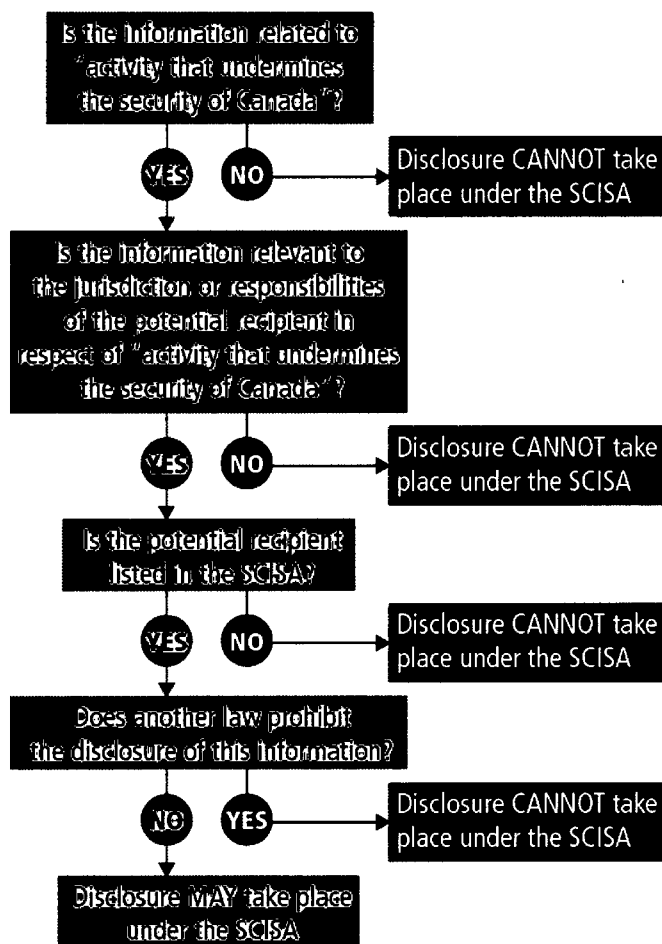
During a routine check, a passport official at IRCC contacts the references of Mr. F, who has applied for a passport. Mr. F has been attending Mr. A’s weekly meetings. Without prompting, one referee tells the passport official that she is worried that Mr. F may be travelling to a country to become a fighter with a terrorist group, since he supports the group’s goals. IRCC proactively shares information under the SCISA with CSIS and the RCMP, which have responsibilities for investigating this type of activity.

To decide whether they can disclose information under the SCISA, federal institutions go through the following process:

¹² These 17 recipients already have legal authorities to collect information for national security reasons. The SCISA neither expands nor changes these collection authorities.

¹³ Relevant: Because national security information sharing often engages privacy rights, the SCISA requires that information be disclosed only if it is actually—and not potentially or possibly—relevant to the recipient’s lawful responsibilities for activity that undermines the security of Canada. There must be a reasonable basis to conclude that the information is related to the recipient’s exercise of their responsibilities for such activity. Reliability and accuracy are also important factors in determining whether information is relevant under the SCISA.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.



When the SCISA Can and Cannot be Used:

The definition of “activity that undermines the security of Canada” only includes activities that have an impact on national security. Some Canadians expressed concern during the parliamentary examination of the bill that became the ATA, 2015 that their right to lawful protest may be impacted by the SCISA. The SCISA was amended to make it clear the activities of advocacy, protest, dissent, and artistic expression *do not* fall within the definition of “activity that undermines the security of Canada.” As a result, information about these activities cannot be disclosed under the SCISA.

However, if violent actions take place that meet the definition of “activity that undermines the security of Canada,” they cannot be considered to be advocacy, protest, dissent or artistic expression. Information about these actions can be disclosed under the SCISA.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Consider another scenario...

A national park is located near a natural gas pipeline, a critical infrastructure site. An official at the park notices a group gathering to protest near the pipeline. Even though this information deals with critical infrastructure, the official cannot disclose this information under the SCISA to another federal institution. This is because protest, advocacy, dissent, and artistic expression are explicitly excluded from the definition of "activity that undermines the security of Canada" under the SCISA.

What the SCISA Does Not Do

The SCISA cannot be used to bypass other laws prohibiting or limiting disclosure. If another law restricts use or sharing of information, these restrictions continue to apply and must be respected. For example, Employment and Social Development Canada's program legislation addresses how it protects and discloses personal information. The SCISA does not override this program legislation.

Who Decides Whether to Use the SCISA?

The institution disclosing information is responsible for determining whether the information may be disclosed. The disclosing institution may need discussions with the potential recipient to see if the information relates to the national security responsibilities of the recipient. These discussions should not require the sharing sensitive operational information.

An institution has the discretion whether or not to disclose information under the SCISA. This decision always rests with the disclosing institution even if all the SCISA requirements for disclosure are met.

Who Receives the Information?

All recipients under the SCISA have national security responsibilities. However, not necessarily all parts of the recipient institutions will be involved in carrying out these responsibilities. The SCISA requires that information be provided to the head of the institution or to delegates of the head. This helps to ensure that only officials who need the information receive it.¹⁴

Potential Impacts on *Charter* Rights

The *Charter* protects individuals' privacy against unreasonable government intrusions. The *Charter* allows intrusions into privacy that are authorized by a reasonable law. In some cases, disclosure of information among federal institutions could impact privacy rights.

Information sharing under the SCISA may be reviewed like other instances of government information sharing. In particular, the *Privacy Act* allows the Privacy Commissioner of Canada to review institutions' handling of personal information and to hold institutions accountable by

¹⁴ Once information is disclosed to a recipient under the SCISA, the recipient may further disclose it under the SCISA or under another authority outside the SCISA. The recipient's use of the information disclosed to it under the SCISA continues to be governed by authorities found outside the SCISA.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

releasing public reports. Some institutions – the RCMP, CSIS and the CSE – also have specific bodies that review their work, including information sharing practices that are part of this work.

The SCISA includes a power to make regulations; however no regulations have been made. Regulations made under the SCISA would support how the SCISA works in practice. For example, regulations could outline record-keeping requirements.

A number of government-wide information sharing guidance and support resources are available for federal institutions. Public Safety Canada has prepared a deskbook and a public framework to guide institutions in using the SCISA. Federal institutions may also set policies and give guidance on how their officials should use the SCISA.

What are other countries doing?

Many countries seek to promote the sharing of information for national security purposes, while protecting the privacy rights of individuals. As each country has a unique legislative and policy framework for the sharing of information for national security purposes, the challenges they face in this area vary considerably across jurisdictions. Some countries allow the sharing of information between government agencies without express consent to do so in each case. Others have more explicit powers or policies.

The UK's information sharing provisions are included in its *Counter-Terrorism Act, 2008*. These provide broad information sharing powers, including from persons to UK security agencies. Denmark has express authority in privacy legislation (the *Act on Processing of Personal Data*) to share personal information for national security purposes. Australia has a 10-year plan (Vision 2020) to enhance national security information sharing, which includes a harmonized policy and legislative framework.

What do you think?

The Government has made a commitment to ensure that Canadians are not limited from lawful protest and advocacy. The SCISA explicitly states that the activities of advocacy, protest, dissent, and artistic expression do not fall within the definition of “activity that undermines the security of Canada.” Should this be further clarified?

Should the Government further clarify in the SCISA that institutions receiving information must use that information only as the lawful authorities that apply to them allow?

Do existing review mechanisms, such as the authority of the Privacy Commissioner to conduct reviews, provide sufficient accountability for the SCISA? If not, what would you propose?

To facilitate review, for example, by the Privacy Commissioner, of how SCISA is being used, should the Government introduce regulations requiring institutions to keep a record of disclosures under the SCISA?

Some individuals have questioned why some institutions are listed as potential recipients when their core duties do not relate to national security. This is because only part of their jurisdiction or

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

responsibilities relate to national security. Should the SCISA be clearer about the requirements for listing potential recipients? Should the list of eligible recipients be reduced or expanded?

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

THE PASSENGER PROTECT PROGRAM

Air travel is an important means of transportation, both within Canada and abroad. Without appropriate security measures, air travel is vulnerable to criminal and national security threats. Tragedies such as the 1985 Air India bombing, the attacks of September 11, 2001, and the October 2015 bombing of a Russian airliner in Egypt, each demonstrate the cost in lives, economic and social disruption that threats to aviation security can cause.

Direct threats to aviation security, such as terrorists bringing or placing explosive devices aboard aircraft, continue to be of concern. In addition, concern is growing about individuals travelling abroad, often by air, to engage in terrorism offences. These individuals are known as “extremist travellers.” They pose a threat at home and also pose a threat abroad when they participate in conflicts in countries as Syria and Iraq. These individuals are involved in training, fundraising and other terrorist activities on behalf of groups such as Daesh. Trained, radicalized and experienced extremist travellers pose another serious risk if they return to Canada. Here, they might launch or inspire domestic attacks.

The Government provides aviation security in part by preventing individuals who have the intent and capability to harm passengers and aircraft from boarding. The ATA, 2015 enacted the *Secure Air Travel Act* (SATA). Under the SATA, the Government can use the Passenger Protect Program (PPP) – an air passenger identity screening program – to prevent individuals from boarding a flight if they pose a threat to transportation security or are seeking to travel by air to commit certain terrorism offences.

Consider a scenario...

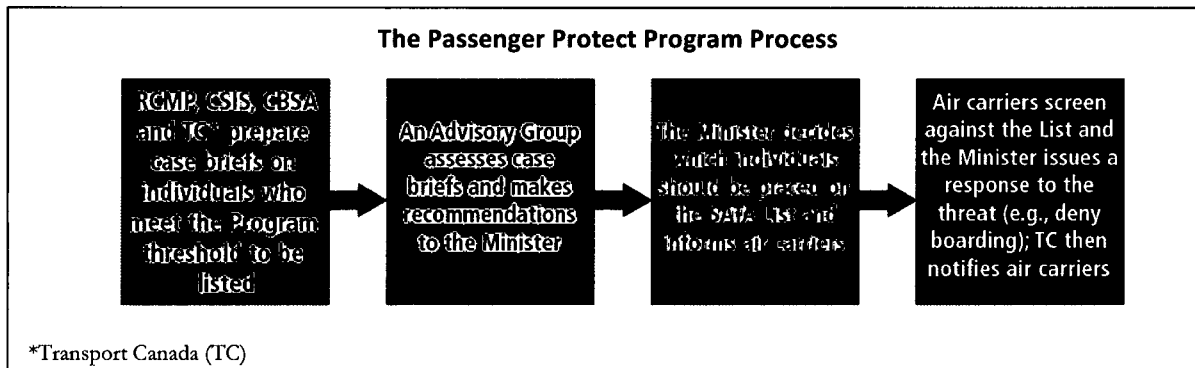
Ms. G is a 22-year-old high school graduate who has been drifting between jobs over the past few years. She attends Mr. A's discussion meetings in her neighbourhood and has rapidly radicalized to violence.

