Analysis of the *Communications Security Establishment Act* and Related Provisions in Bill C-59 (*An Act respecting national security matters*), First Reading (December 18, 2017)

December 2017

Report by Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson, and Ronald Deibert

This page has intentionally been left blank.

The Citizen Lab and CIPPIC are collaborative research partners. Together, the two groups engage in research that investigates the intersection of digital technologies, law, and human rights.

Document Version: 1.0

About the Citizen Lab and Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic

The **Citizen Lab** is an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a "mixed methods" approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

The **Canadian Internet Policy & Public Interest Clinic (CIPPIC)** is a legal clinic based at the Centre for Law, Technology & Society (CLTS) at the University of Ottawa, Faculty of Law. Its core mandate is to ensure that the public interest is accounted for in decision-making on issues that arise at the intersection of law and technology. It has the additional mandate of providing legal assistance to under-represented organizations and individuals on law and technology issues, as well as a teaching mandate focused on providing law students practical training in a law and technology setting.

CIPPIC adopts a multilateral approach to advancing its mandate, which involves placing objective and comprehensive research and argumentation before key political, regulatory and legal decision makers. It seeks to ensure a holistic approach to its analysis, which integrates the socio-political, technical and legal dimensions of a particular policy problem. This regularly includes providing expert testimony before parliamentary committees, participating in quasi-judicial regulatory proceedings, strategic intervention at all levels of court and involvement in domestic and international Internet governance fora.

About This Report

This report is intended to provide timely legal analysis, political context, and historical background on the *Communications Security Establishment Act* and Related Provisions in Bill C-59 (*An Act respecting national security matters*), First Reading (December 18, 2017). We hope that by producing this resource, members of parliament, journalists, researchers, lawyers, and civil society advocates can engage more effectively on the issues at stake. It represents an analysis of the legislation as it enters political debate in Canada, and should be understood in the context of a rapidly evolving legal and political landscape.

The authors are grateful for the in-depth discussions that took place with leading Canadian experts on national security law, policy, and practice at the Citizen Lab's Summer Institute in the summer of 2017. We also appreciate the opportunity to have discussed and received feedback on aspects of our analysis of the legislation at the *Security Intelligence and Surveillance in the Big Data Age* workshop held in Ottawa in the fall of 2017. We also appreciate Public Safety Canada's efforts to engage with us on issues pertaining to Bill C-59. Finally, we appreciate the opportunity to have discussed aspects of this legislation at a briefing on C-59 which was held by members of the Communications Security Establishment, Canadian Security Intelligence Service, Public Safety Canada, and parties external to those agencies in the fall of 2017, as well as discussions with other national security professionals.

The authors would like to graciously thank the John D. and Catherine T. MacArthur Foundation, the Ford Foundation, and Frederick Ghahramani, whose generous funding made this report possible. We would also like to thank Kate Robertson for her legal research and her substantive contributions to this report. Responsibility for any errors or omissions remains with the authors.

Send all questions and feedback to: christopher@christopher-parsons.com; lex@citizenlab.ca; tisrael@cippic.ca.

About the Authors

This analysis was researched and written by Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson, and Ronald Deibert.

Christopher Parsons received his Bachelor's and Master's degrees from the University of Guelph, and his Ph.D from the University of Victoria. He is currently a Research Associate at the Citizen Lab, in the Munk School of Global Affairs with the University of Toronto as well as the Managing Director of the Telecom Transparency Project at the Citizen Lab.

Lex Gill is a Research Fellow at the Citizen Lab, Munk School of Global Affairs. She is also the National Security Program Advocate at the Canadian Civil Liberties Association. Lex is a former Google Policy Fellow for the Canadian Internet Policy & Public Interest Clinic, and a former researcher and affiliate to the Berkman Klein Center for Internet & Society at Harvard University. She holds a B.C.L./LL.B. from McGill University's Faculty of Law.

Tamir Israel is Staff Lawyer at the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) at the University of Ottawa, Faculty of Law. He leads CIPPIC's privacy, net neutrality, electronic surveillance and telecommunications regulation activities and conducts research and advocacy on a range of other digital rights-related topics. He also lectures on Internet regulation at the University of Ottawa, Faculty of Graduate & Post-doctoral Studies.

Bill Robinson is a Research Fellow at the Citizen Lab, Munk School of Global Affairs. He writes the blog *Lux Ex Umbra*, which focuses on Canadian signals intelligence activities past and present.

Ronald Deibert, (OOnt, PhD, University of British Columbia) is Professor of Political Science, and Director of the Citizen Lab at the Munk School of Global Affairs, University of Toronto. The Citizen Lab is an interdisciplinary laboratory focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security. In 2013, he was appointed to the Order of Ontario and awarded the Queen Elizabeth II Diamond Jubilee medal, for being "among the first to recognize and take measures to mitigate growing threats to communications rights, openness and security worldwide."

Acronyms

BCCLA	British Columbia Civil Liberties Association
CERT	Computer Emergency Response Team
CSE	Communications Security Establishment of Canada
CSIS	Canadian Security Intelligence Service
GCHQ	Government Communications Headquarters (United Kingdom)
GDPR	General Data Protection Regulation (European Union)
HUMINT	Human Intelligence
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP Address	Internet Protocol Address
NDA	National Defense Act
NSA	National Security Agency (United States)
NSIRA	National Security and Intelligence Review Agency
NSI-CoP	National Security and Intelligence Committee of Parliamentarians
PIPEDA	Personal Information Protection and Electronic Documents Act
RCMP	Royal Canadian Mounted Police
SECU	Standing Committee on Public Safety and National Security
SIGINT	Signals Intelligence
SIRC	Security Intelligence Review Committee
VEP	Vulnerabilities Equities Process
VPN	Virtual Private Network

Table of Contents

Table of Recommendations

Review, Oversight, Control and Accountability

Scope of Mandate and Powers

Issues with Defined (and Undefined) Terms

Arrangements

Reporting and Transparency Measures

Overview

The Communications Security Establishment ("the CSE" or "the Establishment") is Canada's national signals intelligence and cybersecurity agency. This report contributes to the ongoing national security debate in Canada by providing an analysis of the proposed *Communications Security Establishment Act* (*"CSE Act"*), a major component of the reforms proposed by the Government of Canada in Bill C-59, *An Act respecting national security matters* ("Bill C-59" or "the Bill").[1] In the course of this analysis, we summarize the CSE's mandate, activities, operations, and powers, with an emphasis on their potential implications for human rights and global security. We also offer a series of recommendations which, if adopted, would ensure a more legally sound framework for the CSE, better protect global security interests in a rapidly changing technological environment, and more effectively account for Canada's domestic and international human rights obligations.

In **Section I**, we provide a brief overview of the CSE's current mandate and certain controversial activities undertaken as part of that mandate. We also provide a high-level overview of Bill C-59 and its primary implications for the CSE.

In **Section II**, we undertake a detailed analysis of key issues arising from Bill C-59 related to the CSE, focusing on aspects with the most critical implications for human rights, political transparency, and global security. In particular, some of the issues we highlight in the legislation relate to:

- Longstanding problems with the CSE's foreign intelligence operations, which are predicated on ambiguous and secretive legal interpretations that legitimize bulk collection and mass surveillance activities. These activities both attract *Charter* protections and engage Canada's human rights obligations.
- The complete lack of meaningful oversight and control of the CSE's activities under the proposed active and defensive cyber operations aspects of its mandate.
- The absence of meaningful safeguards or restrictions on the CSE's active and defensive cyber operations activities, which have the potential to seriously threaten secure communications tools, public safety, and global security.
- The absence of meaningful safeguards or restrictions on the CSE's activities more generally. As drafted, the *CSE Act* appears to include a loophole which would allow the Establishment to cause death or bodily harm, and to interfere with the "course of justice or democracy," if acting under its foreign intelligence or cybersecurity powers while prohibiting these outcomes under its new cyber operation powers.
- The risk that the CSE's cybersecurity and assurance operations for the federal government could threaten independence of the courts or the separation of powers.
- Concerns regarding the framework for the CSE's acquisition of malware, spyware and hacking tools, which may legitimize a market predicated on undermining and subverting, rather than strengthening, the security of the

[1] House of Commons of Canada. *An Act respecting national security matters* (Bill C-59), 1st Sess 42nd Parl. First Reading, June 20, 2017.

global information infrastructure.

- Serious issues related to the CSE's provision of technical and operational assistance to other entities—including Canadian law enforcement—which may lead the CSE to proffer capabilities that would otherwise be illegal or unconstitutional for domestic partners to develop, use or possess, or which would be inherently disproportionate if deployed in those contexts (e.g., in policing operations).
- Potential issues with the National Security Intelligence Review Agency's ability to access foreign-provided information, and the risk of regulatory capture through its hiring policies.
- Serious shortcomings—both legal and practical—in the role of the Intelligence Commissioner, which does not resolve the constitutional challenges surrounding the current CSE Commissioner or the constitutionality of the CSE's activities more generally.
- The Intelligence Commissioner's inability to exercise meaningful and comprehensive oversight and control over the CSE's activities (including its most problematic activities) due to an under-inclusive mandate, issues of independence, and insufficient powers of a quasi-judicial nature.
- Weak and vague protections for the privacy of Canadians and persons in Canada, alongside an abject disregard for privacy rights as an international human rights norm.
- Extraordinary exceptions to the CSE's general rule against "directing" activities at Canadians and persons in Canada significantly expand the CSE's ability to use its expansive powers domestically.
- A general failure to recognize that the highly interconnected and interdependent nature of the global information infrastructure means that protections or limits on the CSE's powers that begin and end at national boundaries are insufficient to protect Canada's security interests.
- Deep tensions at the core of the CSE mandate, which requires the Establishment to both protect and defend against security threats while simultaneously exploiting, maintaining, and creating new vulnerabilities in order to further its foreign intelligence agenda. These tensions are exacerbated by the introduction of new offensive powers and the two new aspects of its mandate.
- A lack of legal clarity regarding how, when, and whether vulnerabilities discovered by the CSE are disclosed to vendors or the public, and how the CSE accounts for the public interest in the process.
- The lack of oversight or reporting requirements for "arrangements" with equivalent agencies to the CSE in foreign jurisdictions. There is a risk that these partnerships could involve receipt of information derived from torture or other activities that would be unlawful or unconstitutional if conducted by a Canadian agency.

In **Section III**, we summarize recommendations emerging from our analysis for committee members and other members of Parliament studying the proposed *CSE Act*. In particular, we make recommendations to improve systems of review, oversight, and control of the CSE and to constrain the CSE's ability to engage in activities that are problematic, abusive, unconstitutional, or in violation of international human rights norms.

Section I – Background

About the Communications Security Establishment

The CSE is Canada's national signals intelligence and cybersecurity agency. Originally called the Communications Branch of the National Research Council, the CSE was created by Order-in-Council P.C. 54/3535, dated April 13, 1946, following the merger of two wartime cryptologic offices. The agency remained under the National Research Council until April 1, 1975, when it was transferred to the Department of National Defence and renamed the Communications Security Establishment.

In 2001, Part V.1 was added to the *National Defence Act* (*NDA*), giving the agency its first basis in public statute.[2] This small section of the *National Defence Act* remains the primary legislation governing the CSE's activities, and while the Establishment is no longer part of the Department of National Defence (it became a stand-alone agency in 2011) the Minister of National Defence remains responsible for the agency.

The *National Defence Act* sets out a three-part mandate for the Establishment, commonly referred to as Mandates A, B, and C (*NDA* 1985, s. 273.64(1)).

- **Mandate A:** "acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence."
- **Mandate B:** "provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada."
- **Mandate C:** "provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties."

Activities carried out under the foreign intelligence ("A") and cybersecurity ("B") aspects of the mandate cannot be "directed at" Canadians or persons in Canada. In other words, the CSE is an agency primarily concerned with foreign actors and foreign threats (*NDA* 1985, s. 273.64(2)(a)).

The CSE operates across what it calls the "global information infrastructure" (GII) which is defined in the current law as including "electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those emissions, systems or networks" (*NDA,* s. 273.61). The proposed definition in the new *CSE Act* also adds "any equipment producing such [electromagnetic] emissions, and any data or technical information carried on, contained in or relating to … that equipment" to the definition of the GII (*CSE Act*, s. 2). Practically, this means that the playing field in which the CSE operates includes everything from the Internet, mobile communications, radio, and satellite, to computer systems of every kind imaginable, microwaves, heat signals, and more.

The CSE has traditionally conducted its activities in near-complete secrecy, with almost

[2] *National Defence Act*, RSC 1985, c. N-5.

all aspects of its programs, operations, and activities shielded from meaningful public scrutiny or debate. As a result, information about the agency only began to enter the public consciousness in a widespread sense in late 2013 by way of the Snowden revelations. While as of 2017, only 3% of survey respondents were able to correctly name the CSE as Canada's foreign signals intelligence and cybersecurity agency,[3] many Canadians are undoubtedly familiar with the legal and human rights controversies these documents raised.

Before detailing how the proposed *CSE Act* (and Bill C-59 more generally) may ultimately modify, constrain, or expand the legal framework in which the CSE operates, it is useful to begin by providing a few examples of what is already known about the Establishment's activities. Below, we provide five examples of activities authorized under the CSE's existing three-part mandate, as revealed by the primary source documents disclosed by Edward Snowden. Together, they demonstrate the existing breadth of the CSE's known domestic data collection activities, the extent to which the CSE depends on foreign partners for surveillance operations, the extent to which bulk surveillance data is shared between Canada and its closest intelligence allies, the CSE's targeting of innocent persons' devices, and the ways in which the CSE's programs can leverage multiple aspects of the mandate simultaneously.

- **Collection and Use of Domestic Metadata**: A primary source document revealed that the CSE conducted experiments using Canadian communications metadata—such as Internet Protocol (IP) addresses, cookies, email addresses, or similar routing data—to develop techniques for tracking targeted individuals detected at unidentified IP addresses. Starting with a 'seed' of digital identifiers detected at a major Canadian airport, the Establishment used other airport-linked data, along with data associated with Canadian universities, coffee shops, libraries, and businesses, to track the mobile devices of individuals as they travelled throughout the country. These documents revealed the extent to which the CSE has regular access to domestic Canadian data as well as one of the ways that such information is used by its analysts. Despite the fact that these activities involved deeply revealing information about the private lives and locations of individuals, neither the CSE nor its review body regarded the collection or use of this metadata as an infringement upon Canadians' reasonable expectations of privacy or a violation of the CSE's "directed at" Canadians limitation.[4]

- **Data Collection by Foreign Partners**: While the CSE is ostensibly limited from deliberately targeting Canadians or persons in Canada, reports have shown how its foreign partners (such as the National Security Agency) have deliberately targeted portions of the global information infrastructure located in Canada. When the Agency sought to map the Virtual Private Networks (VPNs)

[3] Canadian Press. (2017). "Just 3% Of Canadians Can Name The Communciations Security Establishment: Survey," *Huffpost*,, http://www.huffingtonpost.ca/2017/11/08/just-3-of-canadians-can-name-the-communications-security-establishment-survey_a_23270492/.

[4] See: Communications Security Establishment. (2012). "IP Profiling Analytics & Mission Impacts," Government of Canada, https://christopher-parsons.com/writings/cse-summaries/#ip-profiling.

of companies around the world, including Canadian banks, the documents and research were released to the CSE. Even when the CSE may not be authorized to collect intelligence information about domestic organizations, Canadians, or persons in Canada, its partner agencies may collect this information and subsequently make it available to the CSE to use, analyze, or share.[5]

- **Data Sharing with Foreign Entities**: Primary source documents revealed the degree to which Canadian intelligence operations relied on data collected and, potentially, access provided by allies to conduct a bulk surveillance operation. After working with a 'special source' to comprehensively monitor the uploading and downloading of documents from free file upload websites, the CSE developed comprehensive pattern-of-life analyses of persons who used these kinds of services. These analyses included linking digital identifiers associated with the file activity to other online actions of individuals—such as browsing the web or visiting Facebook. On its own, the CSE could not have engaged in this type of surveillance operation or pattern-of-life analysis: the Establishment could only do so by querying foreign databases of bulk surveillance data collected by Canada's closest foreign intelligence allies, including the National Security Agency (NSA) and the Government Communications Headquarters (GCHQ).[6]

- **Exploiting Non-Targeted Persons' Devices**: The CSE uses an automated system to identify devices which can subsequently be exploited. These devices are not necessarily operated by parties who represent a threat to Canada. Instead, the devices can be used to simply mask operations which are undertaken by the CSE, helping the Establishment avoid having activities traced back to CSE-hosted systems (instead, activities appear to take place from the unrelated devices identified and exploited by the Establishment). This subterfuge has the effect of transforming the uninvolved owners of exploited devices into unknowing and unwilling 'participants' in the Establishment's activities. This type of activity can have detrimental impacts on the rights and interests of unsuspecting individuals if the CSE's adversaries attempt to compromise or otherwise interfere with those who own or control the exploited devices—either treating them as collateral damage or holding them somehow responsible for the CSE's activities.[7]

- **Leveraging Multiple Mandates for Operations**: The CSE's foreign intelligence and cyber defence operations have involved the deployment at least 200 sensors around the world. Sensors which operate exclusively on Government of Canada networks are authorized under the cybersecurity (B)

---

[5] See: Colin Freeze and Christine Dobby. (2015). "NSA trying to map Rogers, RBC communications traffic, leak shows," *Globe and Mail*, https://www.theglobeandmail.com/news/national/nsa-trying-to-map-rogers-rbc-communications-traffic-leak-shows/article23491118/.

[6] See: Communications Security Establishment. (Post 2012). "LEVITATION and the FFU Hypothesis," Government of Canada, https://christopher-parsons.com/writings/cse-summaries/#levitation-and.

[7] See: Communications Security Establishment. (Unknown). "LANDMARK," Government of Canada, https://christopher-parsons.com/writings/cse-summaries/#landmark-associated.

> aspect of the mandate. However, many of these systems are also authorized under the foreign intelligence (A) or the assistance (C) aspect of the mandate. This framework means that the network is capable of actively impeding, modifying, or comprehensively monitoring and tracking data traffic. That no single mandate contains this operation is an indication that the CSE's mandates and associated actions should not necessarily be read in isolation. Instead, it is more accurate to see these efforts as interlinked and mutually enabling.[8]

The information revealed about the CSE in the Snowden documents came as a surprise to both the public and experts alike, who did not realize the degree to which such intrusive conduct was possible under the CSE's current legal framework. However, it is essential to understand that not all of the activities described above—nor all of the activities undertaken by the CSE more generally—are necessarily lawful or constitutional. In particular, the British Columbia Civil Liberties Association (BCCLA) is currently engaged in a major constitutional challenge with regard to the CSE's mass surveillance activities, arguing that the agency's purported ability to engage in warrantless interception of Canadians' private communications and to engage in the mass collection of Canadian metadata violate the protection against unreasonable search and seizure under sections 8 of the *Charter of Rights and Freedoms*.[9]

Moreover, and in contrast to some of Canada's closest allies, public glimpses into the CSE's activities have been comparatively limited. This has meant that it is impossible for the public to fully understand the ways in which the proposed *CSE Act* would modify, limit, or expand the activities currently undertaken by the Establishment. It is also impossible to understand the extent to which the proposed *CSE Act* might serve to anchor constitutionally problematic aspects of the CSE's pre-existing activities in public law. In the absence of meaningfully detailed information about the scope and nature of the CSE's current activities, it is extremely difficult to evaluate their current or future lawfulness, their impact on *Charter*-protected and international human rights, and their relationship to Canada's national interests.

However, in the absence of greater transparency from the Establishment—and accounting for certain differences in mandate, legal context, and scale—it is reasonable for onlookers to infer that the CSE is generally engaged in similar types of activities as its closest intelligence allies, including the NSA and the GCHQ. Many of those other agencies' activities have been considered extremely controversial, and would potentially be unconstitutional if carried out by the Canadian government. Parliamentarians must better understand the kinds of activities currently undertaken by the Establishment, as

---

[8] See: Communications Security Establishment. (2012). "IP Profiling Analytics & Mission Impacts," Government of Canada, https://christopher-parsons.com/writings/cse-summaries/#ip-profiling; Communications Security Establishment. (2009 or 2010). "CSEC Cyber Threat Capabilities: SIGINT and ITS: an end-to-end approach," Government of Canada, https://christopher-parsons.com/writings/cse-summaries/#cse-cyber-threat-capabilities.

[9] British Columbia Civil Liberties Association v. Canada (Attorney General), Statement of Claim T-2210-14, Federal Court of Canada at para32, https://bccla.org/wp-content/uploads/2014/12/20141027-CSEC-Statement-of-Claim.pdf.

well as its plans for the future to fully appreciate the implications of the currently proposed legislation: though the Minister may be unwilling to provide specific answers to questions about the CSE's activities, it is nevertheless imperative that the public and parliamentarians better understand the specific types of activities that are currently authorized and which could or would be authorizable under the proposed *CSE Act*.

About Bill C-59 (*An Act respecting national security matters*)

The federal government proposed Bill C-59 in June 2017, framing the reforms as a response to the previous government's controversial *Anti-Terrorism Act 2015* (formerly Bill C-51). Bill C-59 offers a partial response to some of the constitutional issues with Bill C-51 and responds to some of the public concerns raised in the course of the National Security Consultation that took place in late 2016.[10] C-59 covers a vast range of issues in the area of national security law—from information-sharing and the no-fly list to criminal law terrorism provisions. Some of these reforms were clearly foreshadowed by the 2016 consultation, others offer a partial response to decades of government inquiries and commissions on national security,[11] and still others seek to legitimize government conduct in light of recent Federal Court rulings.[12]

Yet many of the proposed changes in Bill C-59—including dramatic reforms to the mandate and authorization frameworks of the CSE—have received little public consultation or debate. While much of Bill C-59 was widely foreshadowed—either in court decisions, past legislation, Commissions of Inquiry, or through public consultation—the legal reforms to the CSE were largely unexpected. Save for two recommendations at the end of the May 2017 Roadmap for National Security prepared by the Standing Committee on Public Safety and National Security, there was little hint that the CSE would be undergoing major reform.

> Recommendation 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.
>
> Recommendation 41

[10] Public Safety Canada. (2016). "Consultation on National Security," Government of Canada, https://www.canada.ca/en/services/defence/nationalsecurity/consultation-national-security.html?wbdisable=true.

[11] See: The Honourable Dennis R. O'Connor. (2006). Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/index.htm; The Honourable Frank Iacobucci, Q.C. (2008). Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmed Abou-Elmaati and Muayyed Nureddin, http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/internal_inquiry/2010-03-09/www.iacobucciinquiry.ca/pdfs/documents/final-report-copy-en.pdf; The Honourable John C Major. (2010), Air India Flight 182: A Canadian Tragedy, http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/air_india/2010-07-23/www.majorcomm.ca/en/reports/finalreport/default.htm.

[12] See X (Re), 2013 FC 1275, X (Re), [2017] 2 FCR 396, 2016 FC 1105.

> That cyber security strategies need to adopt a whole of government approach, such as the GCHQ (UK Government Communications Headquarters) approach.
>
> SECU Roadmap (2017) at 43[13]

Part 3 of the bill enacts a new statute for the CSE (the *CSE Act*), amends the *National Defence Act* (the CSE's current enabling legislation), and makes consequential amendments to other Acts. Notably, the *CSE Act* would:

- Make substantial changes to the mandate of the Communications Security Establishment and potentially significantly expand its powers;
- Set out a longer and more explicitly permissive list of exceptions to the general rule barring the Establishment from 'directing' its activities at Canadians, persons in Canada, and in some cases infrastructure in Canada, in the pursuit of certain mandates;
- Create a new framework for the authorization of the CSE's activities under the authority of the designated Minister and the newly-created Intelligence Commissioner;
- Create an enabling framework for the disclosure of information by the CSE to designated persons and classes; and
- Set out the authority of the Establishment to enter into "arrangements" with foreign and international bodies for the purpose of information sharing and cooperation.

Bill C-59 also enacts and amends other legislation with implications for the CSE, including the *National Security and Intelligence Review Agency Act* ("*NSIRA Act*") and the *Intelligence Commissioner Act*.

The proposed National Security and Intelligence Review Agency (NSIRA) would have a mandate to review activities carried out by the CSE and the Canadian Security Intelligence Service (CSIS); activities carried out by other government departments related to national security or intelligence; and other related matters referred to NSIRA by a Minister. It would also have the ability to investigate complaints, issue findings and recommendations (*NSIRA Act*, s. 8).

The *Intelligence Commissioner Act* would abolish the position of the Commissioner of the Communications Security Establishment and create the office of the Intelligence Commissioner. The proposed Intelligence Commissioner would have an independent, quasi-judicial oversight role over both the CSE and CSIS, with the power to review and approve certain authorizations, amendments to authorizations, and determinations sought under those agencies' respective Acts.

---

[13] Standing Committee On Public Safety and National Security. (2017). "Protecting Canadians And Their Rights: A New Road Map For Canada's National Security," 42nd Parliament of Canada, 1st Session, https://www.ourcommons.ca/Content/Committee/421/SECU/Reports/RP8874869/securp09/securp09-e.pdf, p 43.

Section II – Analysis of the CSE Act

i. Mandate

The proposed *CSE Act* would expand the Establishment's current three-part mandate to a five-part mandate (*CSE Act*, s. 16(1)). In addition to the current categories of foreign intelligence, cybersecurity, and assistance, this change would establish two "new" aspects of the Establishment's mandate:

- Defensive cyber operations (*CSE Act*, s. 19)
- Active cyber operations (*CSE Act*, s. 20)

However, the *CSE Act* modifies the framing and scope of all aspects of the Establishment's mandate, even beyond these two "new" categories. Similarly, rather than conceiving of the "defensive cyber operations" (s. 18) aspect of the mandate as entirely novel, it may be more accurate to see it as both a split and extension of the *National Defense Act*'s current Mandate B (cybersecurity) into two distinct categories in the new *CSE Act*: cybersecurity and information assurance (s. 18) and defensive cyber operations (s. 19), respectively.

In general, and with regard to the "active cyber operations mandate" in particular, the extent to which the five-part *CSE Act* mandate would facilitate activities of a nature and type not already undertaken by the Establishment remains unclear. The secrecy of the CSE's activities means that it is difficult to distinguish whether the legislative intent of these changes is to grant the Establishment new powers, or to provide legal clarity and an explicit authorization framework in public law for activities which the Establishment already conducts, or which it has conducted in the past.

Table 1 indicates how Bill C-59 would modify the CSE's current mandate and offers a touchstone for understanding the five aspects of the mandate proposed in the *CSE Act*.

National Defence Act	***CSE Act***
Mandate A (s. 273.64 (1)(a)) The mandate of the Communications Security Establishment is (a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;	**Foreign intelligence (s. 17)** The foreign intelligence aspect of the Establishment's mandate is to acquire, covertly or otherwise, information from or through the global information infrastructure, including by engaging or interacting with foreign entities located outside Canada or by using any other method of acquiring information, and to use, analyse and disseminate the information for the purpose of providing foreign intelligence, in accordance with the Government of Canada's intelligence priorities.

Mandate B (s. 273.64 (1)(b)) The mandate of the Communications Security Establishment is ... (b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada;	**Cybersecurity and information assurance (s. 18)** The cybersecurity and information assurance aspect of the Establishment's mandate is to (a) provide advice, guidance and services to help protect (i) federal institutions' electronic information and information infrastructures, and (ii) electronic information and information infrastructures designated under subsection 22(1) as being of importance to the Government of Canada; and (b) acquire, use and analyse information from the global information infrastructure or from other sources in order to provide such advice, guidance and services.
	Defensive cyber operations (s. 19) The defensive cyber operations aspect of the Establishment's mandate is to carry out activities on or through the global information infrastructure to help protect (a) federal institutions' electronic information and information infrastructures; and (b) electronic information and information infrastructures designated under subsection 22(1) as being of importance to the Government of Canada.
N/A	**Active cyber operations (s. 20)** The active cyber operations aspect of the Establishment's mandate is to carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security.
Mandate C (s. 273.64 (1)(c)) The mandate of the Communications Security Establishment is ... (c) to provide technical and operational assistance	**Technical and operational assistance (s. 21)** The technical and operational assistance aspect of the Establishment's mandate is to provide technical and operational assistance to federal law enforcement and security agencies, the Canadian Forces and the Department of National Defence.

to federal law enforcement and security agencies in the performance of their lawful duties.	

In the remainder of this section, we outline the types of activities associated with each aspect of the mandate, how such activities would be authorized under the proposed *CSE Act,* the potential for interference with *Charter*-protected rights and human rights more generally, and implications for global security.

Foreign Intelligence

National Defence Act	***CSE Act***
Mandate A (s. 273.64 (1)(a)) The mandate of the Communications Security Establishment is (a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;	**Foreign intelligence (s. 17)** The foreign intelligence aspect of the Establishment's mandate is to acquire, covertly or otherwise, information from or through the global information infrastructure, including by engaging or interacting with foreign entities located outside Canada or by using any other method of acquiring information, and to use, analyse and disseminate the information for the purpose of providing foreign intelligence, in accordance with the Government of Canada's intelligence priorities.

The CSE has a mandate to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence (*NDA,* s. 273.64 (1)(a), *CSE Act,* s. 17). These operations include targeted as well as mass surveillance activities with the purpose of acquiring intelligence about foreign individuals, states, organizations or terrorist groups as they relate to international affairs, defence, or security (*NDA,* 273.61, *CSE Act*, s. 2). The proposed revisions to the foreign intelligence aspect of the mandate in the *CSE Act* are more explicit than the *National Defence Act* with regard to the fact that the CSE may acquire this information covertly, that the information may be acquired with the assistance of foreign entities, and that such information can be not only acquired and used, but also analyzed and disseminated (*CSE Act*, s. 17).

The breadth of the proposed new version of the CSE's foreign intelligence mandate is such that it might enable the Establishment to employ human agents to implant tapping devices or undertake other activities in support of SIGINT operations outside Canada.[14] The Canadian Security Intelligence Service (CSIS) is able to undertake these types of activities

[14] Bill Robinson. (2017). "CSE and Bill C-59 overview," *Lux Ex Umbra*, https://luxexumbra.blogspot.ca/2017/08/cse-and-bill-c-59-overview.html.

for CSE inside Canada, but the scope of CSIS' mandate to conduct foreign intelligence remains unclear, and it has been suggested that the CSE would benefit from human intelligence (HUMINT) support abroad.[15] While in certain cases, this could potentially allow the Establishment to operate in a more targeted and proportionate manner (e.g. by creating the means to access a specific computer rather than a whole network), it could also creates a range of new avenues for disproportionate and problematic conduct (e.g., by targeting an otherwise inaccessible node on the global information infrastructure in order to create generalized access). The government should make its intentions clear on this question: if it is contemplating the addition of a HUMINT component to the CSE's operations, it should inform Parliament and Canadians of this significant change to the Establishment's nature; if not, it should make that position explicit.

The current *National Defence Act* permits the CSE to incidentally intercept private communications when carrying out activities under a foreign intelligence Ministerial authorization, allowing the Establishment to contravene Part VI of the *Criminal Code* (*NDA,* ss. 273.65, 273.61; a private communication is defined in section 183 of the *Criminal Code*). By contrast, in the proposed *CSE Act*, a foreign intelligence authorization can be sought by the CSE for foreign intelligence related activities that would contravene any Canadian law, including the *Charter* (*CSE Act* s. 23(1)). Under this regime, the Minister can authorize the CSE to commit a much broader range of otherwise unlawful activities than currently allowed under the *National Defence Act*. At the same time, the CSE is not required to operate under a Ministerial authorization (and its included protections) where it is of the view that its activities will not violate a law of Canada.

Under the *CSE Act*, foreign intelligence authorizations are issued on the basis of a written application by the Chief of the CSE that sets out the facts which allow the Minister to conclude there are reasonable grounds to believe the authorization is necessary and that the criteria in subsection 35(2) of the Act are met (s. 34). Specifically, an authorization may be issued only if the Minister has reasonable grounds to believe that:

- Any activity that would be authorized by it is contextually "reasonable and proportionate" (*CSE Act* s. 35(1));
- Any information acquired under the authorization could not reasonably be acquired by other means s. 35(2)(a) and if information is to be acquired on an unselected basis, that it could not reasonably be acquired without resort to unselected acquisition means (35(2)(b);
- Any information acquired under the authorization will not will be retained for

[15] In 2007, Bob Brûlé, the CSE's former Deputy Chief, SIGINT Operations told the Standing Senate Committee on National Security and Defence that "organizations such as the CSE desperately require a foreign intelligence service for them to continue to be successful in the future. From a purely selfish point of view, some decision that the government could make to move forward would be of benefit to technical organizations such as the CSE." See: Standing Committee on National Security and Defence. (2007). "Proceedings of the Standing Senate Committee on National Security and Defence," Senate of Canada, Issue 17 - June 11, 2007, https://sencanada.ca/en/Content/Sen/committee/391/defe/17eva-e.

longer than is reasonably necessary 35(2)(a); and
- The measures referred to in section 25 will ensure that information acquired under the authorization that is identified as relating to a Canadian or a person in Canada will be used, analysed or retained only if the information is essential to international affairs, defence or security (35(2)(c).

In addition, the *CSE Act* also permits the CSE to disclose information capable of identifying Canadians to persons designated as appropriate recipients if the information is deemed essential to international affairs, defence, security or cybersecurity (ss. 44 and 46). Only information that has been "used, analysed or retained" under a foreign intelligence authorization can be disclosed through this section, providing some measure of insulation against cross-mandate data creep. However, section 44 is problematic to the extent that it expands the already broad and imprecise objectives of "foreign intelligence" to include "cybersecurity," a term left undefined in the *CSE Act* in general and specifically in relation to the CSE's foreign intelligence mandate. It is unclear why the addition of this ambiguous term is required here. To the extent that the CSE can carry out cybersecurity activities under its foreign intelligence mandate, these concerns will already be captured by the foreign intelligence objectives "international affairs, defence and security."

Recommendation 41.
Amend section 44 to exclude the term "cybersecurity," which is not defined in the *CSE Act* and is not otherwise mentioned in relation to the CSE's foreign intelligence activities.