Ms. G is keen to travel overseas to join a terrorist group. Mr. A has been communicating with a terrorist overseas to plan Ms. G's departure. The goal is for Ms. G to get weapons and explosives training and fight for her cause. She then wants to return to Canada and train others to become terrorists.

The RCMP become aware of Ms. G's plans and alert Public Safety Canada. Based on this information, the Minister of Public Safety and Emergency Preparedness adds Ms. G to the list created under the SATA. If Ms. G attempts to check in for a flight, Public Safety Canada will be alerted and may issue a direction to deny her boarding.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

The PPP, as governed by the SATA, works as follows:



Through the PPP, the Minister of Public Safety and Emergency Preparedness (the Minister¹⁵) has the authority to establish a list of individuals (known as the SATA List) who may (1) pose a threat to transportation security or (2) travel by air to commit certain terrorism offences.¹⁶ Listed individuals can be prevented from flying. To list an individual, the Minister must have reasonable grounds to suspect that the individual will engage in at least one of these two acts. For example, if it is reasonably suspected that an individual will travel by air to commit certain terrorism offences,¹⁷ such as to participate in the activities of a terrorist group, the individual can be listed under the PPP.

The listing process is conducted confidentially and is based on intelligence and other information from investigations. Public Safety Canada chairs an advisory group composed of the RCMP, CSIS, the CBSA, TC and IRCC. The advisory group nominates individuals to the SATA List, assesses the information supporting the nominations and recommends to the Minister which individuals should be listed. The SATA List is reviewed at least every 90 days to ensure that there are still reasonable grounds to suspect that individuals on the List pose a threat to transportation security and/or will travel by air to commit certain terrorism offences.

Once an individual is listed, the Minister can direct an air carrier on how to respond when the individual attempts to board an aircraft. The direction will be issued to air carriers only once an individual's identity is verified and confirmed to be a positive match to the SATA List, and after any new information is considered. These responses are tailored to the specific situation, based on what is reasonable and necessary to prevent the threat from being carried out. For example, individuals who are assessed as posing a high risk to transportation security may be denied boarding to protect both passengers and aircraft. Other listed individuals may undergo additional screening to provide greater certainty that they are not, for example, carrying any weapons or prohibited items.

¹⁵ The Minister can delegate his or her authority to take any action under the SATA.

¹⁶ Pursuant to paragraphs 8(1)(a) and (b) of the SATA.

¹⁷ The SATA refers to offences under sections 83.18, 83.19 and 83.2 of the *Criminal Code*.

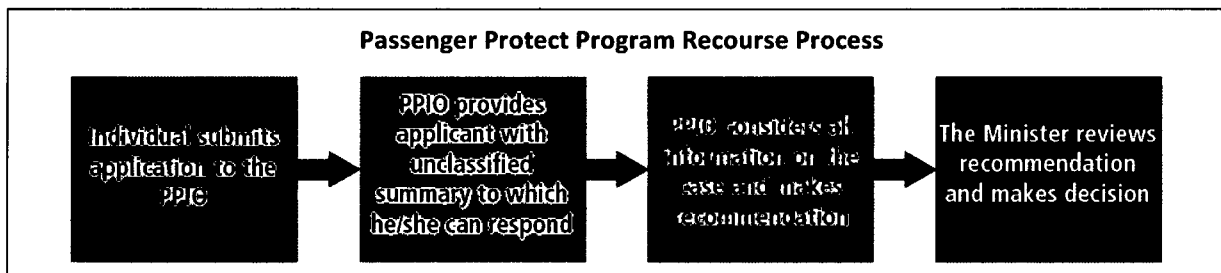
This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Potential Impacts on Charter Rights

A direction to deny boarding can impact a citizen's right to enter and leave Canada. Section 6 of the *Charter* protects this right. Individuals also have an interest in not being delayed or prevented from travelling by air. A direction to deny boarding would only be made when the Minister considers it is reasonable and necessary to prevent a listed person from taking a specific action.

Recourse

Because of the acknowledged impacts of being denied boarding, an individual in this situation can apply in writing for recourse to the Passenger Protect Inquiries Office (PPIO) within 60 days of being denied boarding.¹⁸ The application seeks to have the individual's name removed from the List. The applicant receives an unclassified summary of the information used to support the listing and has an opportunity to respond. The Minister may take up to 90 days¹⁹ to review the application and decide whether there are still reasonable grounds to maintain the applicant on the List. If the Minister does not make a decision within 90 days,²⁰ the Minister is deemed to have decided not to remove the applicant's name from the List. This is done to err on the side of caution, while the 90-day deadline ensures that the applicant has timely access to the Federal Court, as explained below.



If an individual is not satisfied with the Minister's decision, the individual may appeal the decision to the Federal Court. Most decisions made under the PPP rely on sensitive information that, if disclosed, could be injurious to national security or endanger the safety of a person. The judge hearing the appeal can see all information relevant to the Government's decision. To protect against disclosure of sensitive information, the applicant sees a summary of the relevant sensitive information. The applicant can also introduce new information to respond to the Government's case. The judge may appoint an *amicus curiae* to assist the Court with any aspect of the proceeding, including during the closed portion of the proceedings where the applicant cannot be present because sensitive information is being presented.

¹⁸ Subsection 15(2) of the SATA allows the Minister to extend that limit if there are exceptional circumstances.

¹⁹ Subsection 15(6) of the SATA allows this period to be extended, as agreed by the applicant and the Minister.

²⁰ Or a further period agreed upon between the applicant and the Minister.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Consider a scenario...

Mr. H intends to fly to Florida for the Labour Day weekend but is delayed at the airline ticket counter while the desk agent contacts his supervisor. After a few minutes, Mr. H is allowed to continue, but he leaves on his flight frustrated. He suspects that his name is similar to that of someone on Canada's aviation security list. He contacts the Passenger Protect Inquiries Office, which works with relevant partners to help facilitate his future travel.

Redress

The SATA List is not the only reason for delaying an individual or preventing them from flying. There can be many other reasons, unrelated to the SATA, including air carriers' own security lists and/or aviation security lists maintained by other countries. As well, a false positive match to an aviation security list, whether that of an air carrier, a foreign country or the SATA List itself, may cause travel to be delayed.

The PPIO provides assistance to air travellers who have experienced delays or difficulties related to aviation security lists. The PPIO can assist the traveller in identifying the reason for this situation and suggest what to do next. Following a joint announcement by the Prime Minister of Canada and the President of the United States on March 10, 2016, the governments established the Canada-U.S. Redress Working Group. The Working Group is a bilateral mechanism. It allows the PPIO to collaborate closely with the U.S. on certain matters of redress and recourse about Canadian and American citizens and permanent residents who may be affected because of their potential presence on the SATA List or the U.S. No Fly List.

In addition, the Government is considering possible changes to the SATA and its regulations to help reduce instances of false positive matches to the SATA List. The objective is to create a process where individuals who have experienced a false positive match can obtain a redress number, which would be provided to the air carrier prior to travel and assist in avoiding delays.

What are other countries doing?

A number of Canada's key international partners, including the U.S., the UK, Australia and New Zealand have some form of air passenger screening prior to departure. In most cases, these programs are designed to determine an individual's admissibility status before they can travel to that country, and/or whether they pose a security risk. The U.S., for example, operates a number of air passenger screening programs that address both immigration and security considerations.

Canada's PPP does not operate in conjunction with the U.S. No Fly list or with any other countries' and organizations' aviation security programs. While the SATA permits the Minister of Public Safety to share information with another country to address potential threats, both countries' programs will continue to operate subject to their respective laws.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

What do you think?

At present, if the Minister does not make a decision within 90 days about an individual's application for removal from the SATA List, the individual's name remains on the List. Should this be changed, so that if the Minister does not decide within 90 days, the individual's name would be removed from the List?

To reduce false positive matches to the SATA List, and air travel delays and denials that may follow, the Government has made a commitment to enhance the redress process related to the PPP. How might the Government help resolve problems faced by air travellers whose names nonetheless generate a false positive?

Are there any additional measures that could enhance procedural fairness in appeals of listing decisions after an individual has been denied boarding?

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

CRIMINAL CODE TERRORISM MEASURES

The *Criminal Code* defines terms such as “terrorist activity,” “terrorism offence” and “terrorist group.” It sets out a wide range of terrorism offences, provides a process to “list” entities as terrorist groups and outlines a range of anti-terrorism powers for law enforcement.²¹ Many of the terrorism provisions were enacted in 2001 and amended in 2013 to include specific terrorist travel offences. Since 2001, a number of people have been convicted of terrorism offences in Canada, with some receiving life sentences. The courts have found key *Criminal Code* terrorism provisions to be consistent with the *Charter*.²²

Some provisions of the ATA, 2015 introduced changes to *Criminal Code* terrorism provisions. The Code was amended to accomplish several goals:

- to make it easier for peace officers to detain individuals temporarily, and to apply to a court to have reasonable conditions imposed on individuals to prevent the carrying out of terrorist activity and the commission of terrorism offences;
- to create a new offence that criminalizes the advocacy or promotion of the commission of terrorism offences in general;
- to give the courts the authority to order the seizure and forfeiture of tangible terrorist propaganda material and the removal of online terrorist propaganda from Canadian websites; and,
- to provide additional protection to witnesses and other participants in national security proceedings and prosecutions.

Preventive Law Enforcement Tools (Recognizance with Conditions and Terrorism Peace Bond)

Canadian criminal law generally focuses on prosecuting offences that have already occurred. However, criminal courts can also impose **preventive conditions** on an individual where there is evidence that the individual is likely to commit an offence in future. Two specific tools allow for a court to impose conditions to prevent terrorism: the **recognizance with conditions** and the **terrorism peace bond**. Some aspects of these tools first appeared in 2001 when the *Anti-terrorism Act* came into force.

²¹ “Terrorist activity” is a term made up of a list of specific offences that implement Canada’s international obligations, as well as a general definition. It is used as the basis for many of the terrorism offences in the *Criminal Code*, such as knowingly facilitating a terrorist activity

²² See, for example, *R. v. Khawaja* [2012] 3 SCR 555.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

A **terrorism peace bond** is used to prevent a specific individual from committing a terrorism offence, such as leaving or attempting to leave Canada to commit an offence for a terrorist group.

A **recognizance with conditions** is used when the police suspect someone is connected in some way to the carrying out of a terrorist activity. For example, they suspect that someone is connected to a broad plot to attack Parliament, but the person's exact role may not be known.

Both the terrorism peace bond and the recognizance with conditions aim to prevent individuals from carrying out terrorist acts.

Consider a scenario where a terrorism peace bond could be used...

A family notifies the RCMP that they feel their son, Mr. I, has become radicalized to violence. He is a good friend of Mr. A. The RCMP investigate and learn that Mr. I has told a number of people close to him that he plans to join a terrorist group active in a conflict zone abroad. The RCMP also learn that Mr. I has been pricing air travel to a country that borders an ongoing conflict zone where the group is active.