Section 44 operates as an exception to the limitation imposed by section 23 (which prohibits the Establishment from directing its foreign intelligence activities at Canadians) and to section 25 (which requires measures to protect the privacy of Canadians in disclosures made by the CSE under its foreign intelligence mandate). In practice, it appears the CSE will be able to incidentally disclose de-identified Canadian data in bulk with minimal restriction under its foreign intelligence mandate, but will only be able to link such de-identified data to Canadian persons under the auspices of section 44. This is particularly concerning given the broad scope of entities that can be authorized as legitimate recipients of section 44 disclosures by the Minister (*CSE Act*, s. 47). Indeed, section 47 appears to place no limitations at all on the persons or classes of persons that might be designated as recipients of section 44 disclosures, including foreign agencies and private sector organizations. While section 55 of the *CSE Act* provides an additional framework by which information sharing with foreign entities can occur (subject to approval by the Minister of Foreign Affairs), section 55 is optional, meaning that it is not a prerequisite for information sharing with designated foreign bodies to occur under section 44.

The *CSE Act* also sets out an explicit framework for the acquisition of "unselected" information, which is defined in the proposed Act as meaning "that the information is acquired, for technical or operational reasons, without the use of terms or criteria to identify information of foreign intelligence interest" (*CSE Act*, s. 2). In other words, where "unselected" information is concerned, we are discussing activities that are explicitly forms of non-targeted mass surveillance, which many have argued constitutes

a violation of internationally protected human rights obligations as well as of the privacy rights of incidentally affected Canadians under the *Charter*.[16]

A foreign intelligence authorization allows the CSE to engage in any otherwise unlawful activity, "despite any other Act of Parliament or of any foreign state," in furtherance of the mandate, subject to the conditions for authorization set out in subsection 35(2) of the *CSE Act* and the terms of the Authorization. The broad range of activities that can be authorized under this aspect of the new mandate is described at section 27 of the new Act. Paragraph 27(2)(e) also creates a residual category, which allows the CSE to carry out "any other activity that is reasonable in the circumstances and reasonably necessary in aid of any other activity, or class of activity, authorized by the authorization."

Foreign intelligence authorizations are valid only if the Intelligence Commissioner has approved the authorization in writing (*CSE Act,* s. 29). The authorization remains valid for up to one year following Commissioner approval and can be extended by the Minister for up to one additional year. While the decision to extend an authorization is not subject to review by the Intelligence Commissioner, a new authorization must be issued after that year (*CSE Act*, s. 37). This is an improvement on the *National Defence Act*'s current system, which allows the Chief of the CSE to seek annual renewal of authorizations from the Minister on an indefinite basis, so long as each renewal period does not exceed one year (*NDA*, s. 273.68(1)). The *CSE Act* also introduces an additional safeguard, requiring the Chief of the CSE to provide notice to the Minister if there has been a significant change in the facts set out in the original application for authorization, and for the Minister to bring this change to the attention of the Intelligence Commissioner and the NSIRA (*CSE Act*, s. 38). The Intelligence Commissioner may then re-review the authorization and potentially either repeal it or require amendments. These are important additions, as the factual, technical and operational parameters under which the CSE operates evolve rapidly, as do the Establishment's technical capabilities.

Ambiguous Legal Interpretations and Low Thresholds

Much of the CSE's foreign intelligence activity operates under highly ambiguous legal footing, and judicial interpretations of this legal footing are exceedingly rare because of the inherent secrecy of the CSE's operations. Protections offered by the *Charter* in this context are equally ambiguous, if only because they have not been rigorously tested in court. For example, does gaining access to a portion of the global information infrastructure implicate Canadian law even if such access is gained through an entry point located abroad? The underlying activities might be intrusive, but the manner in which Canadian law is engaged remains ambiguous. Similarly, ss. 342.1 and 430(1.1) of the Criminal Code provide the primary legal prohibitions that limit intrusion into computing devices or networks.

---

[16] Report of the Office of the United Nations High Commissioner for Human Rights, "The Right to Privacy in the Digital Age", *Advanced Edited Version*, June 30, 2014, A/HRC/27/37, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf; Tamir Israel. (2015). "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation." in Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283.

However, neither prohibitions apply if the activities in question are undertaken with 'colour of right'.[17] 'Colour of right' is a legal concept that refers to situations where an individual carries out an action with the honest belief that she is legally entitled to carry it out.[18] The CSE might honestly believe that its mandate to, for example, "acquire, covertly or otherwise, information from or through the global information infrastructure … for the purposes of providing foreign intelligence" provides it with the 'colour of right' to carry out activities otherwise prohibited to individuals by ss 342.1 and 430 of the *Criminal Code*. The federal court recently reached a similar conclusion with respect to CSIS, holding that s 12 of the *CSIS Act* provides the service with 'colour of right' to interfere with cell phone transmissions in ways that might otherwise be prohibited by s 430 of the *Criminal Code*, even in the absence of any other legal authorization such as a warrant.[19] The CSE may similarly argue its mandate furnishes it with sufficient 'colour of right' to carry out such activities even in the absence of an authorization. It is, then, not clear in what contexts the CSE's network intrusion activities would trigger the need for an authorization. In short, requiring a violation of Canadian laws as a 'trigger' for Ministerial Authorization means that some of the CSE's problematic activities could potentially bypass the authorization process entirely, as well as the proportionality and necessity obligations that accompany it.

Recommendation 16.

Amend sub-sections 23(3) and (4) so that activities carried out in furtherance of the foreign intelligence and cybersecurity and information assurance aspects of the CSE's mandate may only incidentally affect or relate to a Canadian or a person in Canada if carried out further to an authorization under subsections 27(1), 28(1) or (2) and 41(1).

Recommendation 17.

Amend the triggering threshold for the CSE to seek an authorization from "must not contravene any other Act of Parliament unless…" (*CSE Act*, at ss. 23(3), 23(4)) to also include breaches of provincial law and common law.

Ambiguous legal interpretations can also affect the proportionality assessment that Bill C-59 includes as part of the authorization process. In particular, there has been a long-standing disagreement between the CSE and many CSE Commissioners over legal terms such as 'interception', 'acquisition' and 'collection', which are central to the CSE's

[17] See sub-section 429(2) "No person shall be convicted of an offence under sections 430 to 446 where he proves that he acted with legal justification or excuse and with colour of right"; and section 342.1(1) "Everyone is guilty of an … offence … who, fraudulently and without colour of right."

[18] *R v Bahr*, 2006 ABPC 360, paras 24-26.

[19] *Re X*, 2017 FC 1047, paras 101-106 and, specifically, paras 103, 105 and 106 ("I will simply add in passing that, in their oral submissions, the *Amici* conceded that if I find that section 12 provides sufficient authorization for the capture of IMSI and IMEI identifiers through the use of CSS technology, that would be sufficient to bring that activity within the scope of the defence afforded by section 429 of the *Criminal Code*."). Section 12 of the *CSIS Act*, RSC 1985, c C-23, defines the duties and functions of the Service: "The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada."

monitoring of the global information infrastructure.[20] In particular, many foreign intelligence agencies will argue that information is only 'acquired', 'intercepted' or 'analyzed' once it is persistently collected by the agency in question. This permits such agencies to discount the privacy impact of network traffic and other data that is analyzed and searched remotely.[21] For example, the CSE Commissioner, who must assess CSE activities based on the CSE's own legal interpretations, assess the scope of the CSE's interception activities in terms of private communications 'intercepted and retained' while ignoring all the private communications that were searched in real time to produce the 'retained' communications.[22] This approach can discount significant volumes of searched traffic, even while such searching can have serious chilling effects.[23] The end result is a substantially skewed proportionality analysis that undermines the true impact of the CSE's network filtering activities.

---

[20] Communications Security Establishment Commissioner, "Annual Report: 2007-2008", May 2008, https://www.ocsec-bccst.gc.ca/a76/ann-rpt-2007-2008_e.pdf, p 4: "My second principal recommendation is to define the terms intercept and interception, or to provide a reference to the existing definition of intercept in the Criminal Code. At present, these terms are not defined in the National Defence Act. However, they have both legal and operational significance for CSEC. In the absence of definitions that are universally understood and consistently applied, it is difficult for me to interpret CSEC's legislated authority and to review how it is applied."

[21] Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", July 2, 2014, p 7; Open Rights Group, "GCHQ and Mass Surveillance," *OpenRightsGroup.org*, 11 March 2015, <https://www.openrightsgroup.org/ourwork/reports/gchq-andmass-surveillance>, p 6–8

[22] Tamir Israel. (2015). "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation." In Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283, p 79.

[23] *R v Taylor*, [1990] 3 SCR 892, paras 76-77: "... s. 13(1) works to suppress private communications, demons trating an extensive and serious intrusion upon the privacy of the individual. ... I do not disagree with the view that telephone conversations are usually intended to be private; it is surely reasonable for people to expect that these communications will not be intercepted by third persons. ... The connection between s. 2(b) and privacy is thus not to be rashly dismissed, and I am open to the view that justifications for abrogating the freedom of expression are less easily envisioned where expressive activity is not intended to be public, in large part because the harms which might arise from the dissemination of meaning are usually minimized when communication takes place in private, but perhaps also because the freedoms of conscience, thought and belief are particularly engaged in a private setting." *Bennett v Lenovo*, 2017 ONSC 1082, para 27 ("The risk of unauthorized access to private information is itself a concern even without any actual removal or actual theft. For example, if a landlord installs a peephole allowing him to look into a tenant's bathroom, the tenant would undoubtedly feel that her privacy had been invaded even if the peephole was not being used at any particular time.") UNGA, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", A/HRC/29/32, May 22, 2015 ("Surveillance systems ... may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information."; Jon Penney, "Chilling Effects: Online Surveillance and Wikipedia Use", (2016) 31(1) Berkeley T L J 117; Human Rights Watch & American Civil Liberties Union, "With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law & American Democracy", July 2014, Human Rights Watch; Cindy Cohn, "Protecting the Fourth Amendment in the Information Age: A Response to Robert Litt", (2016) 126 Yale LJ 107; Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring", (2016) 93(2) Journalism & Mass Communication Q 296; PEN America, "Global Chilling: The Impact of Mass Surveillance on International Writers", Pen.org, January 5, 2015.

Recommendation 37.

Amend the *CSE Act* to clarify that the words "intercept", "analysis", "interception" and "acquisition" have the same meaning in the *CSE Act* as in Part VI of the *Criminal Code*.

Recommendation 38.

Define the words "acquire," "use", "analyze" and "collect" in the *CSE Act* so that what constitutes an incidence of "acquisition" and an incidence of "collection" is explicit, and so that there is a clear distinction between the analysis and use of information already acquired, and the analysis and use of information that the CSE has not already acquired.

Bulk Collection and Mass Surveillance

The CSE currently engages in what is often referred to as "bulk collection" (or mass surveillance) using a number of different techniques. Some types of mass surveillance include the use of keywords, terms or other types of "selectors" that are used to filter vast amounts of network traffic and intercept any traffic streams that register a "hit" on a given selector. Selectors can be email or IP addresses, keywords like "bomb," or more sophisticated criteria such as "originating from the country of Brazil and written in simplified Chinese characters." Perhaps the most expansive form of mass surveillance mechanism occurs when agencies such as the CSE collect *all* network traffic without relying on any selectors or targeting criteria at all. While the CSE has always been able to carry out such activities, the proposed *CSE Act*—unlike the *National Defence Act*—is explicit that the CSE can engage in such activities and clarifies that an authorization can be granted to collect unselected information in the course of the foreign intelligence aspect of the Establishment's mandate (27(2)(b)).

The *CSE Act* requires the CSE to independently demonstrate conditions under which unselected collection would be necessary—that is, to demonstrate why normal collection methods are insufficient—in Ministerial authorizations prior to engaging in such acquisition methods (35(2)(b)). However, the fact that the CSE would remain capable of "unselected" collection in the proposed Act raises important questions about the authorization framework as a whole, and casts serious doubt on whether any of the language which appears to potentially constrain the Establishment's foreign intelligence activities (see ss. 27 and 35) will have any meaningful impact. In effect, the *CSE Act* statutorily defines "reasonable and proportionate" to include not only "selector" based bulk collection, but even the most egregious and unmitigated forms of unselected mass surveillance. By contrast, many have argued that mass surveillance is inherently disproportionate given the significant privacy interests engaged.[24] In the proposed *CSE Act*, the purported "proportionality" of the CSE's mass surveillance of unselected

[24] Report of the Office of the United Nations High Commissioner for Human Rights, "The Right to Privacy in the Digital Age", Advanced Edited Version, June 30, 2014, A/HRC/27/37, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf; Article 19 & Electronic Frontiers Foundation, "Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance: Background and Supporting International Legal Analysis", May 2014, https://cippic.ca/uploads/IPAHRCS-legal_analysis.pdf.

information has been statutorily predetermined at the outset. If such activities are to be expressly listed in the *CSE Act*, the Intelligence Commissioner and the courts must have latitude to statutorily determine they are *inherently* disproportionate.

Recommendation 5.

Amend the *Intelligence Commissioner Act* and the *CSE Act* so that the Intelligence Commissioner has the ability to impose conditions on approved authorizations; the obligation to rule on the legality, constitutionality, reasonable necessity, and proportionality of any activity undertaken by the CSE; and order-making powers to prevent the CSE from carrying out any activities that are either illegal, unconstitutional, disproportionate or not reasonably necessary.

An Ongoing Constitutional Challenge

The British Columbia Civil Liberties Association has an ongoing constitutional challenge regarding the CSE's surveillance activities. The challenge calls into question the current Ministerial Authorization framework (*NDA* 1985, ss. 273.65 and 273.68), which purports to allow the CSE to engage in the interception and collection of private communications and metadata in the absence of prior judicial authorization, without an application of the 'reasonable and probable grounds' standard (or any identifiable standard), or other basic safeguards such as limits on retention or a prohibition on disclosure to foreign entities. The Association's challenge also argues that these activities infringe the right to freedom of thought, belief, opinion and expression protected under section 2(b) of the *Charter*.[25] Bill C-59's proposed inclusion of an Intelligence Commissioner tasked with approving and reviewing the Minister's authorizations—while a marginal improvement—is unlikely to provide the independent control demanded by section 8 of the *Charter,* and does not respond to the full range of constitutional concerns raised by the BCCLA.

Entrenching Problematic Foreign Intelligence Activities

As noted above, proposed subsection 27(2) of the *CSE Act* encodes a range of activities that the CSE can undertake further to its foreign intelligence mandate. While none of the activities in question will constitute new additions to the CSE's toolset, their explicit encoding has at least two implications. First, it enhances transparency by providing a specifically itemized indicative list of what the CSE might undertake in furtherance of its foreign intelligence mandate. Second, explicitly encoding certain activities in subsection 27(2) undermines the statutory scope of critical normative restrictions placed on the CSE, such as the need for the Minister to authorize only what is "reasonable and proportionate" and what is "reasonably necessary." However, this is somewhat undercut by proposed subsection 27(2)(e), a catchall provision that allows the CSE to undertake "any other activity that is reasonable in the circumstances."

---

[25] *British Columbia Civil Liberties Association v. Canada (Attorney General)*, Statement of Claim T-2210-14, Federal Court of Canada at para32, at: https://bccla.org/wp-content/uploads/2014/12/20141027-CSEC-Statement-of-Claim.pdf.

Potentially problematic activities that might be more readily viewed as "proportionate" due to the inclusion of an enumerated list in 27(2) include:

- Using malware to target specific routers on the Internet or specific persons' electronic devices in order to gain access to a portion of the global information infrastructure;
- The indiscriminate and non-targeted collection of extremely large volumes of Canadian and non-Canadian data from digital devices and networks;
- Degrading the effectiveness or co-opting the utility of anti-virus software in order to maintain the covert nature of a CSE activity;
- Compromising system update servers that provide security patches in order to either deliver malware to targeted systems or prevent systems from remedying vulnerabilities being exploited by the CSE; or
- Weakening globally approved cryptographic protocols to enable access to information meant to be secured using those protocols.[26]

Overbroad Scope of "Foreign Intelligence"

In both the *NDA* and the proposed *CSE Act*, "foreign intelligence" is defined as any "information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security." At the outset, the scope of this definition is overly broad, particularly in its inclusion of the intentions of any foreign individual as these relate to international affairs. Historically, foreign intelligence agencies were given broad powers but these were focused on foreign states and their agents. In the late 1990s and early 2000's, the National Security Agency and its intelligence partners reoriented their surveillance programs to encompass the intentions of *any* foreign individual, not merely those associated with state agents.[27] Globalization and the ascendancy of the Internet has internationalized many political issues that were once determined primarily on a domestic basis.[28] Political debates increasingly occur on the international stage—domestic policy is negotiated in trade agreements, domestic Internet policy is developed at international governance venues.[29] Allowing the CSE to level its formidable powers at the intentions of individuals (as opposed to states, states agents or terrorist groups) as

---

[26] See e.g., James Ball, Julian Borger and Glenn Greenwald. (2013). "Revealed: how US and UK spy agencies defeat internet privacy and security," *The Guardian*, https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; Jeff Larson. (2013). "Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security," *ProPublica*,, https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

[27] Tamir Israel. (2015). "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation." In Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283, pp 81-83.

[28] Tamir Israel. (2015). "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation." In Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283, pp 81-83.