The RCMP now suspect that Mr. I may commit a terrorism offence – travelling or attempting to travel abroad to participate in the activity of a terrorist group. They seek the consent of the Attorney General of Canada to apply to a judge for a terrorism peace bond to prevent Mr. I from travelling abroad.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Consider a scenario where a recognizance with conditions could be used...

The police conduct an urgent investigation into a group of ten people based on an anonymous tip. Some of these people attend Mr. A's weekly meetings. Some members of the group are apparently planning to bomb an unknown public gathering that week. Further investigation reveals that one person in the group, Ms. J, recently downloaded bomb-making instructions. The police hope to obtain a recognizance with conditions to stop Ms. J from making, providing or using an explosive device. They seek the consent of the Attorney General of Canada to apply to a judge for a recognizance with conditions.

The judge considers the application and is satisfied that a terrorist activity may be carried out. The judge also has reasonable grounds to suspect that the imposition of the recognizance with conditions is likely to prevent the carrying out of the terrorist activity. As a result, the judge issues a recognizance with conditions.

The ATA, 2015 amended the provisions on recognizance with conditions and the terrorism peace bond. The amendments were designed to make it easier for police to apply to provincial court for the imposition of reasonable conditions, such as travel restrictions.

The 2015 amendments did the following:

- lowered the threshold to obtain a **recognizance with conditions** to where a peace officer believes on reasonable grounds that a terrorist activity “may be carried out.” Previously, the law required that police believe on reasonable grounds that a terrorist activity “will be carried out.” The amendments also replaced the former requirement that a recognizance is “necessary to prevent” the carrying out of a terrorist activity with “is likely to prevent.”
- increased the period of detention before a recognizance with conditions hearing is held to up to seven days, which includes periodic review by a judge. Previously, such detention could last only up to three days – a possible 24-hour police-initiated detention and a 48-hour judge-ordered detention.

Further periods of detention beyond the possible 24-hour initial police detention are allowed only if the judge finds that it is necessary to ensure public safety, to ensure that the person attends the hearing or to maintain confidence in the administration of justice. In addition, there are two new possible 48-hour periods of judge-ordered detention. In these instances, it must also be demonstrated that the investigation in relation to which the person is being detained is being conducted “diligently and expeditiously.” If these criteria are not met, the person must be released – with or without conditions – but will be required to return to court for the hearing on whether conditions should be imposed on them.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

- lowered the threshold to obtain a **terrorism peace bond** so that it may be obtained when a person believes an individual “may commit” a terrorism offence. Previously, the threshold was “will commit” a terrorism offence.
- for both the recognizance with conditions and the terrorism peace bond, there are now additional requirements for the judge to consider whether to impose a geographical restrictions condition on the person and whether to require the person to surrender their passport(s) or other travel documents.
- increased the length of time these measures can be applied if the person has been previously convicted of a terrorism offence. For the recognizance with conditions, the conditions can apply for up to two years. For the terrorism peace bond, the conditions can apply for up to five years.
- if a person breached their conditions under a recognizance with conditions or a terrorism peace bond, increased the maximum penalty to four years imprisonment (from a maximum of two years).
- sought to improve the efficiency and effectiveness of the recognizance with conditions and peace bonds across Canada by allowing for the use of video conferencing and for the transfer of peace bonds between provinces.

Potential Impacts on Charter Rights

The terrorism peace bonds and recognizance with conditions impact liberty interests protected under the *Charter*. Persons subject to these measures may face detention and other restrictions on their liberty without being charged with or convicted of an offence.

The consent of the Attorney General of Canada or of a province is required before the police can even apply to a judge for a recognizance with conditions or terrorism peace bond. In addition, the Crown or the affected person may apply to change any of the conditions. The recognizance with conditions also continues to be subject to a requirement to report annually on its use, whereas no similar reporting requirement applies in respect of the terrorism peace bond. Finally, the provisions on these recognizances are subject to a five-year sunset clause. This means that the recognizance provisions will no longer be in force five years after July 15, 2013, unless Parliament renews them.

Criminalizing the Advocacy or Promotion of Terrorism Offences in General

The ATA, 2015 added a new *Criminal Code* offence on advocating or promoting the commission of terrorism offences in general.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Consider a scenario...

Ms. K has also been attending Mr. A's weekly discussion groups. She feels that what Mr. A is saying should be known by more people and that Mr. A's views deserve a wider audience. To do this, Ms. K has started posting some of her views online. Over time, she has gained some followers on social media. She is now clearly stating that violence should be used as the only way to change the Government's position on foreign policy.

Ms. K has been communicating with some of her online followers. One has stated that they would be willing to "take direct action." In response to what she believes is support for her views, she decides to use her latest post to appear in a video message dressed in military clothing. In the video, she urges her followers to support a terrorist group by saying, "Do not wait for us to tell you what to do. From now on, you have permission to do whatever you want, do whatever is in your capability. Just act."

As noted above, the 2015 change to the *Criminal Code* makes it a criminal offence for a person, by communicating statements, to knowingly advocate or promote the commission of terrorism offences in general. To commit the offence, the person must *know* that any of those offences will be committed or *be reckless* as to whether any of those offences may be committed as a result of such communication.

Counselling generally involves one person procuring, soliciting or inciting another to commit a criminal offence. Counselling is a long-standing offence. It requires some specificity about the offence or type of offence being counselled.

The definition of "terrorism offence" in the *Criminal Code* includes a broad range of conduct – from violence against people and destruction of property to providing financial and material support and recruitment. Before the 2015 change to the *Criminal Code*, the scope of the offence of counselling was unclear. There was some uncertainty about whether it constituted counselling if a person actively encouraged committing terrorism offences but was not specific about the offences or the type of offences (for example, whether terrorist bombing or terrorist financing). There was also uncertainty about what the penalty would be. This new offence makes it clear that such conduct is criminal. The new offence is modelled on the existing law of counselling. It extends the concept of counselling to cases where no specific terrorism offence is being counselled, but where it is evident nonetheless that terrorism offences are being counselled.

The maximum penalty for the new offence is five years imprisonment. This is the same maximum as that for advocating or promoting genocide against an identifiable group, the most serious of the three hate propaganda offences in the *Criminal Code*.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Potential Impacts on Charter Rights

Because this offence criminalizes communicating statements, it could be viewed as limiting freedom of expression. However, it is important to consider that the expression in question is generally directed at violent activities. As well, this offence involves more than mere expression. The offence is not an attempt to criminalize glorification of terrorism or praise of terrorism. The offence prohibits active encouragement to commit terrorism offences, not mere expressions of opinion about the acceptability of terrorism.

To ensure appropriate oversight, the prior consent of the appropriate Attorney General is needed to begin proceedings in respect of terrorism offences.

Seizure and Forfeiture (or Removal) of Terrorist Propaganda

The ATA, 2015 created two new warrants of seizure (court orders that allow police to seize materials) in the *Criminal Code* to apply to “terrorist propaganda” material. This is material counselling the commission of a terrorism offence or advocating or promoting the commission of terrorism offences in general.

Related amendments to the *Customs Tariff* also allow CBSA border services officers to seize terrorist propaganda being imported into Canada without a warrant, as they would other contraband.

Some Canadians raised concerns about the definition of terrorist propaganda during the debate about the ATA, 2015. The Government has made a commitment to address the issue.

The new provisions allow a judge to order the seizure and forfeiture of terrorist propaganda material that is in printed form or is in the form of audio recordings. A judge may also order the removal of terrorist propaganda when it is in electronic form and is made available to the public through a Canadian Internet service provider (ISP).

Continuing the scenario from above...

Ms. K's posts on social media are made available through a Canadian ISP. Her posts have clearly been promoting the commission of terrorism offences in general.

With the consent of the Attorney General, the police seek a warrant from a judge requiring the Canadian ISP to remove this content from the site.

Potential Impacts on Charter Rights

The new warrants could impact the right to free expression. However, the warrants are similar to those already available under the *Criminal Code* for the seizure of material deemed criminal, such as hate propaganda. As well, the consent of the Attorney General is needed before the police can apply for a warrant, to ensure that the Attorney General considers public interest issues, such as protecting freedom of expression.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Protections for Witnesses and Other Justice System Participants

The ATA, 2015 introduced changes to the *Criminal Code* to improve protection of witnesses, in particular in proceedings involving security information or criminal intelligence information. Security certificate proceedings under the *Immigration and Refugee Protection Act* are examples.

The changes on how witnesses can testify include the following:

- Judges can order that witnesses testify behind a device, such as a screen, to prevent the public from seeing them while they testify;
- Judges must consider whether a witness has responsibilities relating to national security or criminal intelligence when deciding whether to allow that witness to testify using a pseudonym or via closed-circuit television; and
- Judges have explicit authority to make any order necessary to protect the security of any witness, including those who have responsibilities relating to national security. One such order could be to allow a witness to testify while partially disguised.

In addition, the ATA, 2015 amended the *Criminal Code* to better protect justice system participants from intimidation. The *Criminal Code* prohibits their intimidation and provides a maximum of 14 years imprisonment for the offence. The ATA, 2015 amended the *Criminal Code* to expand the definition of “justice system participant” to include persons who play a role in proceedings that involve various types of information, including security information and criminal intelligence information. This ensures that punishment for intimidation is proportional to the gravity of the conduct, its effect on the victims and, more broadly, its effect on the proper functioning of the justice system.

The ATA, 2015 also amended the *Criminal Code* to remove the requirement to publish the names of federally-designated prosecutors and peace officers who have obtained authorizations to intercept private communications (“wiretap” authorizations). This increases protection from intimidation or retaliation for federal prosecutors and law enforcement officers who obtain such authorizations. The amendment puts them in the same situation as their provincial counterparts. The Minister of Public Safety and Emergency Preparedness will continue to report annually to Parliament on the number of federally-designated prosecutors and peace officers who have obtained authorizations for wiretaps. This maintains ministerial accountability for their use.

Potential Impacts on Charter Rights

These measures on how witnesses can testify could impact the open court principle (the principle that information before a court ought to be public information as far as is possible), which is protected by the *Charter*, because the public is deprived of some information about the proceeding.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

These measures could also impact fair trial rights because some witnesses may testify behind a device shielding their identity.

What are other countries doing?

Terrorism Peace Bonds and Recognizance with Conditions

The recognizance with conditions and peace bond provisions are consistent with counter-terrorism laws in countries such as the UK and Australia.

The UK, for example, currently allows for pre-charge detention in respect of a terrorist offence for up to 14 days, which also requires independent review on grounds similar to those contained in the ATA, 2015. They also have a tool similar to a peace bond, called a Terrorism Prevention and Investigation Measure, which allows for the imposition of conditions on individuals where satisfied, on the balance of probabilities, that the individual is or has been involved in terrorism-related activity.

Australia also allows for preventative detention which, under federal law, can last for three days. Australian law also permits the imposition of "Control Orders," which are similar to peace bonds and which can result in the imposition of conditions on individuals where evidence establishes that, for example, making the order would substantially assist in preventing a terrorist act.