[29] Tamir Israel. (2015). "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation." In Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283, pp 81-83.

these relate to international affairs invites surveillance of individuals on the basis of legitimate political views, leading to a chill on the voicing of dissenting views globally.[30] This breadth can also threaten the adequacy status of PIPEDA, Canada's federal commercial data protection statute. Adequacy status is conferred under the European Union data protection framework to various foreign privacy laws, allowing companies governed by these laws to receive personal information from EU residents. The unlimited nature of the CSE's foreign intelligence mandate, which includes its targeting of individuals based on political motivations, may lead European courts to suspend PIPEDA's adequacy status.[31]

Recommendation 15.
Redefine "foreign intelligence" so that it retains within its scope information and intelligence regarding the capabilities, intentions or activities of foreign terrorist groups, foreign states and their agents as these relate to international affairs, defence or security, but limits inclusion of information or intelligence relating to the capabilities, intentions or activities of foreign individuals to situations that pose a threat to the security of Canada, as defined in the CSIS Act.

Cybersecurity and Information Assurance

National Defence Act	***CSE Act***
Mandate (s. 273.64 (1)(b)) The mandate of the Communications Security Establishment is	**Cybersecurity and information assurance (s. 18)** The cybersecurity and information assurance aspect of the Establishment's mandate is to

[30] Jonathan W. Penney. (2017). "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study," *Internet Policy Review* 6(2); Jonathon W. Penney. (2016). "Chilling Effects: Online Surveillance and Wikipedia Use," *Berkeley Technology Law Journal* 31(1) 117; Elizabeth Stoycheff. (2016). "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," *Journalism & Mass Communication Quarterly* 93(2); Christopher Parsons. (2016). "Transparency in Surveillance: Role of various intermediaries in facilitating state surveillance transparency," *Centre for Law and Democracy*, http://responsible-tech.org/wp-content/uploads/2016/06/Parsons.pdf; Suné von Solms and Renier van Heerden. (2015). "The Consequences of Edward Snowden NSA Related Information Disclosures," ICCWS 2015 - the Proceedings on the 10th International Conference on Cyber Warfare and Security, Sukuza, South Africa; Bruce Schneier. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W.W. Norton & Company; Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Citizen Lab*, http://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[31] *Schrems v Data Protection Commissioner*, Case C-362/14, October 6, 2015 (CJEU, Grand Chamber); EU Parliament, Committee on Civil Liberties, Justice and Home Affairs, Report: On the US NSA Surveillance Programme, February 21, 2014, 2013/2188(INI), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0139+0+DOC+PDF+V0//EN, in general and in particular paragraphs AQ and QR; Ryan Chiavetta. (2017). "Could Canada lose its adequacy standing?" *IAPP*, https://iapp.org/news/a/could-canada-lose-its-adequacy-standing/.

…	(a) provide advice, guidance and services to help protect
	(i) federal institutions' electronic information and information infrastructures, and
	(ii) electronic information and information infrastructures designated under subsection 22(1) as being of importance to the Government of Canada; and
(b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada;	(b) acquire, use and analyse information from the global information infrastructure or from other sources in order to provide such advice, guidance and services.

The second aspect of the CSE's mandate is to engage in cybersecurity and information assurance activities. Per s. 18 of the *CSE Act*, the CSE is to provide advice, guidance, and services to protect Government of Canada electronic information and information infrastructures as well as electronic information and information infrastructures explicitly designated as being of importance to the Government of Canada (s. 18(a)). Activities under this mandate also entail acquiring, using, and analyzing information from the global information infrastructure and other sources to provide the aforementioned advice, guidance, and services (s. 18(b)).

While proposed subsection 18(a) of the *CSE Act* largely replicates the CSE's existing cybersecurity mandate with respect to Government of Canada controlled information, computer systems, and internal networks, proposed subsection 18(b) will create a framework for the Minister to designate privately held electronic information and information infrastructures as being 'of importance' to the Government of Canada under sub-section 22(1). Notably, subsection 22(1) is open-ended, granting the Minister seemingly limitless discretion to designate any non-government electronic information, infrastructure information, or class thereof as 'important' and bringing it within the scope of the CSE's cybersecurity and information assurance mandate (we will refer to information or infrastructure designated as 'important' under 22(1) as "critical non-government information or infrastructure", as the case may be).

As with the foreign intelligence aspect of the CSE's mandate, the *CSE Act* only obligates the CSE to rely on a Ministerial authorization when carrying out activities falling within the cybersecurity and information assurance aspect of its mandate if those activities would otherwise contravene a Canadian law (*CSE Act*, 23(4)). However, whereas under the existing *National Defence Act* the Minister could only authorize the CSE to contravene one Canadian law (the interception of private communications on a telecommunications network), the *CSE Act* will extend Ministerial authorizations to access infrastructure and acquire "any information originating from, directed to, stored on or being transmitted on or through" that infrastructure (*CSE Act*, 28(1) and (2)). While this provision broadens the scope of activities that the CSE can be authorized to undertake in violation of Canadian law (including the *Charter*), it does not *require* the

CSE to operate under a Ministerial authorization (and under the associated safeguards) unless it is of the view that its actions might contravene a Canadian law. It therefore raises similar concerns to those raised by the *CSE Act*'s mechanism for the foreign intelligence aspect of its mandate.[32]

Recommendation 16.

Amend sub-sections 23(3) and (4) so that activities carried out in furtherance of the foreign intelligence and cybersecurity and information assurance aspects of the CSE's mandate may only incidentally affect or relate to a Canadian or a person in Canada if carried out further to an authorization under subsections 27(1), 28(1) or (2) and 41(1).

Recommendation 17.

Amend the triggering threshold for the CSE to seek an authorization from "must not contravene any other Act of Parliament unless..." (*CSE Act*, at ss. 23(3), 23(4)) to also include breaches of provincial law and common law.

Ministerial Authorizations in furtherance of the cybersecurity aspect of the mandate allow the CSE, despite other Canadian laws, to:

> "...access a federal institution's information infrastructure and acquire any information originating from, directed to, stored on or being transmitted on or through that infrastructure for the purpose of helping to protect it, in the circumstances described in paragraph 184(2)(e) of the Criminal Code, from mischief, unauthorized use or disruption" (*CSE Act,* 28(1)).

In other words, the CSE would be authorized to intercept private communications on the same terms as set out in the *Criminal Code* provision referenced in the *Act*. Namely, the CSE would be permitted to intercept private communications where that interception was reasonably necessary to manage service quality, or to protect the system against acts that would be an offence under subsections 342.1(1) (*unauthorized use of a computer*) or 430(1.1) (*mischief in relation to computer data*) of the *Criminal Code*. The Establishment would also only be permitted to intercept communications transiting the particular computer system (Government of Canada if operating under 28(1) or private sector if under 28(2)) on which the disruption is occurring, in line with paragraph 184(2)(e) which exempts such activity from the general prohibition on intercepting private communications found in the *Criminal Code*.

If, for example, a designated Canadian bank was experiencing some form of an attack, the CSE could intercept private data on the bank's internal networks to analyze that data and determine the nature of the threat following the bank's written request to provide assistance. However, the CSE could not use its foreign intelligence or other resources to intercept private communications from other elements of the Internet in its efforts to analyze or mitigate the attack in question under this aspect of its mandate.[33] This

[32] See discussion under the Foreign Intelligence subheading for an overview of these concerns.

[33] It is important to note that, in the case of other defensive operations undertaken by the CSE under the

appears to correct a problem with the CSE's current cybersecurity regime, which only authorizes the Establishment to intercept private communications under circumstances specified in paragraph 184(2)*(c)* of the *Criminal Code*, i.e. on a telecommunications service provider's network (NDA, 273.65(3)). As pointed out by the CSE Commissioner, the CSE's interception of private communications in furtherance of its cybersecurity mandate rarely occurs under such conditions and, by implication, is at present mostly being conducted in violation of Part VI of the *Criminal Code*.[34] If the unspecified basis for the CSE Commissioner's finding arises because the CSE mostly intercepts private communications on government of Canada networks currently, then the amendment proposed in the *CSE Act* will address the CSE Commissioner's concern.

As noted above, proposed subsection 22(1) of the *CSE Act* grants the Minister broad discretion to designate non-governmental electronic information or information infrastructure as critical, bringing it within the cybersecurity aspect of the CSE's mandate. This is an exceptional departure from the CSE's current legal framework, as it explicitly grants the CSE permission to operate on private Canadian systems and infrastructure potentially implicating a large number of private sector actors. While it is difficult to speculate with regard to the full range of information and infrastructure that will ultimately be designated as critical, at minimum this designation is likely to apply to entities in sectors such as banking, defense, energy, telecommunications, and transportation. Under a Cybersecurity Ministerial Authorization, the CSE may access and interact with critical non-governmental infrastructure--including *any* information hosted or traversing such infrastructure--in the same manner as it can interact with federal government information and infrastructure (*CSE Act,* 28(2)). However, the Minister may only issue a cybersecurity authorization with respect to critical non-governmental infrastructure on written request from the infrastructure owner or operator "to the Establishment to carry out the activity that would be authorized" (s. 34(3)) (the requirement for a written request is maintained even in the case of emergency authorizations: s. 41(4)).

NDA have involved using all three aspects of its mandate to collect information to detect and defend against malicious activity directed towards either Government of Canada systems or information infrastructure designated as of importance by the Government of Canada. See: Communications Security Establishment. (2009 or 2010). "CSEC Cyber Threat Capabilities: SIGINT and ITS: an end-to-end approach," Government of Canada, https://christopher-parsons.com/writings/cse-summaries/#cse-cyber-threat-capabilities.

[34] Office of the Communications Security Establishment Commissioner. (2015). "Highlights of Reviews and Reports Submitted to the Minister in 2014—2015," Government of Canada, https://www.ocsec-bccst.gc.ca/s21/s20/d274/eng/highlights-reviews-reports-submitted: "Since CSE rarely acts in the circumstances set out in paragraph 184(2)(*c*) of the *Criminal Code*, it can be argued that an IT security ministerial authorization issued under subsection 273.65(3) of the *National Defence Act* would not include CSE's primary cyber defence activities. Therefore, if a private communication were intercepted while CSE undertook an activity that was not included "in the circumstances specified in paragraph 184(2)(*c*) of the *Criminal Code*," CSE would not be shielded from the application of Part VI of the *Criminal Code*. Consequently, I believe subsection 273.65(3) of the *National Defence Act* does not accurately reflect CSE's activities because CSE undertakes activities beyond those considered in "the circumstances specified in paragraph 184(2)(*c*) of the *Criminal Code*."

Recommendation 20.

Amend the *CSE Act* to include the criteria used by the Minister to designate electronic information, information infrastructures or classes of electronic information or information infrastructures as "of importance to the Government of Canada" under subsection 22(1) of the CSE Act.

Recommendation 21.

Amend subsection 22(1) of the *CSE Act* such that encoded criteria ensure the designated electronic information and information infrastructures can only be those of "*critical* importance."

The process for the CSE to seek authorization under this aspect of the mandate is otherwise similar to that under the foreign intelligence aspect of its mandate, requiring the Chief of the CSE to make a written application that sets out the facts from which the Minister is able to conclude that there are reasonable grounds to believe that the authorization is necessary and that the criteria in subsection 35(3) of the Act are met (s. 34(3)). As in the foreign intelligence context, the Minister's authorization is similarly subject to approval by the Intelligence Commissioner (s. 29), can also be extended for up to one year without review by the Commissioner, and is subject to the same framework for review, repeal and amendment where a significant change to the facts upon which the authorization was based arises (ss. 38-40). In the case of authorizations pertaining to critical non-government infrastructure, the application must include the written request from the infrastructure owner described above (s. 41(4)).

The *CSE Act* imposes limitations on the collection, use, and retention of any information acquired under a cybersecurity and information assurance authorization. Only information that is necessary to identify, isolate, prevent or mitigate harm to government or critical non-government information or infrastructure may be acquired under such an authorization. Furthermore, the CSE may only retain such information as long as is reasonably necessary (s. 35(3)(a) and (c)), and information identified as relating to a Canadian or Canadian person may only to be analyzed, used, or retained if essential (35(3)(d)). In effect, this loosens safeguards for the privacy of non-Canadians found in the current *NDA* framework, which prohibits the CSE acquiring, using or retaining *any* non-essential information, not just information relating to Canadians (*NDA* para 273.65(4)(d)).

Finally, proposed section 45 of the *CSE Act* provides lawful authority for the CSE to disclose information to designated persons where such disclosure is necessary to protect a federal institutions' electronic information and infrastructure or any critical non-governmental electronic information and infrastructure. Section 45 is limited in application to information "acquired, used or analysed" during activities carried out further to the CSE's cybersecurity mandate, limiting the ability of the CSE to disclose any Canadian data it might acquire through its foreign intelligence or assistance mandates to that applicable to cybersecurity purposes. However, it does not limit the CSE's disclosure of information that it has rendered accessible by means of one of its other mandates (for example, if it has gained access to a Canadian network through its foreign intelligence mandate, but not acquired or analyzed any of the information

passing through it).[35] In terms of oversight and control, the Minister and the Intelligence Commissioner must approve measures to protect the privacy of Canadians when information is disclosed under section 45.

Section 45 is problematic for its use of the permissive 'necessary' standard--a standard the CSE is granted full authority to determine on a case by case basis without input from the Minister or the Intelligence Commissioner. The standard is more permissive than the 'essentiality' standard typically applied when the private data of Canadians is directly engaged. While section 45 does not permit the CSE to direct its disclosure activities at Canadians (sections 23 and 25 continue to apply) it does allow the CSE to include intercepted private communications in its disclosures (subsection 45(2)). As private communications in this context generally relate to interactions with at least a nexus to Canadian persons,[36] the implication is that the CSE will be disclosing Canadian data in at least some contexts, albeit incidentally as part of a larger dataset. This is particularly problematic given the open-ended ability of the Minister to designate any person or class of persons as recipients of information under section 45. Under section 46, the Minister may designate any person or class of persons, including individuals in the private sector and foreign governments, as legitimate recipients of information disclosed further to section 45. The cybersecurity context creates substantial incentives that sensitive private information (acquired or intercepted while internal systems are assessed for security risks) will be disclosed to a broad range of private and public sector parties.

Risks of Purchasing Malware for Defensive Purposes

One type of activity which might be carried out as part of this aspect of the CSE's mandate includes the acquisition of malicious software from vendors for the purpose of developing defensive techniques that are used to protect systems belonging to the Government of Canada or those designated as of importance by the Government of Canada. While such efforts may appear to be to the benefit of Canada's security interests, in practice they must be carefully constrained and subject to thoughtful safeguards, as they necessarily entail supporting an entire industry which operates to undermine and subvert, rather than strengthen and promote, the security of the global information infrastructure. The Citizen Lab's research has consistently demonstrated that companies engaged in this line of work are loosely unregulated, generally unaccountable for the profound human rights implications of the tools they develop, and fail to take steps to ensure that those tools do not fall into the wrong hands—which

---

[35] Communications Security Establishment. (2009 or 2010). "CSEC Cyber Threat Capabilities: SIGINT and ITS: an end-to-end approach," Government of Canada, https://christopher-parsons.com/writings/cse-summaries/#cse-cyber-threat-capabilities.

[36] Craig Forcese. (2017). "Putting the Law to Work for CSE: Bill C-59 and Reforming the Foreign Intelligence Collection and Cybersecurity Process," Ottawa Faculty of Law Working Paper No. 2017-43, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3045507; Tamir Israel. (2015). "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation." In Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283.

they invariably do.[37]

Independence from Executive Control

As noted previously in this section, the CSE would be authorized to intercept private communications on government controlled infrastructure or critical non-government infrastructure where reasonably necessary to manage service quality, or to protect the system against acts that would be an offence under subsections 342.1(1) (*unauthorized use of a computer*) or 430(1.1) (*mischief in relation to computer data*) of the *Criminal Code*. The interception of such communications is not without controversy. As noted by the Library of Parliament, the breadth of the CSE's proposed monitoring of government

---

[37] See as examples: Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert. (2017). "Champing At The Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware," *Citizen Lab*, https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/; John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. (2017). "Reckless V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware," *Citizen Lab*, https://citizenlab.ca/2017/08/nso-spyware-mexico-corruption/; John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. (2017). "Reckless IV: Lawyers for Murdered Mexican women's Families Targeted with NSO Spyware," *Citizen Lab*, https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/; John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. (2017). "Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware," *Citizen Lab*, https://citizenlab.ca/2017/07/mexico-disappearances-nso/; John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. (2017). "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," *Citizen Lab*, https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/; John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. (2017). "Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware," *Citizen Lab*, https://citizenlab.ca/2017/06/more-mexican-nso-targets/; Bill Marczak and John Scott-Railton. (2016). "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender," *Citizen Lab*, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; John Scott-Railton, Morgan Marquis-Boire, Claudio Guarnieri, and Mario Marschalek. (2015). "Packrat: Seven Years of a South American Threat Actor," *Ctiizen Lab*, https://citizenlab.ca/2015/12/packrat-report/; Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune. (2015). "Pay No Attention to The Server Behind The Proxy: Mapping FinFisher's Continuing Proliferation," *Citizen Lab*, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/; Bill Marczak, John Scott-Railton, and Sarah McKune. (2015). "Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware," *Citizen Lab*, https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/; John Scott-Railton and Seth Hardy. (2014). "Malware Attack Targeting Syrian ISIS Critics," *Citizen Lab*, https://citizenlab.ca/2014/12/malware-attack-targeting-syrian-isis-critics/; Morgan Marquis-Boire. (2014). "Schrodinger's Cat Video and the Death of Clear-Text," *Citizen Lab*, https://citizenlab.ca/2014/08/cat-video-and-the-death-of-clear-text/; Morgan Marquis-Boire, John Scott-Railton, Claudio Guarnieri, and Katie Kleemola. (2014). "Police Story: Hacking Team's Government Surveillance Malware," *Citizen Lab*, https://citizenlab.ca/2014/06/backdoor-hacking-teams-tradecraft-android-implant/; Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton. (2014). "Hacking Team and the Targeting of Ethiopian Journalists," *Citizen Lab*, https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/; Morgan Marquis-Boire and John Scott-Railton. (2013). "Quantum Of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns," *Citizen Lab*, https://citizenlab.ca/2013/12/syrian-malware-campaigns/; Morgan Marquis-Boire, Bill Marczak, Caludo Guarnieri, and John Scott-Railton. (2014). "For Their Eyes Only: The Commercialization of Digital Spying," *Citizen Lab*, https://citizenlab.ca/2013/04/for-their-eyes-only-2/.

communications "could have implications with respect to constitutional separation of powers. Both the federal courts and the Supreme Court of Canada have threatened to mount a constitutional challenge in the face of government efforts to force them to use the information technology services provided by Shared Services Canada, which include CSE cybersecurity monitoring on the grounds that to do so would threaten their independence."[38]

Recommendation 22.

Amend the *CSE Act* to allow any federal institution, as defined in s. 2, to submit a written request to the Minister in order to opt-out of cybersecurity advice, monitoring, and other services provided by the CSE, including but not limited to any of the CSE's activities which could otherwise be authorized under s. 28.

Recommendation 23.

Require a written request to carry out the activity from the federal institution in question in order for an authorization to be issued under subsection 28(1), analogous to the provision set out in subsection 34(3) for authorizations under 28(2).

Issues with Existing 'Necessity' and 'Essentiality' Requirements

It is not clear whether collection, use, and retention must meet these thresholds of necessity or essentiality in order to address a *specific* and identified risk of harm, or whether a more generalized scope is envisioned. Similarly, the proposed provisions do not require the minister to issue authorizations on a per-threat basis, meaning that broad authorizations might be issued to generally secure critical non-governmental infrastructure. If this is the case, then the potential breadth of the CSE's new ability to monitor domestic infrastructure is deeply troubling. Were a communications company like Bell or Telus, for example, to request the CSE's help and a Cybersecurity Authorization be subsequently approved, it would then be legal for the CSE to intercept any or all of the private communications carried on that network, as the Establishment would not be limited to intercepting communications relevant only to resolving the specific harm they were requested to address. Moreover, it is not clear that limitations on the retention and use of Canadian data (unless it is essential or reasonably necessary to identify, isolate, prevent, or mitigate harm to electronic infrastructures) would bar retained information from also being analyzed for foreign intelligence, criminal intelligence, or other purposes, when those secondary purposes could assist in the CSE's cybersecurity and information assurance operations.

Defensive and Active Cyber Operations

CSE Act

[38] Tanya Dupuis, Cholé Forget, Holly Porteous, and Dominique Valiquet. (2017). Bill C-59: An Act respecting national security matters - Publication No. 32-1-C59-E," *Library of Parliament*, p. 9.

Defensive cyber operations (s. 19) The defensive cyber operations aspect of the Establishment's mandate is to carry out activities on or through the global information infrastructure to help protect (a) federal institutions' electronic information and information infrastructures; and (b) electronic information and information infrastructures designated under subsection 22(1) as being of importance to the Government of Canada.
Active cyber operations (s. 20) The active cyber operations aspect of the Establishment's mandate is to carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security.

The proposed *CSE Act* creates two "new" aspects of the Establishment's mandate in the form of "defensive cyber operations" and "active cyber operations" respectively. We treat them together in this section because the types of activities that can be authorized, and the authorization framework for each, are broadly similar (though the purpose of each aspect is distinct, and the Minister of Foreign Affairs must consent to offensive cyber operations whereas the Minister is only consulted in the case of defensive cyber operations).

The "defensive cyber operations" aspect of the mandate would enable the CSE to carry out activities "to help protect federal institutions' electronic information and information infrastructures as well as other electronic information and information infrastructures which have been designated as being of importance to the Government of Canada under subsection 22(1) (*CSE Act,* s. 19) (hereafter "critical non-government information or infrastructure"). The "active cyber operations" aspect of the mandate would allow the CSE to carry out activities "to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security" (s. 20). Despite differences in purpose, in both cases, these proposed aspects of the CSE's mandate involve a more "active" role than what legislation has historically afforded the Establishment. The types of activities which could be authorized under either aspect of the mandate would be the same. They may include (*CSE Act,* s. 32):

(a) gaining access to a portion of the global information infrastructure;
(b) installing, maintaining, copying, distributing, searching, modifying, disrupting, deleting or intercepting anything on or through the global information infrastructure;
(c) doing anything that is reasonably necessary to maintain the covert nature of the activity; and
(d) carrying out any other activity that is reasonable in the circumstances and reasonably necessary in aid of any other activity, or class of activities, authorized by the authorization.

The language in section 32 of the proposed *CSE Act* is extraordinarily permissive. Not

only does it set out the legal basis to authorize all manner of state-sponsored hacking, but it also includes two residual categories of activity which allow an authorization for the CSE to also do "anything that is reasonably necessary to maintain the covert nature of the activity" and to carry out any activity "that is reasonable in the circumstances and reasonably necessary in aid of any other activity, or class of activities, authorized by the authorization" (*CSE Act*, 32(c),(d)).

Compared to foreign intelligence and cybersecurity activities, there are some significant differences in the authorization framework for active and defensive cyber operations. In the case of cyber operations, the Chief of the CSE still makes a written application (s. 34(1)) that sets out the facts from which the Minister is able to conclude there are reasonable grounds to believe that the authorization is necessary and that the conditions for issuing it in subsection 35(4) are met (s. 34(2)). Unlike in the course of foreign intelligence or cybersecurity related activities, for the authorization to take effect the Minister does not need to seek the approval of the Intelligence Commissioner.[39] Instead, activities under the defensive cyber operations aspect of the mandate can be authorized by the Minister alone, who needs only to "consult" with the Minister of Foreign Affairs (s. 30). By contrast, where activities under the active cyber operations aspect of the mandate are concerned, the activities can only be authorized if the Minister of Foreign Affairs has requested that the authorization be issued or has consented to its issue (s. 31(2)). What these requests will look like in practice, or what the process of informing the Minister of Foreign Affairs will look like, remains unclear—particularly because these activities can potentially be approved on a class-by-class basis.

Fundamental Problems with Prohibited Activities in Section 33

The only explicit limits on what can be authorized under the permissive framework set out in section 32 power are found section 33(1), which sets out that the Establishment must not:

(a) cause, intentionally or by criminal negligence, death or bodily harm to an individual; or
(b) wilfully attempt in any manner to obstruct, pervert or defeat the course of justice or democracy.

There are three fundamental problems with this section. The first issue is that these explicit limitations for "prohibited conduct" only apply to authorizations issued under the defensive and active cyber operations components of the mandate. In other words, neither causing death or bodily harm (s. 33(1)(a)) nor attempting to interfere with the course of justice or democracy (s. 33(1)(b)) are expressly prohibited activities in the case of foreign intelligence or cybersecurity authorizations. Presuming this is a drafting error, it is essential for legislators to explicitly clarify whether the CSE can be authorized either to cause death or bodily harm, or to interfere with "the course of justice or democracy," as part of the other aspects of its mandate, such as in the course of foreign

[39] This stands in contrast to foreign intelligence or cybersecurity authorizations, which must first be approved by the Intelligence Commissioner before the authorizations come into effect.

intelligence activities.

> **Recommendation 31.**
> Amend section 33 of the *CSE Act* to apply across all aspects of the mandate, and to the entirety of the CSE's activities (with the potential exclusion of activities undertaken subject to the assistance aspect of the mandate).

The second problem is that the wording of this limitation is impermissibly vague. While "bodily harm" carries the same meaning as that term in the *Criminal Code* (s. 33(2)), legal issues of causation and the use of criminal law standards may be less straightforward in the context of the CSE's unique capabilities. More problematically, neither "justice" nor "democracy" are defined in the Act, leaving the door open to shallow or creative interpretations of these terms that undermine their ability to operate as meaningful safeguards. The current provisions provoke more questions than they answer. For example, does the government wish to leave open the possibility to interfere with the electoral or governance processes of foreign states Canada does not deem "democracies," or with courts not operating in accordance with the CSE's understanding of the nebulous concept of "justice"?

> **Recommendation 33.**
> Amend section 33(1)(b) to read, "wilfully attempt in any manner to obstruct, pervert or defeat the course of justice or democracy, including by willfully attempting to obstruct, pervert, or defeat the course of *any judicial proceeding or of any electoral process, directly or indirectly*."

The third problem is that this short list of prohibited conduct—whether it is ultimately applied only to these two aspects of the mandate or to the CSE's conduct more generally—is radically under-inclusive. As drafted, the legislation affords the CSE the ability to engage in a vast range of unenumerated and deeply problematic activities with the potential to seriously interfere with *Charter* protected rights and freedoms, or with Canada's international human rights obligations more broadly. From mass dissemination of false information, to impersonation, leaking foreign documents in order to influence political and legal outcomes, disabling account or network access, large-scale denial of service attacks, and interference with the electricity grid, the possibilities for the types of activities contemplated in section 32 are limited only by imagination. In the case of CSIS' "threat reduction" powers, Bill C-59 would add a longer list of prohibited forms of conduct for CSIS agents acting under the authority of a warrant for such activities (21.1(1.1) of proposed *CSIS Act*). At minimum, the types of limitations imposed on CSIS in proposed section 20(18) should be adopted in the *CSE Act* as an extension of the proposed section 33.

Proposed CSIS Act (s. 20.1(18))	***CSE Act***
Even with prior judicial authorization…	Even with dual Ministerial authorization…

20.1(18) Nothing in this section justifies (a) causing, intentionally or by criminal negligence, death or bodily harm to an individual; (b) wilfully attempting in any manner to obstruct, pervert or defeat the course of justice; (c) violating the sexual integrity of an individual; (d) subjecting an individual to torture or cruel, inhuman or degrading treatment or punishment, within the meaning of the Convention Against Torture; (e) detaining an individual; or (f) causing the loss of, or any serious damage to, any property if doing so would endanger the safety of an individual.	33(1) In carrying out any activity under an authorization issued under subsection 30(1) or 31(1), the Establishment must not (a) cause, intentionally or by criminal negligence, death or bodily harm to an individual; or (b) wilfully attempt in any manner to obstruct, pervert or defeat the course of justice or democracy. **Definition of bodily harm** (2) In subsection (1), bodily harm has the same meaning as in section 2 of the Criminal Code.

Recommendation 32.
Amend section 33(1) of the *CSE Act* to add:
…
(c) violating the sexual integrity of an individual;
(d) subjecting an individual to torture or cruel, inhuman or degrading treatment or punishment, within the meaning of the Convention Against Torture;
(e) detaining an individual; or
(f) causing the loss of, or any serious damage to, any property if doing so would endanger the safety of an individual;
(g) engaging in activities which are likely to undermine the security of publicly available communications technologies, networks, and services, including by weakening or interfering with security standards and protocols.

Low Threshold for Engaging in Activities Described in s. 32

Moreover, the threshold for engaging in the kinds of activities described in section 32 is low—particularly in the context of active cyber operations, where the Establishment can be authorized to interfere "with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security" (s. 20) on no clear basis or grounds. There is no clarification about what "relate" might mean in this context, nor does this section require that the target of the CSE's intervention pose some kind of meaningful threat to Canada's security interests. By contrast, other national security-related legislation uses terms such as a "threat to the security of Canada" (*CSIS Act,* s. 2) or the much more expansive "activity that undermines the security of Canada" (*Security of Canada Information Sharing Act*, s. 2) as a threshold to trigger invasive activities. Indeed, the expansive nature of these

two cyber operations aspects of the CSE's proposed mandate and the corresponding activities set out in section 32 preclude any person from clearly understanding the nature, type, scope, target, triggering conditions, or limitations on the potential activities contemplated by the *Act* in a way that ultimately raises rule of law issues.

Activities authorized under the active or defensive cyber operations aspects of the CSE's proposed mandate have the capacity to be at least as invasive, problematic, and rights-infringing as activities conducted by CSIS in the course of "threat reduction" activities, and (given the nature of the digital ecosystem) are inherently more likely to cause collateral harm to non-targeted parties and infrastructure. The case has not been made that such powers are necessary, nor that they will result in a net benefit to the security of Canadians. It should be noted that even if these new aspects of the CSE's mandate are not ultimately adopted, the Establishment can still participate in "threat reduction" activities alongside CSIS through the assistance aspect of the CSE mandate (*CSE Act*, ss. 21, 26(1), proposed *CSIS Act, s.* 24.1(1)). If Parliament is committed to preserving the disruptive capabilities of the cyber operations aspects of the mandate, an analogous framework to the CSIS warrant regime set out in Bill C-59 or at minimum a more robust framework for independent, real-time oversight is necessary—along with a more extensive list of prohibited activities and a more restrained list of permissible ones. Finally, we would note that a legislative endorsement of state-sponsored hacking by the Canadian government has serious international normative implications, and is likely to legitimize and encourage other states—including those with problematic human rights records—to do the same.

Recommendation 36.
Require Parliament to undertake a study which addresses (1) the division of labour and separation of roles between the CSE and the Canadian Forces with regard to cyber operations, and the division of labour and separation of roles between the CSE and CSIS with regard to foreign intelligence activities.

Technical and Operational Assistance

National Defence Act	***CSE Act***
Mandate (s. 273.64 (1)(c)) The mandate of the Communications Security Establishment is ... (c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.	**Technical and operational assistance (s. 21)** The technical and operational assistance aspect of the Establishment's mandate is to provide technical and operational assistance to federal law enforcement and security agencies, the Canadian Forces and the Department of National Defence.

The technical and operational assistance aspect of the CSE's mandate in the *CSE Act* would entail the use of CSE expertise, resources and surveillance capabilities to assist

federal law enforcement and security agencies (s. 21). The proposed *Act* now also makes explicit that the CSE is able to support the activities of the Canadian Forces and the Department of National Defence (s. 21). When relying on this aspect of its mandate, the CSE operates under the authority of the agency or department it is assisting and is subject to the same limitations as the assisted agency or department (s. 26(1)). The CSE personnel who carry out activities under this aspect of the CSE's mandate also enjoy the same exemptions, protections, and immunities as a person employed by the agency to whom the CSE is providing assistance (s. 26(2)). The *CSE Act* largely retains the CSE's current ability to assist other agencies without adding additional safeguards or limitations. This is problematic, as the CSE's surveillance capabilities have been developed through activities that would be unconstitutional if undertaken by another Canadian agency such as the RCMP. In spite of this, the CSE's technical and operational assistance aspect of its mandate places these surveillance capabilities at the disposal of the agency being assisted.

When operating under its technical and operational assistance mandate, the CSE is not restrained by the minimal requirement of operating under a ministerial authorization as it is when carrying out other otherwise law-infringing aspects of its mandate, nor do these activities require approval from the Intelligence Commissioner. Activities undertaken under the CSE's mandate to provide technical and operational assistance may be directed at Canadian persons or persons in Canada, as well as portions of the global information infrastructure within Canada, to the extent the assisted agency is authorized to do so. According to a recent internal CSE policy document, the Establishment may only provide assistance under this mandate after receiving a written request from the relevant agency, although it "may perform preliminary work in anticipation of a written request for assistance."[40] However, this requirement is not laid out in either the existing or the proposed statute.

The rationale for imposing minimal restrictions on what the CSE may do when providing assistance to other agencies is that the agencies being assisted must be duly authorized to carry out the activity in question and the CSE is simply relying on these agencies' authorization. However, the CSE's assistance entails use of its existing surveillance and disruption network and capabilities as well as those of its Five Eyes partners. For example, in 2013, the Federal Court found that the CSIS had misled it regarding the extent to which it was relying on Five Eye partner agencies when seeking CSE assistance for intercepting the communications of Canadians abroad.[41] The Federal Court found that this constituted an interference with international human rights, and could not be achieved without explicit lawful authority.[42] In response, the Canadian government amended the *CSIS Act* to create a mechanism for authorizing CSIS activities

[40] Communications Security Establishment. (2016). "OPS-4: Policy on Assistance to Law Enforcement and Security Agencies under Part (c) of CSE's Mandate," Government of Canada, released in redacted form under the Access to Information Act, https://christopher-parsons.com/wp-content/uploads/2017/12/A-2016-00101c.P.9703-Ter_001.pdf.

[41] *Re X*, 2013 FC 1275

[42] *Re X*, 2013 FC 1275

abroad.[43] However, when assisting other agencies such as the RCMP, the CSE is presumably still limited to drawing on its own resources.