Advocacy or Promotion of Terrorism Offences in General

Since 2006, the UK has had an offence of direct or indirect encouragement to commit acts of terrorism. For the purposes of the offence, it is irrelevant whether the encouragement relates to one or more particular acts of terrorism or acts of terrorism generally. Indirect encouragement is defined to include a statement which glorifies the commission of such acts and which members of the public could reasonably be expected to infer that what is being glorified is being glorified as conduct that should be emulated by them in existing circumstances.

In 2014, Australia created a new offence of advocating the doing of a terrorist act or the commission of a terrorism offence, while being reckless as to whether another person will engage in a terrorist act or commit a terrorism offence. "Advocates" is defined to include promoting. It applies where one terrorism act or offence is being advocated or more than one of such acts or offences are being advocated. There are statutory defences that may apply depending on the circumstances, such as publishing in good faith a report or commentary about a matter of public interest. The maximum punishment is five years imprisonment.

As the Canadian offence in ATA, 2015 is based on the knowing and active encouragement of the commission of terrorism offences in general, it more closely resembles the Australian rather than the UK model.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Seizing Terrorist Propaganda

The measures are similar to laws that already exist in the UK and Australia. For example, the UK legislation, which allows for the takedown of websites and social media feeds, has been in existence since 2006. In Australia, complaints about on-line content are made to the Australian Communications and Media Authority (ACMA). If the ACMA determines that the content is restricted (i.e., if it incites violence or advocates a terrorist act), it issues a notice and takedown order to the service provider.

Protecting those Involved in National Security Proceedings/Prosecutions

The UK, New Zealand, and Australia have all developed legislative regimes that provide ways for witnesses to testify which seek to mitigate any adverse consequences that may arise from their giving testimony, while protecting the interests of an accused.

What do you think?

Are the thresholds for obtaining the recognizance with conditions and terrorism peace bond appropriate?

Advocating and promoting the commission of terrorism offences in general is a variation of the existing offence of counselling. Would it be useful to clarify the advocacy offence so that it more clearly resembles counselling?

Should the part of the definition of terrorist propaganda referring to the advocacy or promotion of terrorism offences in general be removed from the definition?

What other changes, if any, should be made to the protections that witnesses and other participants in the justice system received under the ATA, 2015?

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

PROCEDURES FOR LISTING TERRORIST ENTITIES

Listing an individual or group as a “terrorist entity” is a public means of identifying their involvement with terrorism and curtailing support for them. Listing is one component of the international and domestic response to terrorism.

There are three listing mechanisms in Canada. Two are established under Canada's *United Nations Act*²³ and a third was created by an amendment to the *Criminal Code* in 2001. Domestically, Canada relies mainly on the *Criminal Code* process. The *Criminal Code* process both helps to fulfill Canada's international obligations and supports domestic counter-terrorism measures. An entity listed under the *Criminal Code* fall under the *Criminal Code*'s definition of a terrorist group. Any funds the group has in Canada are immediately frozen and may be seized by, and forfeited to, government.

More than 50 terrorist entities are now listed under the *Criminal Code*. These include al-Qaida and Daesh. To date, most listed entities are based overseas, though members or supporters can also be found in Canada. Entities originating in Canada can also be listed.

The *Criminal Code* listing process begins with the RCMP or CSIS producing criminal or security intelligence reports on an entity. The Minister of Public Safety and Emergency Preparedness may recommend to the federal Cabinet that an entity be listed if the Minister has reasonable grounds to believe that the entity:

- knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or
- is knowingly acting on behalf of, at the direction of, or in association with an entity that has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity.

To list an entity, Cabinet must also be satisfied that the above test is met. The name of the listed entity is then published in the *Canada Gazette*. A complete list is available on Public Safety Canada's website.

Consider a scenario...

The 123 Group has committed terrorist attacks overseas and is being investigated by CSIS. CSIS informs Public Safety Canada about 123 Group's involvement in these attacks and its links to Canada. The Minister of Public Safety and Emergency Preparedness recommends to Cabinet adding the 123 Group to the list of terrorist entities established under the *Criminal Code* because the group has knowingly carried out a terrorist activity. Cabinet approves the listing. All financial assets

²³ These are the *UN Al-Qaida and Taliban Regulations* and the *Regulations Implementing the UN Resolutions on the Suppression of Terrorism*.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

belonging to 123 Group in Canada are frozen and can be seized by government.

The entity and the public are not made aware that the Government is planning to list the entity until the listing takes effect. This is to prevent the entity removing its Canadian assets from Canada before the listing freezes them.

Once an entity is listed, the *Criminal Code* deems it a “terrorist group” in Canada. This can help with investigating and prosecuting terrorism offences since it is not necessary for investigators and prosecutors to prove independently that the individual or group is a terrorist group. It is not a crime simply to be a terrorist group, but many *Criminal Code* terrorism offences contain the term “terrorist group” in the description of the offence. For example, it is an offence to do any of the following:

- knowingly participate in, or contribute to any activity of, a terrorist group for the purpose of enhancing the ability of any terrorist group to facilitate or carry out terrorist activity;
- leave Canada to participate in the activities of a terrorist group;
- collect money or property knowing that it will benefit a terrorist group; and,
- instruct anyone to carry out an activity for the benefit of a terrorist group.

The listing process also makes it easier to apply other provisions relating to terrorist groups, such as using the *Charities Registration (Security Information) Act* to de-register a charity or refuse to register an organization as a charity.

Canada's closest allies, including the U.S., UK, Australia and New Zealand, have similar terrorist listing regimes that include mechanisms for freezing assets in compliance with international obligations.

Potential Impacts on *Charter* Rights

Being listed as a terrorist entity or being associated with a terrorist entity could impact *Charter* rights. Specifically, section 7 of the *Charter* protects against the deprivation of life, liberty and security of the person, except in accordance with the principles of fundamental justice.

Procedural safeguards have been put in place because of the possible impact of a *Criminal Code* listing on these rights. An entity has the right to apply to the Minister of Public Safety and Emergency Preparedness to be de-listed. If the Minister decides not to de-list the entity, the entity can ask the Federal Court for judicial review of the Minister's decision.

Some of the evidence relating to the listing will be sensitive, and the Government may wish to protect it from being disclosed to the entity. However, this evidence can only be withheld from the entity if a Federal Court judge determines that its disclosure would injure national security or endanger the safety of any person. If evidence is withheld on these grounds, the judge must provide

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

an unclassified summary to ensure that the entity can understand the basis of the listing decision. As part of this process, the entity can also make submissions to the Federal Court. If the judge determines that the listing is unreasonable, he or she will order the entity to be de-listed.

The Government is also required to review all entities on the list every two years and confirm whether they should remain on the list.

Listing an entity could harm individuals and groups with a similar name. To prevent harm from mistaken identity, individuals and groups may apply to the Minister of Public Safety and Emergency Preparedness for a certificate confirming that they are not the entity on the list.

What are other countries doing?

Canada's closest allies all have similar terrorist listing regimes that include mechanisms for freezing assets in compliance with international obligations. UN Security Council (UNSC) Resolution 1267 and its successor Resolutions, including UNSC Resolution 2253, require states to freeze the assets of the Taliban, Usama bin Laden and his associates, members of Al-Qaida, and members of Daesh. The Resolution also imposes a travel ban and arms embargo against those listed by the UN. Canada implements UNSC Resolution 1267 through the *UN Al-Qaida and Taliban Regulations* and through the *Immigration and Refugee Protection Act*. UNSC Resolution 1373 requires states to freeze without delay, the financial assets of persons and entities engaged in terrorism. This obligation is primarily met in Canada by the list under the *Criminal Code*, but is also implemented through the *Regulations Implementing the UN Resolution on the Suppression of Terrorism*. The manner in which these international obligations are domestically implemented by Canada's allies has led to a variety of different terrorist listing regimes.

The UK, for example, implements its international obligations in relation to UNSC Resolution 1267 using regulations made pursuant to the *European Communities Act 1972*. UNSC Resolution 1373 is implemented under Part 1 of the *Terrorist Asset-Freezing etc. Act 2010*. As well, under the UK's *Terrorism Act 2000*, the Home Secretary may proscribe an organization if it commits or participates in acts of terrorism, prepares for terrorism, promotes or encourages terrorism or is otherwise concerned with terrorism. Membership in a proscribed organization is a criminal offence. Proscribed entities may apply to the Home Office to be de-listed and, if denied, an appeal process to a special commission, as well as judicial review of its decision, is available.

Australia, like Canada, has a listing process in its *Criminal Code*. The government may list an entity if the Attorney-General is satisfied on reasonable grounds that it is directly or indirectly engaged in preparing, planning, assisting or fostering the doing of a terrorist act, or advocates the doing of a terrorist act. The Australian government reviews listed entities every three years from the date that they were originally listed. Any person or organisation is entitled to make a de-listing application to the Attorney-General and judicial review of the legality of a decision to list an organisation is also available in the courts. Australia also implements UNSC Resolution 1373 by regulations made under

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

the *Charter of the United Nations Act 1945*, and implements UNSC Resolution 1267 by automatically incorporating the United Nations sanctions list by regulations made under the same Act.

New Zealand's *Terrorism Suppression Act 2002* provides for a list of terrorist entities to be established and maintained. The police are responsible for coordinating requests to the Prime Minister for designation of a terrorist entity. A designation in New Zealand, like in Canada, has the effect of freezing the entity's assets. It is also a criminal offence to participate in or support the activities of the designated terrorist entity. This includes dealing with the property of the designated terrorist entity or making property or financial services available to the entity. Also, New Zealand implements the UNSC Resolution 1267 and automatically incorporates the United Nations sanctions list by regulations made under their *United Nations Act 1946*.

The lists kept by the U.S. government are more complex and diverse. The U.S. implements its obligations relating to financial sanctions under both UNSCR 1267 and UNSCR 1373 primarily through Executive Order (E.O.) 13224. The Office of Foreign Assets Control administers and enforces E.O. 13224 and maintains a public list of groups and individuals designated under the Order as well as those designated under the *Immigration and Nationality Act* as Foreign Terrorist Organizations. There are some general similarities with Canada's listing processes. For example, entities are not informed that they may be listed and they cannot provide evidence or submissions before the listing process is completed.

What do you think?

The Government is interested in your views about the listing of terrorist entities.

Does listing meet our domestic needs and international obligations?

The *Criminal Code* allows the Government to list groups and individuals in Canada and abroad. Most listed entities are groups based overseas. On which types of individuals and groups should Canada focus its listing efforts in the future?

What could be done to improve the efficiency of the listing processes and how can listing be used more effectively to reduce terrorism?

Do current safeguards provide an appropriate balance to adequately protect the rights of Canadians? If not, what should be done?

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

TERRORIST FINANCING

Canada has a stable, open economy, an accessible and advanced financial system, and strong democratic institutions. However, those seeking to raise, transfer and use funds for terrorism purposes try to do so by exploiting some of these strengths. In confronting the evolving challenges of terrorist financing, the Government must ensure that it does not compromise fundamental Canadian values.

Terrorist financing is a multi-faceted global phenomenon. Terrorists (individuals and groups) raise, collect and transfer funds across the globe to carry out attacks and finance day-to-day operations. They raise funds from criminal activities and from legitimate sources, such as donations or business profits. Terrorists use a variety of methods to move their funds. These include the formal banking system, international trade, money services businesses, informal money transfer systems, digital platforms, and the physical transportation of cash or certain high value goods, such as gold or precious stones.

Individuals also finance terrorist activities by raising money themselves to travel abroad for terrorist purposes or to purchase materials for attacks. Since funds are vital to terrorist organizations, depriving them of these funds is one effective mechanism to counter terrorism.

For example, one of the five priorities of the Global Coalition against ISIL is to reduce Daesh's capabilities by cutting off its access to funding. Daesh is likely the wealthiest terrorist group in the world, due to its access to proceeds generated in the territory it controls. Its wealth allows it to carry out attacks, recruit and pay members, provide training and indoctrination, maintain communications networks and disseminate propaganda. Reducing access to funds will diminish Daesh's capability.

Canada's Approach to Counter Terrorist Financing

In Canada, the Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) regime involves 11 federal departments and agencies.²⁴ Together, they work to prevent, detect, deter, investigate and prosecute the financing of terrorist activities. A key component of Canada's regime is the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), which establishes FINTRAC.

The PCMLTFA imposes obligations on more than 31,000 financial service providers and financial intermediaries. The Act makes them active partners in the fight against money laundering and terrorist financing. Under the Act, these entities must keep certain records, know their customers, and report certain transactions to FINTRAC.²⁵ FINTRAC assesses entities' compliance with these

²⁴ Department of Finance, FINTRAC, the RCMP, the CBSA, CSIS, the Canada Revenue Agency, Department of Justice Canada, Public Prosecution Service of Canada, Public Safety Canada, Office of the Superintendent of Financial Institutions, and Global Affairs Canada.

²⁵ International electronic fund transfers (EFTs), cash transactions, disbursement from casinos over \$10,000; transactions suspected of being related to ML or TF; and terrorist property reports must be reported to FINTRAC.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

requirements and can fine them for non-compliance. FINTRAC also has the authority to analyze financial transaction reports and to disclose certain information to law enforcement and intelligence agencies if it has reasonable grounds to suspect that it would be relevant to the investigation or prosecution of a money laundering or a terrorist financing offence.

Law enforcement and intelligence agencies use this information and that from other sources to identify and disrupt terrorist activities. Law enforcement agencies can also lay criminal charges. The *Criminal Code* contains three terrorist financing offences. These prohibit (1) providing or collecting property for terrorist-related activities; (2) providing or making available property or services for terrorist purposes; and (3) using or possessing property for terrorist purposes. As noted earlier,²⁶ the *Criminal Code* also provides for a process to list individuals or groups as terrorist entities. The listing of a terrorist entity results in its property being frozen immediately. The property may then be seized and forfeited to the Government.

Consider a scenario...

Ms. L is a friend of Mr. A. She supports the 123 Group and wants to send it money abroad. Ms. L goes to a bank to send a wire transfer of \$11,000 to a country where it is known that 123 Group operates. Because the amount is more than \$10,000, the PCMLTFA requires the bank to report the transaction to FINTRAC. FINTRAC concludes that the transaction is suspicious (given its destination and other indicators) and provides the information to RCMP investigators.

Canada's Contribution to International Efforts

Terrorist financing is a global problem that requires a well-coordinated, multilateral response. The Financial Action Task Force (FATF), of which Canada is an active member, is an international organization that sets standards for combating money laundering and terrorist financing, which ensures all members' AML/ATF regimes are held to the same criteria. The FATF monitors the implementation of these standards among its own 37 members and the more than 190 countries in the global network of FATF-Style Regional Bodies through peer reviews and public reporting. The FATF is currently evaluating Canada against these standards and is expected to finalize and publish the results in summer 2016.

As well, Canada works with international partners through fora such as the United Nations, the G7/G20 and the Counter-ISIL Finance Group. Canada also implements several UNSC Resolutions to freeze and seize the assets of persons and entities engaged in terrorism. In addition, Canada supports regions where there is a higher risk for terrorist financing, such as the Middle East and North Africa. Canada does this through technical assistance on counter-terrorist financing. This

²⁶ See chapter "Terrorist Entity Listing Procedures"

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

assistance is designed to strengthen the capacity of financial systems in these regions to prevent them from being exploited as vehicles for terrorist financing.

Potential Impacts on Charter Rights

The current approach requires certain businesses to disclose private financial information to FINTRAC. FINTRAC may disclose it to law enforcement and intelligence agencies for investigation. This could impact privacy rights protected by section 8 of the *Charter*.

Because of the potential impact on section 8 privacy rights, the PCMLTFA has safeguards in place. For example, the Act prescribes the information that FINTRAC can receive and disclose. The PCMLTFA also identifies the law enforcement and intelligence agencies that can receive FINTRAC's financial intelligence. The Act also limits when FINTRAC can disclose information to these agencies. It must have reasonable grounds to suspect that the information would be relevant to the investigation or prosecution of a money laundering or a terrorist financing offence, or relevant to the investigation of threats to the security of Canada. FINTRAC is independent from law enforcement agencies and does not conduct investigations.

To ensure that the terrorist financing regime addresses emerging risks and maintains appropriate safeguards, Parliament reviews the PCMLTFA every five years. As well, the PCMLTFA requires the Privacy Commissioner of Canada to conduct a review of the measures taken by FINTRAC to protect information it receives or collects under the Act every two years. This is to ensure that FINTRAC protects the information it receives as part of its operations. The Privacy Commissioner reports the findings of the review to Parliament.

Finally, the Government continues to monitor its AML/ATF regime to ensure that it aligns with international standards and that it takes into consideration government policy priorities, including its impact on businesses and the rights of individuals.

Challenges

Canada's financial sector has evolved significantly since the PCMLTFA came into force in 2001. The Act has been amended several times in the past fifteen years, but staying current in the changing financial environment presents challenges. Financial technology is changing rapidly. The regime needs to keep pace with evolving techniques of using new platforms for illicit fundraising or financial transfers. In addition, the reporting thresholds under the Act may be set too high in terrorism matters. Banks and other financial institutions do not need to report to FINTRAC any transactions below these thresholds unless they deem them suspicious. For example, the \$10,000 threshold for reporting international funds transfers may be appropriate for investigations involving money laundering, but terrorists often transfer much smaller amounts. Enhanced coverage of new technologies and a lower reporting threshold would provide more information for investigations.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

However, it would also increase the personal information collected by FINTRAC, and the number of businesses required to report.

Consider a scenario...

Ms. L sends \$3,000 to a member of the 123 Group outside Canada. As the transaction is below the \$10,000 threshold, it is not reported to FINTRAC. The business transferring the funds has no information causing it to consider the transaction suspicious and so does not notify FINTRAC of the transaction. FINTRAC has no information to pass on to law enforcement agencies through legislated reporting mechanisms. Had FINTRAC known about the transfer, the PCMLTFA would have allowed it to inform law enforcement if it had reasonable suspicion that the transaction was related to the financing of a terrorist activity.

Terrorists are adaptable and may exploit weaknesses to avoid detection, impeding Canada's efforts to reduce terrorist financing. In addition, terrorists can procure goods or services without actual transfers of funds, limiting detection through the financial system. Terrorists have also used financial professionals with no ties with or sympathies for the terrorists' cause to help move money and resources between countries.

Terrorist financing investigations require extensive resources and significant sharing of information within Canada and with other countries. Investigation and detection also require cooperation within the private sector and between the private and the public sectors. Effective partnerships require a clear understanding by both the public and private sectors of terrorist financing methods and trends, to better and more accurately identify suspicious behaviour. These challenges suggest that an approach that adapts to technological advances and strengthens partnerships between government and the private sector, may be the most effective way to deny terrorists the resources they need.

What do you think?

The Government would like your views about how best to address gaps and other challenges in the regime.

What additional measures could the Government undertake with the private sector and international partners to address terrorist financing?

What measures might strengthen cooperation between the Government and the private sector?

Are the safeguards in the regime sufficient to protect individual rights and the interests of Canadian businesses?

What changes could make counter-terrorist financing measures more effective, yet ensure respect for individual rights and minimize the impact on Canadian businesses?

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

INVESTIGATIVE CAPABILITIES IN A DIGITAL WORLD

Evolving technology has changed the way Canadians communicate and live their lives. Canadians are increasingly active online. They may use multiple communications devices and a wide variety of tools such as email, Internet banking, instant messaging and various social media applications. This evolution provides enormous benefits for Canadian society, but criminals and terrorists can use these same technologies. Digital communications are now a fundamental tool for terrorism-related activities, including radicalization to violence, facilitation of travel for terrorist purposes, acquisition of funding and equipment, and even training for terrorist actions. The potential harm resulting from the exploitation of evolving technologies is not limited to national security. Traditional criminal activity – from planning violent crime to committing frauds – also relies on these technologies. New public safety challenges continue to appear via the Internet, such as the distribution of terrorist propaganda and child pornography, cyberbullying, and the “Dark Web” and its associated criminal marketplace.

Digital information is sometimes more important than physical evidence or intelligence in investigating national security threats, solving crimes and prosecuting offenders.

To protect Canadians from crime or threats to safety and security, Canada's law enforcement and national security investigators must be able to work as effectively in the digital world as they do in the physical. Law enforcement must also have the ability to cooperate effectively with their international partners who seek digital evidence from Canada to further their criminal investigations and prosecutions. The laws governing the collection of information and evidence have not, however, kept pace with the rapid advancements of digital technology in the last 20 years and the role technology plays in the lives of Canadians today. Whether information comes from more traditional sources or from within the increasingly complex digital landscape, investigators need access to that information to investigate threats to national security and criminal activity, and to cooperate with foreign partners in a timely manner.

The term “lawful access” has been used as an umbrella term to refer to certain legally authorized procedural powers and techniques, as well as criminal laws, which may come into play when national security and law enforcement agencies conduct investigations. The Government has attempted to ensure that investigative tools are adequate to deal with new forms and uses of technology. These efforts have included multiple public consultations on “lawful access”²⁷ and updating cybercrime

²⁷ These include the 2002-2003 Lawful Access Consultations, details of which can be found at www.justice.gc.ca/eng/cons/la-al/index.html.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

and cyberbullying laws through the *Protecting Canadians from Online Crime Act*.²⁸ Canada's digital environment, however, continues to change dramatically. More data has been created in the last five years than ever before. As we move forward, discussions of the investigative capabilities of law enforcement and national security agencies in a digital world must take into account technological advances, the legal context and the current threat environment.

Potential Impacts on Charter Rights

Access by national security and law enforcement agencies to digital communications, information for investigative or intelligence purposes, or both, could impact the privacy rights protected by the *Charter*. Some aspects of the issues discussed here could also impact freedom of expression or the right against self-incrimination, also protected under the *Charter*.

These issues are complex. Each raises specific concerns about its intersection with considerations of security and individual rights, including privacy. International and economic considerations also come into play.