This reliance on an expansive surveillance web changes both the nature and the scope of activity that occurs further to a lawful authorization, rendering it significantly more intrusive. Yet there is no mechanism to account for this greater level of intrusiveness. In developing its surveillance capabilities, the CSE can employ a broad range of practices, including: developing and gaining access to key data transit points, compromising stored data repositories held by third party Internet companies such as social media networks or email providers, acquiring or developing security vulnerabilities, promulgating deficient encryption protocols, degrading or co-opting the effectiveness of anti-virus software, developing a global sensor network capable of analyzing global data traffic in real-time and acting on such traffic on a case-by-case basis, collecting bulk data sets that are publicly available for sale, acquiring and using malware or exploits designed to compromise the security of information infrastructure, engaging in effects operations designed to psychologically disturb or disrupt a person for the purpose of gaining access to a communications network or database, or interfering with or compromising software update processes to provide a measure of access to those reliant on targeted equipment or software. Many of these activities and capabilities fall well outside the scope of what most assisted agencies could be lawfully authorized to accomplish, yet these agencies are able to pick the poisoned fruit that grows from the CSE's operational infrastructure.

In addition to its own activities, the CSE draws on data sources and operational techniques gathered and undertaken by its partner agencies, and may include activities or operations that exceed the scope of operations the CSE is authorized to engage in. As examples, active cyber operations might be conducted by the CSE's allies which would, were they conducted by the CSE, require the Minister of Foreign Affairs to consent to the activity in question. Similarly, foreign intelligence services working on behalf of the CSE to fulfil an operation may conduct operations that would exceed those that have been, or would be, approved by the Intelligence Commissioner, thus enabling the CSE to engage in activities on behalf of domestic agencies which exceed the CSE's own legally authorized range of activities.

Recommendation 29.

Specify that data acquired and capabilities developed further to the CSE's foreign intelligence and cybersecurity and information assurance aspects of its mandate cannot be used, analyzed or disclosed when carrying out activities under the technical and operational assistance aspects of its mandate.

[43] See for example, *Canadian Security Intelligence Service Act*, RSC 1985, c C-23, sub-section 21(3.1).

Recommendation 30.
When providing technical or operational assistance to domestic law enforcement and other agencies, restrict the CSE from providing access to capabilities or information developed by its international partners—in other words, the assistance aspect of the mandate should be limited to the provision of "in house" expertise.

ii. Review, Oversight, and Independent Control

One of Bill C-59's most important CSE-related reforms is its addition of a framework for integrated review and external control in the form of the National Security and Intelligence Review Agency (NSIRA) and the Intelligence Commissioner, respectively. The newly constituted bodies address many long-standing problems in Canada's national security framework but several shortcomings may prevent these new mechanisms from fully realizing their potential in practice. In particular, the Intelligence Commissioner falls far short of providing the level of effective external control required for the CSE to operate in a proportionate manner, and fails to meet the constitutional minimum for such control.

Review

Bill C-59 replaces the Security Intelligence Review Committee (SIRC)—which is currently tasked with reviewing the activities of CSIS—with the NSIRA. NSIRA also replaces the functions of the current CSE Commissioner, who is presently responsible for reviewing the Establishment's activities, investigating and responding to complaints, and reporting on the CSE's legal compliance, among other reporting obligations (*NDA*, s. 273.63).

The existing gaps in Canada's national security review framework are well-documented and closely linked to the heavily siloed nature of current review.[44] SIRC review is limited to CSIS activities, the CSE Commissioner may only review the CSE's activities, and various other agencies with a national security dimension to their mandate remain altogether lacking in adequate review. [45] By contrast, modern national security investigations often engage multiple agencies in a highly integrated manner. The CSE in particular, under the 'assistance' component of its mandate, is able to leverage significant resources and capacities to support the efforts of other agencies. Despite these close

[44] Craig Forcese and Kent Roach. (2017). "The roses and the thorns of Canada's new national security bill," *Macleans*, http://www.macleans.ca/politics/ottawa/the-roses-and-thorns-of-canadas-new-national-security-bill/; Bill Robinson. (2017). "Bill C-59: New dogs for new tricks," *Lux Ex Umbra*, https://luxexumbra.blogspot.ca/2017/07/bill-c-59-new-dogs-for-new-tricks.html; Michael Geist. (2017). "Five Eyes Wide Open: How Bill C-59 Mixes Oversight with Expansive Cyber-Security Powers," *Michael Geist* (blog), http://www.michaelgeist.ca/2017/06/billc59/; Chuck Strahl. (2013). "The Standing Committee on National Security and Defence: Evidence," Parliament of Canada, http://www.parl.gc.ca/content/sen/committee/412%5CSECD/51109-E.HTM.

[45] Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Citizen Lab*, http://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

relationships, the CSE Commissioner is currently limited from examining the activities of recipient agencies, which significantly limits her or his ability to evaluate the full impact or scope of the activities in question. Conversely, the entities tasked with review of assisted agencies (such as SIRC) cannot assess the CSE's activities in relation to their own mandates, creating blind spots in instances of multi-agency collaboration. By contrast, NSIRA would be an integrated body with jurisdiction over activities carried out by CSIS, the CSE, as well as the national security or intelligence activities of other departments to the extent these relate to national security or intelligence (*NSIRA Act,* s. 8).

The newly created agency would be able to trace the impacts of national security and intelligence activities across different agencies and be able to more comprehensively review the CSE's activities. The existing role of the CSE Commissioner is largely preoccupied with reviewing the Establishment's activities to ensure that they are in compliance with the law (*NDA* s. 273.63(2)). However, this approach constitutes a limited form of review, as under the *National Defence Act* the CSE operates under a vague and highly permissive legal framework and is subject to broadly framed ministerial authorizations that afford the Establishment significant operational latitude. Even where this latitude is exercised in a highly disproportionate manner, it may still appear to remain within legal boundaries, leaving the CSE Commissioner with a limited toolset to meaningfully review such practices. Making matters worse, the CSE Commissioner cannot impose her or his own interpretation of the CSE's enabling legislation, which means that the Commissioner's analysis of the CSE activities largely occurs through the lens of the Establishment's own legal theories and interpretations.[46] By contrast, NSIRA is mandated to evaluate not only whether the CSE is in compliance with the law, but also the overall reasonableness and necessity of the Establishment's use of its powers (*NSIRA Act*, s. 33(2)). This mandate provides NSIRA a more robust baseline against which to assess and evaluate the activities of the CSE.

NSIRA Access to Foreign-Provided Information

One potential issue with this review framework is the NSIRA's inability to review the CSE's interaction with foreign agencies. While in theory NSIRA is to have access to all "information that is in the possession or under the control of any department" in the course of its reviews, there may be some gaps where Canada's intelligence bodies act in concert with foreign allies and cannot be said to be in possession or control of certain documents or may be otherwise unable to share them due to principles of 'originator

[46] Communications Security Establishment Commissioner, Annual Report 2005-06, April 2006, https://www.ocsec-bccst.gc.ca/a78/ann-rpt-2005-2006_e.pdf, pp 9 and 17: Former Chief Justice of Canada, Antonio Lamer: "With respect to my reviews of CSE activities carried out under ministerial authorization, I note that I concluded on their lawfulness in light of the Department of Justice interpretation of the applicable legislative provisions. … My one regret will be if I leave this position without a resolution of the legal interpretation issues that have bedevilled this office since December 2001." Communications Security Establishment Commissioner, Annual Report 2006-07, May 2007, https://www.ocsec-bccst.gc.ca/a77/ann-rpt-2006-2007_e.pdf, pp 2-3. Tamir Israel, "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation", in *Ed* Michael Geist, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, (Ottawa: University of Ottawa Press, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283, pp 72-76.

control (NSIRA *Act*, s. 9). Specifically, there is concern that foreign-provided information will be immunized from NSIRA access if caveats indicating 'originator control' are applied to shared information. The concern is that the CSE may interpret third party information and intelligence obtained in this manner as beyond its "possession or control", placing it outside the scope of NSIRA's right of access.[47] Given the high frequency with which the CSE interoperates with foreign agencies, this interpretation could potentially operate as a significant limitation on NSIRA's ability to gauge the full impact of the CSE's activities.

Recommendation 1.

Amend section 9 of the *National Security and Intelligence Review Agency Act* to clarify that the NSIRA is entitled to access documents in the possession or under the control of any department, including all documents originating from foreign governments, their respective intelligence agencies, and international bodies—despite any limitation imposed by those foreign bodies or by "originator control."

NSIRA Employment of Former Intelligence Agency Staff

The *NSIRA Act* also provides for a secretariat to support the work of the review agency. The legislative summary of Bill C-59 produced by the Library of Parliament points out that "section 48 mobility provisions enable the secretariat to hire employees from departments and agencies, raising the possibility of direct hiring from intelligence and national security agencies." From our perspective, while such individuals are certain to have a great deal of relevant expertise, they will also generally lack the independence and distance necessary, or will be perceived to lack the independence and distance necessary, to perform activities in the service of the review agency.

Recommendation 2.

Amend section 48 of the *National Security and Intelligence Review Agency Act* to prohibit the secretariat from engaging in direct hiring from intelligence and national security agencies, and to impose a reasonable time limitation for prospective secretariat employees who have been employed by those agencies in the past.

Reporting on Collection of Canadian and Canadian-Related Data

The CSE will likely collect significant swathes of information pertaining to Canadians and of persons in Canada, in the course of the foreign intelligence, cybersecurity and information assurance, and technical and operational aspects of its mandate. This information will now include CSE's collection of publicly available information and infrastructure information—which will include information of Canadians or persons in Canada. Given the permissive capacity for the CSE to collect this information it should at a minimum collect statistics on the number of times it has collected this information,

---

[47] Tanya Dupuis, Cholé Forget, Holly Porteous, and Dominique Valiquet. (2017). Bill C-59: An Act respecting national security matters - Publication No. 32-1-C59-E," *Library of Parliament*, p. 3 as well as footnote 12.

reasons or aspects of its mandate for which the information was collected, number of times masked and unmasked information was provided to foreign partners, number of times masked and unmasked information was provided to domestic partners, and retention periods for all collected information. Such reporting should also include the number of times that the CSE acted under the technical and operational assistance aspect of its mandate, and to which agency or agencies it provided such assistance. Finally, the Government of Canada should report, on an annual basis, the foreign intelligence and cybersecurity priorities it issues to the CSE. Either the *National Security and Intelligence Committee of Parliamentarians* (NSI-CoP),[48] or the NSIRA should be tasked with compiling the provided statistics in annual reports which are made public and should be authorized to periodically evaluate expand the recordkeeping requirements imposed on the CSE and, correspondingly, whether additional ranges or kinds of statistics should be provided in their annual reports. The decision to expand the CSE's reporting requirements and to expand what either the Committee of Parliamentarians or NSIRA subsequently report on should be left to the respective oversight or review body.

Recommendation 48.
Require the Government of Canada to publicly report, on an annual basis, the foreign intelligence_and cybersecurity priorities it establishes for the CSE.

Recommendation 52.
Require public reporting on the frequency at which the CSE provides technical and operational assistance to other entities, as well as reporting about which agencies receive that assistance, in the CSE's annual review documents.

Recommendation 53.
Require the NSIRA to review, on a regular basis, the structure and information provided by the CSE in its annual report and be authorized to recommend the CSE include specific information in future reporting, including periodic inclusion of statistical information regarding the nature and scope of its activities.

Recommendation 54.
Require public reporting on the frequency of defensive and active cyber operations.

Oversight and Control

In addition to the creation of NSIRA, Bill C-59 replaces the current CSE Commissioner with a new Intelligence Commissioner, which would have the effect of introducing a degree of external control over the CSE's activities for the first time. The Intelligence

[48] Enacted by Bill C-22, *National Security and Intelligence Committee of Parliamentarians Act*, Royal Assent received June 22, 2017, 1st Sess, 42nd Parl, 2017, http://www.parl.ca/Content/Bills/421/Government/C-22/C-22_4/C-22_4.PDF.

Commissioner will have the power to review some Ministerial authorizations and conclude whether the basis upon which these authorizations were issued or amended is reasonable (*IC Act*, pr ss. 13-16). In particular, the Commissioner must approve any foreign intelligence and cybersecurity Ministerial authorizations before the CSE can undertake any activities further to these authorizations, except in "emergency" circumstances (*CSE Act*, s. 41(2)).

The Intelligence Commissioner addresses a long-standing gap in the CSE's framework. Currently, the primary source of legal control over the CSE's activities is the Minister of National Defence. The Minister currently issues the authorizations that the CSE must obtain before it can intercept private communications protected by the Canadian *Criminal Code* and is also responsible for providing any lawful authority the CSE might require to interfere with *Charter* protected rights.[49] Under the Canadian *Charter*, authorization to interfere with reasonable expectations of privacy must be issued by an "entirely neutral and impartial" arbiter capable of acting judiciously.[50] Yet at present, the Minister of National Defence (alongside the rest of the executive branch) is responsible on the one hand for determining the CSE's intelligence priorities while on the other for authorizing how far the CSE can go to achieve these objectives. [51] Ministers in general are governed by considerations of expediency, public policy, and their duty as members of the executive branch of the government.[52] They lack the impartiality, independence, and objectivity necessary to control the activities of an agency such as the CSE in a judicial manner. The existing CSE Commissioner, while exercising a degree of independence, has no capacity to control the CSE's activities—only to perform after-the-fact review without any power to bind the Establishment's future activities. Indeed, many of the recommendations and legal interpretations proposed by CSE Commissioners over the years have simply been ignored by the Establishment.

The proposed Intelligence Commissioner, by contrast, may refuse to approve Ministerial authorizations related to the foreign intelligence and cybersecurity aspects of the CSE's mandate, providing an element of independent control over those aspects of the CSE's activities. However, while government statements present the Intelligence Commissioner as independent and quasi-judicial in nature, [53] the Intelligence

---

[49] Tamir Israel. (2015). "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation." in Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283.

[50] *Hunter v Southam Inc,* [1984] 2 SCR 145 at 160—62; *R v Vu,* [2013] 3 SCR 657 at 46.

[51] Tamir Israel. (2015). "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation." In Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283; National Defence Act, s 273.64(1)(a); Office of the Communications Security Establishment Commissioner. (2017). "Frequently Asked Questions," Government of Canada, http://ocsec-bccst.gc.ca/new-neuf/faq_e.php: "Establishing intelligence priorities is a prerogative of the executive arm of government."

[52] *Canada (Minister of National Revenue) v Coopers and Lybrand Ltd*, [1979] 1 SCR 495, 507–8.

[53] See, for example, Department of Justice, "Charter Statement - Bill C-59: *An Act respecting national secrity matters*", June 20, 2017, http://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/ns-sn.html, "… Part 2 of Bill C-59, the *Intelligence Commissioner Act*, would establish an independent, quasi-judicial Intelligence Commissioner…"

Commissioner lacks sufficient independence, procedural safeguards, and powers to carry out a judicial function. The position is further hampered by the limited scope of oversight and control granted to it.

Quasi-Judicial Nature of Intelligence Commissioner

While the Intelligence Commissioner has consistently been described as "quasi-judicial"[54] the position lacks certain hallmarks of judicial independence that would otherwise strengthen the Commissioner's role. In particular, the Commissioner serves during good behaviour, with remuneration set and renewal determined by the Governor-in-Council. These factors have implications for security of tenure and may implicate the Commissioner's ability to act in a fully independent manner, or impact public perception of that independence (*Intelligence Commissioner Act*, 4(1), 4(4)).[55] By contrast, the Commissioner's UK counterpart "may not…be removed from office before the end of the term" of appointment, barring certain explicitly itemized and non-discretionary conditions, such as if the Commissioner is convicted of a criminal offence leading to imprisonment.[56] We are also concerned about the extent to which the Intelligence Commissioner can be expected to meaningfully fulfill her or his duties on a part-time basis (*Intelligence Commissioner Act*, s 4(3).

Recommendation 3.

Amend section 4(3) of the *Intelligence Commissioner Act* to require, or at least provide the option for, a full-time Intelligence Commissioner.

Recommendation 4.

Amend section 4(4) of the *Intelligence Commissioner Act* so that remuneration of the Intelligence Commissioner is set in relation to the salary of a judge of the Federal Court under paragraph 10(d) of the *Judges Act* (if the Commissioner remains part-time, this amount can be pro-rated).

Appeal of Intelligence Commissioner Decisions

While decisions of the Intelligence Commissioner must be in writing, she or he is only required to issue *reasons* when rejecting an authorization (*IC Act*, compare s. 21(a) and s. 21(b)). This, in combination with the fact that decisions will be entirely secret to the public, means that decisions of the Commissioner can only be appealed where she or he rejects a Ministerial authorization—and not where an authorization has been approved that perhaps should not have been. As a result, the Commissioner remains limited in her or his capability to become a source of jurisprudence in relation to the CSE's activities, and though NSIRA will

---

[54] See, for example, Department of Justice, "Charter Statement - Bill C-59: *An Act respecting national secrity matters*", June 20, 2017, http://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/ns-sn.html, "… Part 2 of Bill C-59, the *Intelligence Commissioner Act*, would establish an independent, quasi-judicial Intelligence Commissioner…"

[55] *Provincial Judges Reference*, [1997] 3 S.C.R. 3.