Challenges

In the physical world, law enforcement and national security agencies use a variety of tools to collect information and evidence to further their investigations and to assist foreign counterparts. The *Criminal Code* and other statutes, such as the *CSIS Act* and the *Mutual Legal Assistance in Criminal Matters Act*, authorize the use of these tools. For example, investigators at a crime scene may look for physical evidence such as DNA, fingerprints, weapons or other items of importance that may relate to the crime. In the digital world, investigators use other tools to collect digital information and evidence. In the digital world, investigators may be looking for information and evidence (data) such as online addresses (website or IP addresses), the types of communication that took place, with whom, and for how long.

Law enforcement and national security agencies obtain access to such data as authorized by law. However, the legislation providing for certain investigative tools may not be adequate to deal with the complexity, diversity, and rapid pace of change in the digital world. Current challenges impacting investigative capabilities include the following:

- lack of consistent and timely access to **basic subscriber information** to help identify the subscriber to a communications service;

²⁸ Some of the measures introduced by this Act were new production orders that allow for authority to obtain tracking data, tracing communication, and transmission data, new powers for preservation of data, and the creation of a new offence for the non-consensual distribution of intimate images, known as "revenge porn." The Act also introduced measures to adapt some existing investigative tools to current technology and aligned those changes with privacy safeguards and requirements for judicial oversight.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

- lack of consistent and reliable technical **intercept capability** on domestic telecommunication networks;
- diminished ability to investigate due to the use of **encryption**; and
- inconsistent **retention** of communications data.

These challenges are discussed in order below.

In addition, cyberspace is not easily bound by domestic borders and laws. Many communications service providers (CSPs) have no infrastructure or business presence in Canada, but provide Internet-based communications services. These providers operate in Canada but may fall beyond the reach of Canadian law. This can cause significant challenges and delays for law enforcement and national security agencies in acquiring the information necessary to advance investigations. It can also lead to critical intelligence and evidence being unobtainable.

Basic Subscriber Information

Consider a scenario...

There is suspicion that Mr. A. has inspired Mr. M. to begin planning a terrorist attack in Canada with an unidentified person. Much of Mr. M's collaboration happens through exchanges over the Internet, such as through online forums.

As part of the investigation of this suspicious activity, a police officer wants to request the identity (basic subscriber information) related to a particular Internet Protocol (IP) address that has been involved in these online exchanges. However, to get the information from the Internet service provider (ISP), the officer would need a court order. The officer is in the early stages of the investigation and does not have enough information to meet the threshold for obtaining this court order, since getting an order requires more than suspicion that the activities are taking place. As a result, the officer is unable to pursue an investigative lead in a timely and effective manner.

"Basic subscriber information" (BSI) consists of basic identifying information that corresponds to a customer's telecommunications subscription. This can include name, home address, phone number, email address, and/or IP address. BSI does not include the contents of communications. BSI provides law enforcement and national security agencies with key information. This information is particularly useful at the outset of an investigation and may also be used to follow investigative leads. The information allows the police and national security agencies to identify an individual.

In 2014, in *R. v. Spencer*, the Supreme Court of Canada decided that the police could not request the name and address of a person in relation to his or her IP address where it would reveal intimate details of his or her anonymous online activities, except in an emergency situation or pursuant to a reasonable law. The Court concluded that the manner in which the police in this case obtained such information interfered with privacy interests protected by the *Charter*.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Without specific legislation designed to permit access, law enforcement and national security agencies have had difficulty getting timely and effective access to BSI since the *Spencer* decision. As a result, law enforcement agencies have used tools already available in the *Criminal Code*, such as general production orders. These tools are designed for a larger search scope. They are meant for situations such as seeking the complete browsing history, medical records or financial history of an individual. Because of this a high degree of judicial scrutiny is necessary.

The use of these tools for BSI presents the following challenges, especially during early stages of an investigation:

- The information needed to apply for a court order -- for example, a general production order -- may not be available at the beginning of an investigation. The existing information may not attain the threshold required for a court to grant an order.
- The process to obtain a search warrant or a general production order can be slow and involve considerable work and resources. The process has requirements that may be disproportionate when the only information investigators are seeking is BSI, even if the requirements are proportionate in other situations involving greater privacy intrusions.

As a result of these challenges, key evidence may be lost and opportunities to prevent a crime from happening missed. A tool designed to access BSI specifically could, with appropriate safeguards, both enhance investigative capabilities and respect privacy interests.

Laws in many foreign jurisdictions specifically permit law enforcement and national security agencies to obtain BSI. In many cases, this can occur without prior judicial authorization (generally, obtaining BSI without prior judicial authorization is called administrative access). These foreign jurisdictions include the U.S., the UK, Australia, Germany, Sweden, Ireland, Denmark, Spain, Finland, the Netherlands and Norway.

The laws and regulations in these jurisdictions vary in how they limit and safeguard administrative access to BSI. Some jurisdictions give certain agencies access to BSI administratively but require other agencies to obtain judicial authorization first. In some cases, a general administrative scheme for obtaining BSI operates, but an order from a judge may be required under certain conditions. These conditions requiring a court order may include when BSI is stored as part of a data retention requirement, or when certain categories of BSI are sought, such as an IP address or other data unique to mobile cellular devices, such as an International Mobile Subscriber Identity (IMSI) number. Other limitations in getting administrative access to BSI include requirements for senior police officers to approve requests and limiting BSI access to certain types of crime, or including prosecutors in the process to obtain some types of BSI.

Any measures to address the need for consistent and timely access to BSI would have to take into consideration the investigative needs of law enforcement and national security agencies and the

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

impact of those measures on industry. The measures would also have to protect privacy rights in accordance with the *Spencer* decision.

Interception Capability for Communications Services

Law enforcement and national security agencies intercept private communications under the *Criminal Code* and the *CSIS Act* to obtain communications when investigating certain crimes (as listed in the *Criminal Code*) or threats to national security. Each Act sets out procedures to obtain judicial authorization to use interception techniques. These procedures are designed to uphold privacy rights.

Law enforcement and national security agencies obtain the necessary court orders to intercept communications. However, in some cases CSPs may not be able to perform the interception because the technical capability to intercept communications has not been built into their infrastructure. This hinders investigations that are being pursued under judicial authorization. In turn, this can prevent law enforcement and national security agencies from fulfilling their mandates.

Canada does not impose a general legal requirement for CSPs to have interception capabilities on their networks. Many other countries do. Australia, the U.S., the UK and many other European nations require CSPs to have an interception capability. In the U.S., for example, the *Communications Assistance for Law Enforcement Act*, usually referred to as CALEA, imposes this obligation. The U.S. Federal Communications Commission website explains CALEA.²⁹ Because of CALEA, traditional voice switches in the U.S. today include an intercept feature.

Continuing the scenario from above...

The investigation has now proceeded to a point well beyond suspicion and the police have received an authorization from a judge to intercept the communications of Mr. M.

However, when the police contact the telecommunications service provider, they learn that the service provider has not built a capability to intercept communications into its infrastructure. The service provider cannot complete the work required to develop and implement this intercept capability before the authorization expires. As a result, the police miss out on obtaining key evidence, even though they had court authority to intercept the communications.

Several issues need to be taken into account when discussing whether to require CSPs to introduce intercept capability. These include the impact on privacy, the investigative needs of law enforcement and national security agencies, and how introducing requirements for intercept capability may affect the costs and competitiveness of industry.

²⁹ <https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance>

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Encryption

Encryption converts a readable electronic message into an unreadable message. To decrypt the message (make it readable again), the reader must use one or more specific decryption “keys.” Encryption is widely regarded as a best practice to enhance security and protect privacy online. It is commonly used to protect individual messages, personal devices and transmission channels. Secure encryption is also vital to cybersecurity, e-commerce, data and intellectual property protection, and the commercial interests of the communications industry. Canada's policy on cryptography (established in 1998) underlines the importance of encryption to the viability, stability and growth of the economy and e-marketplace and encourages the use of encryption to protect privacy, personal information and data. Today, free encryption technologies and services are widely available. These include encryption that often operates without the users' knowledge or need to activate it. Encryption technologies may be built in to a user's communication service.

However, encryption technology also helps criminals and terrorists to avoid discovery, investigation and prosecution by making their communications unreadable to investigators. The international availability of encryption tools and the complexities of encryption make law enforcement and national security investigations more difficult. They also pose challenges for law enforcement working with foreign partners in fighting serious international crimes.

It is difficult to address the problematic use of encryption without also reducing its benefits. As a result, very few countries have proceeded to limit encryption through legislation in the interests of protecting law enforcement and national security agency capabilities. This is despite the challenges posed by encryption for law enforcement and national security agencies being well known. Encryption has been the subject of concern and discussion in many jurisdictions since the 1990s.

The UK is among the few countries to impose limits on encryption through law – in this case, the *Regulation of Investigatory Powers Act, 2000*. The Act gives legally authorized persons (such as law enforcement and national security agencies) the authority to serve notices on individuals or bodies requiring the disclosure of protected (for example, encrypted) information in an intelligible form. This can be done through decryption or disclosure of encryption keys that the person is believed to hold. These provisions have attracted controversy.

In the 1990s, a series of legislative initiatives (sometimes referred to as “Clipper Chip” proposals) were suggested in the U.S. to impose built-in decryption capabilities. These proposals were highly controversial and attracted vigorous opposition from privacy and civil liberties groups and from groups concerned about the potential damage to industry. None of these proposals became law. However, vigorous debate about encryption continues in the U.S., as do concerns of law enforcement about encryption. This was seen most recently in the controversy that arose when the U.S. government asked Apple to help it obtain information contained on a phone associated with the San Bernardino terrorist incident.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Continuing the scenario from above...

The police were finally able to develop intercept capability and obtain court authority again to intercept the communications of Mr. M.

To avoid having his plans discovered, however, Mr. M had encrypted his communications, which were unreadable to the police as a result. In addition, the service provider advised the police that it could not help decrypt the communications. After months of investigative delays and despite court authority to intercept the communications of Mr. M, the police cannot read them to obtain potential evidence. As a result, Mr. M's communications remain protected from law enforcement.

Even when law enforcement or national security agencies can intercept a communication, with assistance from a service provider under a court order, the data that is obtained is often unreadable due to the layers of encryption that cannot be decrypted or otherwise removed. Encryption challenges also apply to the court-ordered production of historical data, such as email, text messages, photos and videos from lawfully seized smartphones, computer hard drives and other digital devices. Since encryption can be used by anyone, a private sector organization may not be able to help law enforcement and national security agencies decrypt communications because the organization might not have the technical ability to decrypt material encrypted by someone else.

No provisions specifically designed to compel decryption are found in the *Criminal Code*, the *CSIS Act* or in other Canadian laws. In other words, there is no law in Canada designed to require a person or organization to decrypt their communications.

Discussion about encryption and decryption must take into account the potential impact on the following:

- human rights, including privacy rights, freedom of expression, and the right against self-incrimination;
- the investigative needs of law enforcement and national security agencies;
- commercial interests, such as competitiveness and the protection of intellectual property;
- how compelling decryption could weaken existing IT infrastructure models and systems;
- cybersecurity; and
- e-commerce.