[56] Government of the United Kingdom. (2016). "Investigatory Powers Act 2016 (Chapter 25)," The National Archives, http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf, subsections 228(4)-(5).

have the ability to review authorizations, there is no real judicial mechanism to contest illegal or unconstitutional authorizations once made. In theory, the Ministerial authorizations themselves may be subject to judicial review—but because they are secret to the public, there is no party that would have either the awareness or standing to contest them. It is notable that even the decisions of the United States Foreign Intelligence Surveillance Court (FISC), though generally highly redacted, are sometimes made public in some form.

Recommendation 6.
Amend section 21(a) of the *Intelligence Commissioner Act* to require the Commissioner to issue written reasons when approving the authorization, amendment or determination mentioned in that section.

Recommendation 8.
Create a mechanism for challenging or appealing decisions rendered by the Intelligence Commissioner.

Recommendation 12.
Require that both authorizations made by the Minister and decisions made by the Intelligence Commissioner be made public to the greatest extent possible

Recommendation 14.
Require the CSE to proactively provide the NSIRA with any internal legal interpretations it adopts that are novel or which have been subject to substantial change.

Lack of Intervenor or Adversarial Input

Given the important constitutional and human rights concerns at stake, the process is lacking an adversarial dimension more generally. While we are supportive of the fact that the Commissioner will be empowered to retain technical advisors or other specialists (*IC Act*, s. 10), there is no framework for intervenors to participate or to provide adversarial input. The system of review is also highly deferential at all levels: Ministers grant authorizations on the basis of "reasonable grounds to believe" that the authorization is necessary and that the issuing conditions have been met; the Intelligence Commissioner approves those authorizations on a reasonableness standard; and presumably (though it is not mentioned in statute) the standard for judicial review of the Intelligence Commissioner's decisions is also reasonableness.

Recommendation 5.
Amend the *Intelligence Commissioner Act* and the *CSE Act* so that the Intelligence Commissioner has the ability to impose conditions on approved authorizations; the obligation to rule on the legality, constitutionality, reasonable necessity, and proportionality of any activity undertaken by the CSE; and order-making powers to prevent the CSE from carrying out any activities that are either illegal, unconstitutional, disproportionate or not reasonably necessary.

Recommendation 8.
Create a mechanism for challenging or appealing decisions rendered by the Intelligence Commissioner.

Recommendation 13.
Introduce some form of security-cleared *amicus* or other manner of adversarial input in the authorization process for activities under the foreign intelligence, cybersecurity, and cyber operations aspects of the mandate.

Lack of Fact-finding and Order-Making Powers

An effective quasi-judicial body must be empowered to do more than simply approve or disapprove Ministerial authorizations presented to it on the basis of the record available to the Minister issuing the authorization. An effective quasi-judicial body must, at minimum, possess the ability to inquire into the underlying facts on which it is called upon to render its decisions. The current CSE Commissioner, for example, is imbued with all the powers of a commissioner granted under Part II of the *Inquiries Act* (*NDA*, subsection 273.63(4)). The Intelligence Commissioner's UK counterparts (the newly created Investigatory Powers Commissioner and other Judicial Commissioners) are likewise empowered to "carry out such investigations, inspections and audits as the Commissioner [in question] considers appropriate for the purposes of the Commissioner's functions", may compel the disclosure of any required information or documents, and may even inspect locations and technical facilities required to carry out its functions.[57] Similarly, as noted below, the Intelligence Commissioner must be able to exert oversight and control not over the Ministerial authorizations alone, but also underlying CSE activities to ensure these are lawful, proportionate and reasonably necessary. To achieve this objective, the Intelligence Commissioner should be granted order-making powers so that it may prevent the CSE from carrying out any activity or to compel it to undertake certain measures beyond those contained in the Ministerial authorizations, as required. If necessary, these powers can be contingent on approval by the Federal Court.

Recommendation 5.
Amend the *Intelligence Commissioner Act* and the *CSE Act* so that the Intelligence Commissioner has the ability to impose conditions on approved authorizations; the obligation to rule on the legality, constitutionality, reasonable necessity, and proportionality of any activity undertaken by the CSE; and order-making powers to prevent the CSE from carrying out any activities that are either illegal, unconstitutional, disproportionate or not reasonably necessary.

[57] Government of the United Kingdom. (2016). "Investigatory Powers Act 2016 (Chapter 25)," The National Archives, http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf, section 235.

Recommendation 7.
Amend the *Intelligence Commissioner Act* to grant the Intelligence Commissioner all powers granted to commissioners under Part II of the *Inquiries Act*, as subsection 273.63(4) of the *NDA* grants the current CSE Commissioner.

Limited Scope of Oversight and Control

As currently set out in Bill C-59, the position of the Intelligence Commissioner is deficient in its scope of envisioned control. It would remain the case that Ministerial authorizations could, and in most cases probably would, be issued with respect to "classes of activities" as opposed to specific activities, operations, or programs undertaken by the CSE. As a result, the authorizations would inherently lack the specificity necessary to allow the Commissioner to be fully apprised of that which is being authorized, or to ensure that the CSE's activities remain proportionate. For example, a single Ministerial authorization might provide a general framework for acquiring data from the Internet. The framework itself might be reasonable, yet specific problematic acquisition activities—from the compromise of data links in a cloud provider's data centre to the coercion of a system administrator to obtain network access—would likely to be too granular for the Intelligence Commissioner to review. Moreover, when faced with an authorization for the CSE's activities, the Commissioner only has two choices: to approve or reject the authorization (*IC Act*, s. 21(1)). By contrast, when the Intelligence Commissioner reviews CSIS' retention of foreign datasets under the Bill C-59 framework, she or he is actually able to approve an authorization *with conditions* (*IC Act,* s. 21(2)(b)). Affording the Commissioner an ability to impose additional conditions for *all* authorizations would allow for greater dialogue at the outset of the authorization process and empower the Commissioner to take a more active role in setting boundaries and *Charter* safeguards for the Establishment.

Recommendation 5.
Amend the Intelligence Commissioner Act and the CSE Act so that the Intelligence Commissioner has the ability to impose conditions on approved authorizations; the obligation to rule on the legality, constitutionality, reasonable necessity, and proportionality of any activity undertaken by the CSE; and order-making powers to prevent the CSE from carrying out any activities that are either illegal, unconstitutional, disproportionate or not reasonably necessary.

The Commissioner also cannot review or make determinations on emergency authorizations (*CSE Act,* s. 41(2)). An emergency authorization can be issued to the CSE without the Intelligence Commissioner's approval if the Minister has reasonable grounds to believe that the conditions have been met but that "the time required to obtain the Commissioner's approval would defeat the purpose of issuing an authorization" (*CSE Act,* s. 41(1)). While subject to the same reasonableness and proportionality concerns as a regular authorization (*CSE Act*, s. 35(1)), time appears to be the only additional justifying factor here, which is an extremely low bar for an "emergency" framework. The constitutional minimum for bypassing authorization requirements for intercepting private communications is 'exigent

circumstances', which is a term that the Supreme Court of Canada has defined narrowly.[58] Emergency powers should only be available in circumstances where bypassing authorization processes is necessary to prevent serious harm. Slightly better language might be borrowed from the CSIS dataset context, where exigent circumstances allow otherwise unauthorizable queries to be justified when such a query is required to "preserve the life or safety of any individual," or "to acquire intelligence of significant importance to national security, the value of which would be diminished or lost if the Service is required to comply with the authorization process" (CSIS Act, 11.22(1)(b)). This latter condition remains a fairly low threshold but at least it requires the CSIS Director to undergo a process of identifying the specific value of the specific intelligence sought and the importance of the rationale for seeking it (CSIS Act, 11.22(2)). The Intelligence Commissioner is involved in reviewing these exigent circumstances authorizations for CSIS dataset queries (*CSIS Act*, 11.23) but, under the *CSE Act*, emergency authorizations are sheltered from even after-the-fact scrutiny by the Intelligence Commissioner (*CSE Act*, 41(2)).

Recommendation 11.

Amend the CSE Act to require that any emergency authorization under section 41 be reviewed ex post by the Intelligence Commissioner.

Recommendation 34.

Amend the CSE Act so that emergency authorizations may only be issued in truly exigent circumstances.

Finally, activities further to the CSE's defensive cyber operations, active cyber operations, and technical and operational assistance mandates require no approval from the Intelligence Commissioner at all. The lack of Intelligence Commissioner approval over technical and operational assistance activities mirrors the lack of Ministerial authorization and serves to compound the problems raised by this absence.[59]

Recommendation 10.

Require both approval of the Intelligence Commissioner and authorization by the Minister for activities undertaken further to the technical and operational assistance aspect of the CSE's mandate.

It is deeply problematic that neither the Intelligence Commissioner nor any other institution capable of exercising independent control and oversight is involved in the process of approving authorizations for the CSE's activities that would be carried out under the active and defensive cyber operations aspects of its mandate. Authorizations under either of these two aspects will afford the CSE considerably greater latitude to act than the Establishment currently enjoys under the National Defence Act. While the CSE has always conducted some degree of disruptive activity of the kind that could be authorized under section 32—for example, by using malware or exploiting vulnerabilities latent in software and equipment to facilitate the collection of foreign intelligence—in theory these activities have been done to

[58] *R v Tse*, 2016 SCC 16, para 10.

[59] These problems are discussed above. See: "Technical & Operational Assistance".

facilitate or enable other aspects of the Establishment's mandate. The changes proposed in the *CSE Act*, by contrast, are significant because they would allow the CSE to act offensively and preemptively, unbound by the purposes of furthering the Establishment's foreign intelligence or cybersecurity efforts.

The lack of Intelligence Commissioner control for these two aspects of the mandate appears premised on the government's assumption that "cyber operations would not by definition engage Charter rights or freedoms."[60] The government acknowledges that some cyber operations might engage rights or freedoms, but implies that the nature of the operations, the additional limitation on directing activities at Canadian infrastructure, and the additional limitations on causing death or bodily harm, or attempting to pervert the course of justice or democracy are sufficient to forgo the Intelligence Commissioner approval required for other CSE authorizations.[61] The Government of Canada's *Charter* statement for Bill C-59 correctly indicates that the Minister must exercise their discretion to issue authorizations in a manner that is consistent with *Charter* values, compelling the Minister to consider specific *Charter* impacts when issuing cyber operation authorizations.[62] However, as noted above, the Minister lacks the impartiality, independence, and objectivity necessary to render such determinations in a judicious manner.

Critically, the government's underlying presumption that activities authorized under the cyber operations aspects of the mandate are less likely to engage *Charter* rights and freedoms is difficult to sustain. Cyber operations are at *least* as likely, by their nature, to impact all manner of *Charter* protected interests, as well as to raise international human rights concerns which are in some cases even more acute and complex than activities carried out under the Establishment's other mandates. Cyber operations can be anticipated to regularly implicate reputation, freedom of expression, rights guaranteeing free mobility and freedom from arbitrary detention and others. Many cyber operations have not been rigorously tested in courts, meaning that the degree to which they may impact on these *Charter* protected interests is not well defined. The need for an impartial decision-maker acting judiciously is thus all the more heightened.

The lack of any meaningful oversight or control framework for the cyber operations activities of the CSE is particularly troubling in light of parallel debates concerning the "threat reduction" powers first afforded to CSIS in the *Anti-terrorism Act, 2015* (formerly Bill C-51). The types of activities which can be authorized pursuant to the active and defensive cyber operations aspects of the mandate in the *CSE Act* are significantly analogous to the controversial regime in the *CSIS Act* context. The 2015 Bill afforded CSIS new and highly controversial powers to conduct all manner of "measures, within or outside Canada, to reduce a threat to the security of Canada," allowing the agency to potentially disseminate false

---

[60] Department of Justice. (2017). "Charter Statement - Bill C-59: *An Act respecting national security matters*," Government of Canada, http://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/ns-sn.html.

[61] Department of Justice. (2017). "Charter Statement - Bill C-59: *An Act respecting national security matters*," Government of Canada, http://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/ns-sn.html.

[62] Department of Justice. (2017). "Charter Statement - Bill C-59: *An Act respecting national security matters*," Government of Canada, http://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/ns-sn.html.

information, interfere with communications tools, impersonate members of the press, and conduct other problematic operations in secrecy (*CSIS Act,* 12.1, 12.2, 21.1). Bill C-59 would amend these powers in order to clarify that any measure taken by CSIS which would limit a right or freedom guaranteed by the *Charter* must be authorized by warrant issued by a Federal Court judge. Yet where "active cyber operations" are concerned—the digital equivalent of these new powers granted to CSIS—the *CSE Act* and Bill C-59 provides no such framework for prior judicial authorization for situations in which activities undertaken by the CSE limit a right or freedom guaranteed by the *Charter* are concerned. Indeed, not even more basic forms of oversight through the Intelligence Commissioner are included in the Bill as it is currently drafted.

Recommendation 9.
Require both approval of the Intelligence Commissioner and consent of the Minister of Foreign Affairs for all active and defensive cyber authorizations under sections 30 and 31.

To offer meaningful independent control, the Intelligence Commissioner must at minimum be able to review *all* of the CSE's authorizations and be able to rule on the legality, constitutionality, and proportionality of *any* of the CSE's activity. Though Bill C-59 aspires to impose a regime of quasi-judicial control over the CSE's activities it ultimately fails to do so. Fundamentally, the process remains Ministerially-driven and the Intelligence Commissioner lacks the independence, control, procedural mechanisms, and scope of oversight to provide a meaningful measure of quasi-judicial control.

iii. "Not Directed at Canadians," Except…

No activities - Canadians and persons in Canada
23 (1) Activities carried out by the Establishment in furtherance of the foreign intelligence, cybersecurity and information assurance, defensive cyber operations or active cyber operations aspects of its mandate must not be directed at a Canadian or at any person in Canada.

No activities - global information infrastructure in Canada or without authorization
(2) Activities carried out by the Establishment in furtherance of the defensive cyber operations or active cyber operations aspects of its mandate
(a) must not be directed at any portion of the global information infrastructure that is in Canada; and
(b) must not be carried out except under an authorization issued under subsection 30(I) or 31 (I).

Under the *National Defence Act*, the CSE is barred from carrying out activities "directed at" Canadians or persons in Canada in the course of fulfilling the foreign intelligence and cybersecurity aspects of its mandate (s. 273.64(2)(a)). Bill C-59 expands this limitation to include activities conducted in the course of the new active and defensive cyber operations aspects of the mandate (*CSE* Act, s. 23(1)), and also specifies that cyber operations activities "must not be directed at any portion of the global information infrastructure that is in Canada" (s. 23(2)(a)).

The prohibition on directing activities at Canadians is presented—in both legal terms and public debates—as one of the most significant restrictions on the CSE's activities. It is the rationale generally used to justify the CSE's distinctive and expansive powers that

are not granted to any other Canadian agency. Indicative of this rationale is an excerpt from the CSE Commissioner's Annual Report of 2015-16:

> "CSE's activities are distinct from security and criminal intelligence that is collected by other agencies, which is information on activities that could threaten the security of Canada or public safety and is usually acquired from targeting Canadians. CSE activities are specifically prohibited from being directed at Canadians or persons in Canada."[63]

This rationale has been mirrored in many public communications, parliamentary hearings on the CSE, and in the courts.[64] Legally, it rests on the presumption that the CSE's legal obligation to respect the rights of individuals, as captured in Canadian legislation and the *Charter*, applies only weakly (or not at all) with respect to the CSE's impact on rights and interests of non-Canadian persons.

In spite of the central role that this prohibition on directing activities at Canadians plays in justifying the CSE's expansive activities, the limitation is largely a fiction and offers weak protection for privacy rights. The reality of modern networked digital interactions is that it is inevitable that Canadian data will be deeply intermingled with non-Canadian data. As the CSE is granted near limitless authority to capture any and all non-Canadian data as long as it operates within its mandate, it is openly anticipated that large volumes of Canadian data will be collected, used, and analysed as an incidental byproduct of the CSE's activities. This collection of Canadian data is all the more likely to take place when the CSE engages in unselected bulk collection (that is, dragnet surveillance) of information under its foreign intelligence mandate without even attempting to limit its intake on *any* basis, let alone to reduce the impact of these activities on Canadian persons.

Notably, the term "directed at" remains undefined in the *CSE Act*. Section 24(4) also specifically allows for the "incidental" acquisition of information relating to a Canadian or person in Canada in the course of authorized foreign intelligence and cybersecurity activities, including when these activities are subject to an emergency authorization. "Incidentally" is a newly defined term in the proposed *Act*, which refers to situations where "information acquired was not itself deliberately sought and that the information-acquisition activity was not directed at the Canadian or person in Canada" (*CSE Act*, s. 24(5)). In other words, the acquisition or analysis of large volumes of information about Canadians and persons in Canada is not only inevitable in the course of the CSE's general collection activities, but such acquisition is legitimized and codified in the *CSE Act* itself.

The interplay between the terms "directed at" and "incidental" collection has proven

---

[63] Office of the Communications Security Establishment Commissioner. (2015). "2015-16 Annual Report," Government of Canada, https://www.ocsec-bccst.gc.ca/a216/ann-rpt-2015-2016-eng.pdf, p. 7.