Data Retention

“Data retention” refers to the general requirements to store certain elements of subscribers’ telecommunications data, such as telephone numbers dialed, call length, time of call, and Internet equivalents, for the purpose of supporting law enforcement and national security investigations. These data can provide key pieces of information and evidence. Data retention ensures that this

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

information will be kept for a specified period so that law enforcement and national security agencies can obtain this information with a warrant, if required for an investigation. To date, Canada has not pursued a telecommunications data retention requirement for law enforcement and national security purposes.

Continuing the scenario from above...

As part of its ongoing investigation, the police learn that Mr. M had used his mobile phone over three weeks in July 2015 to communicate with individuals linked to terrorist groups. The police seek a court order to obtain telecommunications data associated with Mr. M's mobile phone account. However, the company keeps records for business purposes only for nine months. As a result, the company has already deleted data from July 2015 and the data are not available to the police.

Parliament recently introduced *preservation* powers into the *Criminal Code* when it enacted the *Protecting Canadians from Online Crime Act*. These powers allow law enforcement agencies to seek a court order or demand the preservation of specific computer data belonging to specific persons for a brief time to assist in investigations.

However, some business practices are changing and companies are deleting data more quickly than before, sometimes before law enforcement can seek a court order for or demand preservation. In addition, the length of time data is held varies from company to company. General data retention requirements would provide for companies to keep data for a standardized period. However, this might mean that companies have to store data for longer than they require strictly for business purposes. Requiring data retention for a given period could also increase risks to personal information held by companies. The longer personal information is kept, the longer it is vulnerable to attack.

General requirements for data retention already exist in some foreign jurisdictions or have been proposed or debated there. In the U.S., some data retention bills have been introduced in Congress, but none have been enacted. Australia recently enacted data retention requirements. On March 15, 2006, the European Union (EU) issued a Data Retention Directive (DRD) to impose data retention requirements for telecommunications data on its member states.

The DRD required that data retention be implemented through legislation enacted by EU member states at the national level. The manner of the implementation varied significantly among member states, in part because of controversy over these requirements in some states. On April 8, 2014, the Court of Justice of the European Union struck down the DRD, calling it inconsistent with privacy rights in Europe.

EU member states are now looking at their respective national laws to determine if and how their national laws on data retention need adjustment after the court decision. Some countries, such as Germany, have already introduced changes. The Federal Constitutional Court of Germany declared

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

the country's own domestic legislation unconstitutional in March 2010. A new data retention law came into effect in Germany on January 4, 2016. The law introduced many safeguards, such as reducing the obligation to retain data from six months to ten weeks and restricting access to such data to cases involving "serious crimes" only.

The discussion of telecommunications data retention requirements should take into account several issues, including the following:

- the investigative needs of law enforcement and national security agencies;
- the impact on privacy interests; and,
- the impact on the costs and competitiveness of companies resulting from data retention requirements.

What do you think?

How can the Government address challenges to law enforcement and national security investigations posed by the evolving technological landscape in a manner that is consistent with Canadian values, including respect for privacy, provision of security and the protection of economic interests?

In the physical world, if the police obtain a search warrant from a judge to enter your home to conduct an investigation, they are authorized to access your home. How should investigative agencies operate in the digital world?

Currently, investigative agencies have tools in the digital world similar to those in the physical world. As this document shows, there is concern that these tools may not be as effective in the digital world as in the physical world. Should the Government update these tools to better support digital/online investigations?

Is your expectation of privacy different in the digital world than in the physical world?

Basic Subscriber Information (BSI)

Since the *Spencer* decision, police and national security agencies have had difficulty obtaining BSI in a timely and efficient manner. This has limited their ability to carry out their mandates, including law enforcement's investigation of crimes. If the Government developed legislation to respond to this problem, under what circumstances should BSI (such as name, address, telephone number and email address) be available to these agencies? For example, some circumstances may include, but are not limited to: emergency circumstances, to help find a missing person, if there is suspicion of a crime, to further an investigative lead, etc... Do you consider your basic identifying information identified through BSI (such as name, home address, phone number and email address) to be as private as the

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

contents of your emails? your personal diary? your financial records? your medical records? Why or why not?

Do you see a difference between the police having access to your name, home address and phone number, and the police having access to your Internet address, such as your IP address or email address?

Interception Capability

The Government has made previous attempts to enact interception capability legislation. This legislation would have required domestic communications service providers to create and maintain networks that would be technically capable of intercepting communications if a court order authorized the interception. These legislative proposals were controversial with Canadians. Some were concerned about privacy intrusions. As well, the Canadian communications industry was concerned about how such laws might affect it.

Should Canada's laws help to ensure that consistent interception capabilities are available through domestic communications service provider networks when a court order authorizing interception is granted by the courts?

Encryption

If the Government were to consider options to address the challenges encryption poses in law enforcement and national security investigations, in what circumstances, if any, should investigators have the ability to compel individuals or companies to assist with decryption?

How can law enforcement and national security agencies reduce the effectiveness of encryption for individuals and organizations involved in crime or threats to the security of Canada, yet not limit the beneficial uses of encryption by those not involved in illegal activities?

Data Retention

Should the law require Canadian service providers to keep telecommunications data for a certain period to ensure that it is available if law enforcement and national security agencies need it for their investigations and a court authorizes access?

If the Government of Canada were to enact a general data retention requirement, what type of data should be included or excluded? How long should this information be kept?

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

INTELLIGENCE AND EVIDENCE

National security information needs to be protected from unnecessary public disclosure. At the same time, there is a need to facilitate its use in legal proceedings, when appropriate, while maintaining the fairness of the proceedings and the integrity of the justice system.

The challenge is significant in criminal and related proceedings involving constitutionally protected interests. National security information might also, for example, be important in advancing or defending against a civil case. The Government might also use such information when making administrative decisions, which in turn can be judicially reviewed.

When national security information is involved—or potentially involved—in a legal proceeding, it brings into play issues of fundamental justice, the rule of law and the confidence of Canadians in the justice system. The potential disclosure of national security information may also limit the effectiveness of national security agencies and make it more difficult to assure foreign partners that national security information they have shared with Canada is protected.

Key Principles

The discussion of intelligence and evidence raises several important principles, including the following:

- the requirement that laws be consistent with the *Charter*;
- the obligation of the Government to protect sensitive sources, capabilities and techniques, and its relationships with international partners, in the interests of national security and international relations;
- the ability of courts and tribunals to consider as much relevant material as possible to ensure that judgments are based on a complete picture of the facts and that justice is done; and
- the need for legislative tools to be flexible enough to apply in a broad range of circumstances.

Section 38 of the *Canada Evidence Act* (CEA) provides the framework for the disclosure and use of national security information in a broad range of legal proceedings. Under section 38, a Federal Court judge must assess whether or not the disclosure would be injurious to international relations, national defence or national security. If disclosure would be injurious, the judge must then consider whether the public interest in disclosure outweighs the public interest in non-disclosure. The process under section 38 of the CEA is conducted in the Federal Court even though, for example, the information may relate to a proceeding in a different court.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

This two-part process, also known as a bifurcated process, has been the subject of criticism.

The Supreme Court of Canada concluded that this bifurcated approach is constitutional in a criminal proceeding (*R. v. Ahmad (2011)*). Still, the Court invited the Government to consider its policy choice of using a bifurcated system. The issues surrounding intelligence and evidence have also been addressed in a number of reports, including reports of parliamentary committees and the Air India Inquiry.³⁰ Intelligence and evidence has also been the subject of consultations in New Zealand and the UK.

Intelligence and evidence issues can be expected to continue to arise for several reasons, including that a number of federal agencies are involved in national security investigations. In some cases, the need for cooperation between federal institutions has resulted in an increasing number of government actions being informed by national security information.

Criminal Proceedings

The Federal Court does not hear criminal cases, unlike the criminal courts in the provinces and territories. However, issues relating to the disclosure of national security information in these cases are largely addressed by Federal Court judges.

This means that, in some instances, the criminal court in a province may be unable to see the national security information and may only be able to rely on unclassified summaries provided by the Federal Court.

In other cases, the Attorney General of Canada, in consultation with investigating agencies, may allow disclosure in court of national security information under certain conditions, determined case by case. However, these proceedings are unable to incorporate the protections for national security information built into the *Canada Evidence Act*. Nor can they benefit from using the Federal Court's secure facilities or relying on its administrative expertise in handling national security information.

Consider a scenario...

After a long investigation, the RCMP lay criminal charges in the superior court of the province against Mr. M for planning a terrorist attack. Information provided by CSIS was essential to the RCMP investigation. This information was obtained from a foreign agency, which provided it on condition that it not be further disclosed without the agency's consent. The foreign agency refuses to consent to the disclosure. Revealing this national security information without the foreign agency's consent would damage CSIS's relationship with it.

To protect against the disclosure of the information provided by the foreign agency, the Attorney General of Canada makes an application under the *Canada Evidence Act* for the Federal Court to decide whether it is in the public interest to protect or disclose the information. The Federal Court judge decides to protect the national security information, which means that the actual information

³⁰ Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

will not be given to the judge of the superior court or be relied on during the prosecution.

However, the judge of the Federal Court also decides to prepare an unclassified summary of the information, which is provided to Mr. M and the judge of the superior court. Mr. M uses this summary to defend himself against the charges and the judge of the superior court may consider it during the proceedings. Because this information is an important part of the prosecution's case, not being able to rely on the complete information in the superior court could cause the prosecution to fail.

National security agencies collect information to advise government, but the information is not generally intended to be used as evidence. In some circumstances, the obligation on the prosecutor to make disclosure in criminal cases may require the prosecutor to approach these agencies to see if they have information relevant to the case. The prosecutor must do this even if the agencies did not provide that information to law enforcement for the criminal investigation. This is one way for national security agencies to get drawn into criminal proceedings.

Potential Impacts on Charter Rights

When trying to protect national security information in a criminal case, the Government must ensure that any measure to do so is consistent with the *Charter*.

An individual accused of a crime has a right to a fair trial, including the right to make full answer and defence. This involves broad access to information that relates to the investigation and charges. The accused also has a right to be present throughout the trial. Finally, the open court principle protected by the *Charter* may come into play when national security information is used in a criminal trial.

Civil Proceedings

National security information may be relevant in a civil proceeding and can sometimes be central to a proceeding. Where national security information is involved, a plaintiff may be unable to make its case, and a defendant may be unable to defend itself, because the information needed to establish the case or defend against a claim needs to be protected. This situation can arise when the federal government is sued for allegedly wrongful conduct, when it is the plaintiff, or in proceedings where the federal government is not at all involved (for example, a dispute between two private companies).

If a judge is unable to take into account the national security information in the civil proceeding, justice may not be served. The lack of relevant information could lead to damage to someone's reputation, costly settlements or loss of public confidence in the legal system.

To protect the national security information from being disclosed to the court and non-governmental parties, the same bifurcated process under the *Canada Evidence Act* described for the criminal process above applies to civil proceedings.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Potential Impacts on Charter Rights

Unlike criminal proceedings, civil proceedings do not automatically bring the *Charter* right to liberty into play. However, parties in civil proceedings generally have a right to documents that contain relevant information that either directly or indirectly advances or damages the case of one party or another. The protection of national security information from disclosure in a civil case could make it difficult to successfully pursue, or defend against, *Charter* claims.

Administrative Proceedings

Many federal administrative decision makers might rely on national security information in their work. These decision makers include federal government officials, ministers, boards and administrative tribunals. The decisions involve a wide variety of matters, such as issuing or revoking permits or licences. For example, decisions about issuing passports are considered administrative proceedings.

As in criminal and civil proceedings, national security information must be protected in administrative and related proceedings, while at the same time the proceedings must ensure fairness. Section 38 of the *Canada Evidence Act* provides a general regime for protecting national security information in some of these situations. Challenges similar to those outlined in the criminal and civil contexts exist here as well.

Apart from section 38 of the *Canada Evidence Act*, a number of specific regimes, varying slightly in their procedures, allow for the protection and use of the national security information during proceedings. Immigration proceedings are one example.

Potential Impacts on Charter Rights

Procedural fairness requirements vary depending on the nature of the administrative decision. The content of the duty of fairness, which includes the rights to know the case to meet and to respond in a meaningful way, varies depending on the rights and interests at stake. Even when *Charter* rights are significantly impacted, the right to know the case to meet is not absolute.

Proceedings under the *Immigration and Refugee Protection Act (IRPA)*

In making immigration decisions, the Government must sometimes rely on classified information (that is, information that if disclosed would be injurious to national security or endanger the safety of a person) to determine whether foreign nationals and permanent residents may enter or remain in Canada (whether they are “admissible”). Division 9 of the IRPA allows the Government to protect and use this information during immigration proceedings. The best known of these Division 9 proceedings are commonly called security certificate proceedings.

The certificate is a document, signed by the Minister of Public Safety and Emergency Preparedness and the Minister of Immigration, Refugees and Citizenship. It states that there are reasonable

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

grounds to believe that the named person is inadmissible to Canada for reasons of security, violating human or international rights, serious criminality or organized criminality. The certificate is referred to a judge of the Federal Court to determine its reasonableness. The proceedings at the Court have two parts:

- (1) public proceedings, where the person named in the certificate, along with their counsel, receive non-classified information and an unclassified summary of the classified information that is part of the certificate; and,
- (2) closed proceedings, where the public, the person named in the certificate and their counsel are not present and a court-appointed special advocate (a private lawyer with an appropriate security clearance) receives the classified and non-classified information relevant to the certificate and protects the interests of the named person.

Consider a scenario...

Ms. N is a permanent resident currently in Canada. CSIS has classified information from sources within Canada, as well as from an international partner, that shows Ms. N is part of a terrorist group and a danger to the security of Canada. She has been attending Mr. A's meetings. CSIS provides this information to the Minister of Public Safety and Emergency Preparedness and the Minister of Immigration, Refugees and Citizenship. The ministers decide to sign a security certificate and a warrant for her arrest. The certificate and warrant are filed with the Federal Court. The security certificate process protects the classified information from being disclosed while allowing it to be used by the Federal Court judge, who must determine if the certificate is reasonable.

Potential Impacts on Charter Rights

A person's rights under the *Charter* are engaged by security certificate proceedings. These include the right not to be deprived of liberty and security of the person, except in accordance with the principles of fundamental justice. These principles include the right to a fair hearing, and the right to know the case to meet and to answer that case.

To protect these rights, the law provides certain safeguards. During closed proceedings, special advocates protect the interests of the person named in the certificate. They can challenge government claims that information cannot be disclosed, as well as the relevance, reliability and sufficiency of the information and evidence in the case. Special advocates can make submissions to the Court, cross-examine witnesses during the closed proceedings, and exercise any other power the judge authorizes.

Also, whenever a person is subject to detention or conditions under a warrant, the Court reviews this detention or these conditions on a regular basis (at least once every six months).

Finally, judges ensure the fairness of these proceedings and decide whether the security certificate is reasonable. The Supreme Court of Canada, in the *Harkat* decision, stated that the "judge is intended to play a gatekeeper role, is vested with broad discretion and must ensure not only that the record

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

supports the reasonableness of the ministers' finding of inadmissibility, but also that the overall process is fair.”³¹

The ATA, 2015 changed three aspects of Division 9 of IRPA proceedings (e.g. security certificates):

- The Government can immediately appeal when a judge orders the public disclosure of information that the Government considers must remain classified;
- The information that the ministers must file with the Federal Court is that which is relevant to the ground of inadmissibility on which the certificate is based and which allows the person to be reasonably informed of the case; and,
- The Government may ask the judge for an exemption from providing some classified information to the special advocate (as part of the disclosure of relevant information in closed proceedings). The judge may grant this exemption only if satisfied that the exempted information would not enable the person to be reasonably informed of the Government's case. The judge is permitted to consult with the special advocates about the information before making this decision.

Continuing the scenario from above...

During the security certificate process for Ms. N, the Federal Court judge decides that some of the classified information should be disclosed publicly. The Government appeals this decision immediately because releasing this information would harm national security. The Federal Court of Appeal reviews the decision to disclose the information. The Federal Court of Appeal decides to protect the information and the case continues without it being disclosed.

What are other countries doing?

Australia, New Zealand, the UK and the U.S. face the same challenges of handling intelligence and evidence in their court systems. In criminal matters, for the most part, courts work from legislated roadmaps to protect national security information and maintain an adversarial legal system.

In general, Australia and the U.S. allow private (non-government) counsel to be security-cleared and have access to national security information in representing their clients. New Zealand and the UK have developed surrogates: special counsel acting as alternatives to disclosure of the national security information to the person involved.

In civil litigation involving the potential disclosure of national security information, some countries differ if national security information is sought to be used as evidence. In the U.S., a legal concept known as the common law State Secrets Privilege has evolved. This permits hearings behind closed

³¹ *Canada (Citizenship and Immigration) v. Harkat*, 2014 SCC 37.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

doors without the affected person or the person's counsel being present which can result in the summary dismissal of claims based on the potential disclosure of state secrets. Elsewhere, including in Australia, procedures established by legislation allow for the substitution of national security information with summaries, admissions of fact or limited disclosure (where possible). Finally, the UK has legislated closed civil proceedings where the judge may review and rely on national security information tendered in closed proceedings, with the interests of the non-government party represented by a special advocate.

Senior administrative tribunals in Australia, the UK and New Zealand consider complaints involving security agencies as a part of their broad supervisory roles. Given their mandate, these senior administrative tribunals involve sitting judges.

What do you think?

Do the current section 38 procedures of the *Canada Evidence Act* properly balance fairness with security in legal proceedings?

Could improvements be made to the existing procedures?

Is there a role for security-cleared lawyers in legal proceedings where national security information is involved, to protect the interests of affected persons in closed proceedings? What should that role be?

Are there any non-legislative measures which could improve both the use and protection of national security information in criminal, civil and administrative proceedings?

How could mechanisms to protect national security information be improved to provide for the protection, as well as the reliance on, this information in all types of legal proceedings? In this context, how can the Government ensure an appropriate balance between protecting national security and respecting the principles of fundamental justice?

Do you think changes made to Division 9 of the IRPA through the ATA, 2015 are appropriately balanced by safeguards, such as special advocates and the role of judges?

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

CONCLUSION

Canada, like other countries, faces national security threats. The threat of terrorism, by global and by domestic actors, is real and evolving. More people are radicalizing to violence. Some are leaving Canada to join terrorist groups overseas, while others focus their attention on Canada itself. Canadians expect the Government to keep them safe. At the same time, the Government must comply with the rights enshrined in the *Charter*.

The issues described in the Green Paper and this background document relate to major components of our counter-terrorism framework. Some chapters discuss measures already in place. Certain chapters highlight current gaps, while others explain where the Government would like to take action. We hope that this information helps Canadians understand this complex area as we begin consultations with them about how best to respond.

Government counter-terrorism actions undoubtedly impact rights protected under the *Charter*.

Views will differ on what are justifiable and reasonable impacts. There will also be strong opinions on the tools we should employ and how they should be employed.

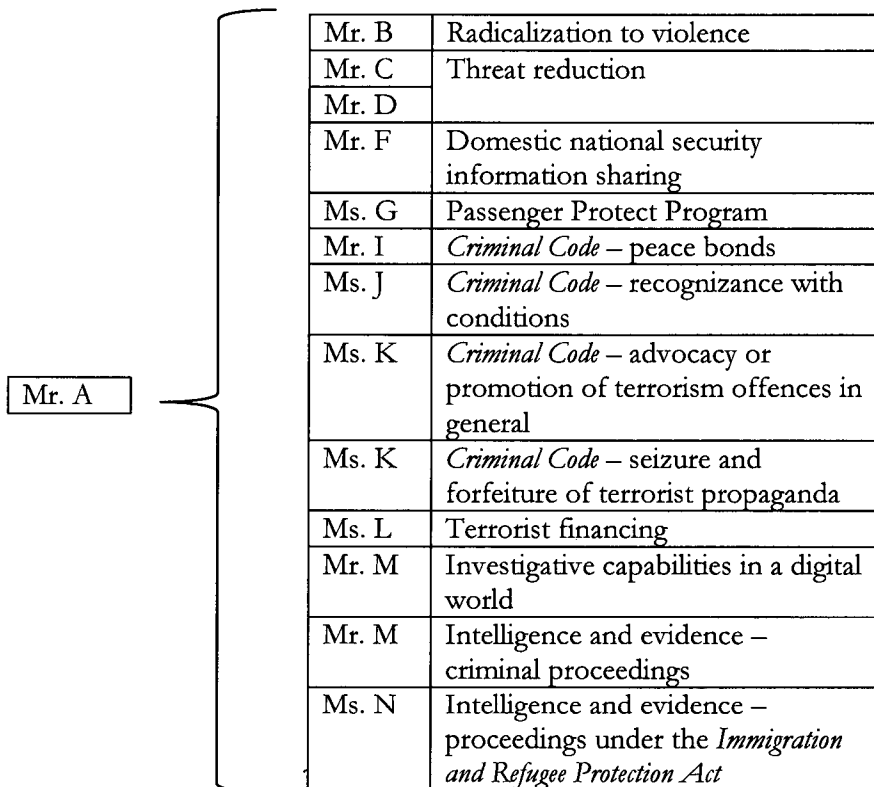
The views of Canadians about these issues – issues affecting us all – will help inform the Government as it designs the most appropriate mechanisms to deal with the evolving terrorism threat facing Canada.

Thank you for taking the time to read through this paper and for providing your thoughts.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

ANNEX – DIAGRAM OF SCENARIO CHARACTERS

The chart below demonstrates Mr. A's links to his followers, and which ones are discussed in various chapters in the document.



There are also two other individuals, who are not associated to Mr. A, but who appear in some chapters.

| | |
|-------|--|
| Ms. E | Domestic national security information sharing |
| Mr. H | Passenger Protect Program |