[64] See Tamir Israel. (2015). "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation." In Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283.

controversial in the past. While the term "directed at" has received some adjudication, this has mostly arisen in the context of CSIS' foreign-facing activities. For example, in 2012, the Federal Court rejected an interpretation of "directed at" that CSIS and its lawyers put forward in a case involving CSIS activities,[65] and in 2014 the CSE suspended certain unspecified activities of its own in response to that ruling.[66] However, the term has not received comprehensive adjudication in the context of the CSE's unique activities. Moreover, in 2016 the CSE Commissioner issued a public announcement that the CSE had inappropriately disclosed information capable of identifying Canadians to foreign agencies. While the disclosure of identifying material was unintended, it highlights the potential for 'incidentally' collected information to be highly revealing and how, even when prohibited from directing its activities towards Canadians or persons in Canada, the CSE collects significant volumes of such information.[67] Moreover, the CSE is generally known to use metadata capabilities compiled by its Five Eyes partners, who are under no obligation to delete any Canadian metadata they incidentally obtain, and whose databases are known to contain significant volumes of Canadian metadata.[68] Overall, despite the central prohibition on directing its activities at Canadians, the CSE has access to and regularly engages with vast amounts of Canadian data.

Recommendation 18.

Clarify that, under its foreign intelligence mandate, the CSE is prohibited from acquiring, using or analysing information relating to events that occur during an interaction between two or more portions of the global information infrastructure known or likely to be end-point devices located within Canada.

Recommendation 19.

Amend sub-section 23(2) of the proposed *CSE Act* so that the CSE is precluded from directing activities carried out in furtherance to the foreign intelligence aspect of its mandate at any portion of the global information infrastructure that is in Canada.

Far from addressing this long-standing issue, the proposed *CSE Act* compounds the problem by introducing three major exceptions at section 24(1) to the general rule

---

[65] *Reference re sections 16 and 21 of the Canadian Security Intelligence Service Act (CA)*, 2012 FC 1437.

[66] Office of the Communications Security Establishment Commissioner. (2015). "2015-16 Annual Report," Government of Canada, https://www.ocsec-bccst.gc.ca/a216/ann-rpt-2015-2016-eng.pdf, p. 21.

[67] Tamir Israel and Christopher Parsons (2016). "Why We Need to Reevaluate How We Share Intelligence Data With Allies," *Just Security*, https://www.justsecurity.org/29138/reevaluate-share-intelligence-data-allies/.

[68] See coverage of LEVITATION, e.g. in: Amber Hildebrandt, Michael Pereira, Dave Seglins. (2015). "CSE tracks millions of downloads daily: Snowden documents," *CBC News*, http://www.cbc.ca/news/canada/cse-tracks-millions-of-downloads-daily-snowden-documents-1.2930120; Ryan Gallagher, Glenn Greenwald. (2015). "Canada Casts Global Surveillance Dragnet Over File Downloads," *The Intercept,* https://theintercept.com/2015/01/28/canada-cse-levitation-mass-surveillance/; Slides available at Christopher Parsons. "LEVITATION and the FFU Hypothesis," *Canadian SIGINT Summaries*, https://christopher-parsons.com/writings/cse-summaries/#levitation-and.

against targeting Canadians or persons in Canada. In this section, we discuss each in turn.

Publicly Available Information

> **Establishment's activities**
> 24 (1) Despite subsections 23(1) and (2), the Establishment may carry out any of the following activities in furtherance of its mandate:
> (a) acquiring, using, analysing, retaining or disclosing publicly available information;
>
> ~
>
> 2 **publicly available information** means information that has been published or broadcast for public consumption, is accessible to the public on the global information infrastructure or otherwise or is available to the public on request, by subscription or by purchase. (information accessible au public)

Subsection 24(1) of the proposed *CSE Act* authorizes the CSE to acquire, use, analyse, retain or disclose any 'publicly available information' despite the restrictions in subsections 23(1) and (2) which preclude the CSE from directing its activities at Canadian persons or Canadian infrastructure. The *CSE Act* defines "publicly available information" broadly, and includes any information that is published or broadcast for public consumption as well as any information that is accessible to the public on the global information infrastructure ("or otherwise") and even information that is available to the public upon request, by subscription, or by purchase (*CSE Act*, s 2). While subsection 24(2) only permits the CSE to interact with publicly available information when acting within its mandate, it does nothing to ensure such information is only acquired, used, analysed, retained or disclosed under the auspices of a Ministerial authorization or Intelligence Commissioner oversight and control. As such, the protections and limitations accompanying the authorization regime will only apply to "publicly available information" if the CSE is of the view that its practices in relation to such information contravene a Canadian law or the *Charter*.

Further, while measures imposed through section 25 of the *CSE Act* to protect the privacy of Canadians will apply to the use, analysis, retention and disclosure of "publicly available information," no protections are imposed with respect to the "acquisition" or "collection" of such information—a green light for bulk surveillance. It has also been pointed out that "use of the term 'disclose' in the proposed new authorities for the CSE suggests that external entities will rely on CSE-acquired and -analyzed publicly available information and that routinization of disclosure is needed."[69] Indeed, while the CSE is mostly limited from disclosing Canadian identifying data to other agencies (with the exception of some instances under its foreign intelligence mandate, see s. 44), section 24(1) places few limits on its disclosure abilities. This can be problematic because if the CSE discloses assumptions regarding Canadian persons to other agencies, that disclosure can have far-reaching implications, potentially leading to the labeling of

[69] Tanya Dupuis, Cholé Forget, Holly Porteous, and Dominique Valiquet. (2017). Bill C-59: An Act respecting national security matters - Publication No. 32-1-C59-E,", Pre-release Unedited Version, November 9, 2017, *Library of Parliament, p.* 7.

affected individuals as 'suspicious' or worse.[70] The implications associated with such disclosures are not lessened by the fact that the assumptions are premised on "publicly available information." Finally, while many of the CSE's publicly revealed mass surveillance activities have historically appeared to focus on the collection and analysis of metadata, it is worth mentioning that the "publicly available information" exception is inclusive of metadata as well as *content* about and created by Canadians and persons in Canada.

The only limit placed on the CSE's acquisition of publicly available information is that the acquisition must fall within its foreign intelligence, cybersecurity and information assurance, or technical and operational assistance mandates. [71] Together, these mandates are exceedingly broad and offer minimal additional restriction on what the CSE can acquire. Indeed, many of the CSE's foreign intelligence agency peers adopt a "collect it all, figure out what to do with it later'" outlook, further to which almost any form of information is fair game.[72] Moreover, the CSE's ability to collect and use such data in furtherance of its assistance mandate is troubling. When operating under this mandate, the CSE is limited by the lawful authority of the agency it is assisting. However, the CSE might justify the historical acquisition of publicly available data on a basis not available to the agency it is assisting, while justifying the provision of this data to the assisted agency on a basis that is consistent with that agency's lawful authority. The overall effect is that the assisted agency is able to do something it would otherwise be prevented from doing.

The underlying presumption behind exempting all "publicly available information" is the persistent—yet mistaken—view that individuals have no privacy interest in any information that is "public." While intuitive, this presumption is both legally and normatively wrong, and the limitless accumulation of "public" data can have wide-ranging implications for privacy. It is notable in this regard that PIPEDA, the *Privacy Act,* and the *Charter* all provide a measure of protection to personal information even when it is "public" and preclude its collection in some circumstances.[73] In fact, that

---

[70] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, "Report of the Events Relating to Maher Arar", (Ottawa: Public Works and Government Services, 2006); CBC News, "Ottawa Reaches $10M Settlement with Arar", *CBC News*, January 25, 2007, http://www.cbc.ca/news/canada/ottawa-reaches-10m-settlement-with-arar-1.682875.

[71] Note: The CSE is barred from acquiring any information from any activities under its cyber operation mandates. See: paragraph 23(2)(b)(the CSE may only carry out activities under its defensive and active cyber operation mandates further to an authorization) and subsection 35(4)(an active or defensive cyber operations authorization can only be issued if there are reasonable grounds to believe "that no information will be acquired under the authorization").

[72] Ellen Nakashima & Joby Warrick, "For NSA Chief, Terrorist Threat Drives Passion to 'Collect it All', Observers Say," *Washington Post*, 14 July 2013, http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html;

[73] *R v Wise*, [1992] 1 SCR 527; Tamir Israel and Christopher A. Parsons, "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada," *Citizen Lab // CIPPIC*, August 2016, https://ssrn.com/abstract=2901522; *Regulations Specifying Publicly Available Information*, SOR/2001-7, March 22, 2006, https://www.canlii.org/en/ca/laws/regu/sor-2001-7/latest/sor-2001-7.html.

section 25 also requires the Establishment to put measures in place to protect the privacy of Canadians and persons in Canada in the use, analysis, retention and disclosure of "publicly available information" serves as an explicit acknowledgment that the types of "publicly available information" contemplated by the CSE under paragraph 24(1)(a) are likely to interfere with the privacy rights of individuals. Canadian constitutional law has long recognized that without clearly defined safeguards (often including prior judicial oversight), legislation that authorizes intrusions on reasonably held expectations of privacy is inconsistent with the section 8 of the Canadian *Charter*. While the *CSE Act* as currently drafted would require the CSE to rely on a Ministerial authorization (and the authorization's accompanying safeguards) if collecting publicly available information of Canadians in a manner that would otherwise implicate section 8 (*CSE Act*, ss 23(3) and (4)), the framing of paragraph 24(1)(a) implies that it is to be treated as a category of information that can be acquired without limitation. It is our view that the provisions related to "publicly available information" in the *CSE Act* therefore fail to meet the minimum protective threshold required by section 8.

Ultimately the publicly available exception itself does offer some limits on what information is engaged, but these limits are insufficient. To the extent that the term "publicly available information" includes information included in public broadcasts or in documents and publications released for public consumption, subsection 24(1) is less controversial. This would allow the CSE to acquire academic and intelligence reports or information in radio and television broadcasts relating to Canadians, or on broadly available public websites such as Wikipedia, and need not occur in a framework for rigorous privacy protection.

More problematic is the blank check granted to the CSE with respect to other forms of information deemed to be publicly available. Beyond weather reports, newspaper articles, or government publications, the definition is also inclusive of vast amounts of personal and private information in which individuals are likely to have a strong privacy interest. For example, this exception grants license to the CSE to engage in the bulk collection of information published or available through social media accounts like Facebook and Twitter—including facial imagery, posts, photographs, videos, relationships, public location data, behaviour patterns and more. It is far from clear that Canadians and persons in Canada have an informed understanding of the extent to which their digital activities create data which may be "accessible." Some degree of anonymity or practical obscurity is an expected feature of much Internet activity, and that expectation of anonymity is the subject of constitutional protection. Moreover, there are important privacy interests engaged beyond the scope of section 8 protection that need to be expressly protected against the CSE's expansive capacities.

Also problematic is the inherently ambiguous nature of some types of metadata and its transmission in digital contexts. State investigative agencies have, at times, argued that digital identifiers such as IP addresses are "publicly available" because they are transmitted over the Internet and specifically transmitted to service providers to facilitate message delivery.[74] Given this public availability, agencies argue that such

[74] Tamir Israel and Christopher A. Parsons, "Gone Opaque? An Analysis of Hypothetical IMSI Catcher

identifiers are not very private and, thus, do not attract privacy protection, including under section 8 of the *Charter* which protects reasonable expectations of privacy. These arguments are advanced despite the fact that these identifiers are highly sensitive and revealing, meaning they *should* attract privacy protection.[75] In one specific case, the government (in this instance on behalf of CSIS) argued its interception of unique mobile device identifiers was not protected by section 8 of the *Charter*.[76] The identifiers were cast as being 'publicly available' because they were transmitted to cellular towers over the public airwaves to facilitate mobile services.[77] While the Federal Court ruled against CSIS' argument in this instance, neither the Minister nor the Intelligence Commissioner will have a similar opportunity to assess any similar claims the CSE might advance under paragraph 24(1)(a).

There is also a major international market for the sale of personally identifying information by private information and data brokers. This information can include, for example, "credit histories, web browsing history, online purchases, social-media connections, marital status, and a variety of information that enables the construction of detailed personal profiles."[78] It can also increasingly include sophisticated psychological profiles on individuals, or even detailed data on individual's emotional states.[79] The data in these profiles, while falling within the strict definition of 'publicly available information' proposed in Bill C-59 for the *CSE Act*, is nonetheless deeply private. Our courts have held that the simple fact deeply private data is available to some does not mean the state is freely available to acquire this data without limitation, particularly in

---

Overuse in Canada," *Citizen Lab // CIPPIC*, August 2016, https://ssrn.com/abstract=2901522.

[75] Christopher Parsons and Tamir Israel. (2016). "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada," *Citizen Lab // CIPPIC*, https://ssrn.com/abstract=2901522.

[76] The specific identifiers being intercepted included by CSIS in this instance, the International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) numbers, are persistently associated with mobile devices and used by telecommunications service providers to identify specific customers and their handsets as these customers connect to the TSP's mobile network, See: Christopher Parsons and Tamir Israel. (2016). "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada," *Citizen Lab // CIPPIC*, https://ssrn.com/abstract=2901522.

[77] *Re X*, 2017 FC 1047, paras 74 and 158: "Finally, [CSIS] stressed that the IMEI and IMSI identifiers that are captured by CSS equipment is not encrypted, but rather is "in the open."... The Attorney General places significant emphasis upon the fact that the IMSI and IMEI numbers that are obtained through CSS operations are captured from the public airwaves, in a context in which that information is being "offered" to cell towers by the mobile device(s) of the subject of investigation. In this regard, the Attorney General draws a parallel between the IMSI and IMEI identifiers that are " voluntarily" provided to TSPs, and the electricity consumption information that was provided to electricity providers in Plant, above. The Attorney General also draws a parallel to cases such as Patrick, above, where it was found that a reasonable expectation of privacy did not exist in respect of information that had been "abandoned" in the garbage."

[78] Tanya Dupuis, Cholé Forget, Holly Porteous, and Dominique Valiquet. (2017). Bill C-59: An Act respecting national security matters - Publication No. 32-1-C59-E," *Library of Parliament,* p. 8.

[79] Jonathan Albright. (2017). "Cambridge Analytica: the Geotargeting and Emotional Data Mining Scripts," *Medium - TOW Center*, https://medium.com/tow-center/cambridge-analytica-the-geotargeting-and-emotional-data-mining-scripts-bcc3c428d77f.

digital contexts.[80]

A central problem with the "publicly available information" exception (beyond its inherent breadth) is the lack of any obligation to evaluate how the data *became* publicly available or the even the legality of its public availability. Yet it is well documented that many of the companies that accumulate this data for commercial or even non-commercial distribution are not operating in compliance with Canadian data protection laws such as the *Personal Information Protection and Electronic Documents Act* (PIPEDA). In part, this arises from the international nature of these companies, which frequently obtain their data from social media sites and other sources operating primarily under non-Canadian laws.[81]

The provision even appears to permit the CSE to acquire information that, while illegal for members of the public to purchase or otherwise access, is nonetheless made "available" to them. It therefore appears to include information acquired through data breaches, hacks, or intentional leaking. In other contexts, it has been recognized that there are serious ethical and practical issues inherent to the use of information of "illicit origin."[82] For example, following the prominent 2015 security breach of Canadian-based Ashley Madison (described as the "most famous name in infidelity and married dating"), 9.7 gigabytes of highly sensitive digital interactions and account activity from the site were dumped online.[83] It is not clear what would prevent the CSE from incorporating this sensitive data on the extra-marital affairs of Canadians (and others) into its general profiling databases under paragraph 24(1)(a). Disregard for legal provenance may even mean that "publicly available information" as drafted would encompass information disclosed in contravention of federal or provincial privacy legislation, or information which is disclosed in contravention of the terms of a contractual agreement (for example, between an online service provider and a subscriber). Indeed, intelligence agencies such as the CSE have been known to view data known to have been illegally obtained by criminals as a legitimate target for intelligence gathering through interception.[84] Presuming that the CSE would restrain itself in acquiring data *known* to

---

[80] R. v. Duarte, [1990] 1 S.C.R. 30; R. v. Marakah, 2017 SCC 59;R. v. Jones, 2017 SCC 60.

[81] Standing Committee on Access to Information, Privacy and Ethics. (2013). "Privacy And Social Media In The Age Of Big Data," House of Commons, April 2013, 41st Parl, 1st Sess, https://www.ourcommons.ca/DocumentViewer/en/41-1/ETHI/report-5/; Affidavit of Tamir Israel, sworn September 11, 2015, *Douze v Facebook Inc*, Application for Leave to Intervene, SCC File No 36616, https://cippic.ca/en/news/CIPPIC_to_intervene_in_Douez_SCC_online_jurisdiction_appeal.

[82] Thomas, D. R., Pastrana Portillo, S., Hutchings, A., Clayton, R. N., & Beresford, A. R. (2017). Ethical issues in research using datasets of illicit origin. Proceedings of IMC '17 https://doi.org/10.1145/3131365.3131389. For a description of the operation of criminal data markets, see: OECD, Exploring the Economics of Personal Data, DSTI/ICCP/IE/REG(2011)2/FINAL, April 2, 2013, http://dx.doi.org/10.1787/5k486qtxldmq-en, p 27 *et seq*.

[83] Kim Zetter. (2015). "Hackers Finally Post Stolen Ashley Madison data," *Wired*, https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/. It is worth nothing that this kind of information could be used for effects operations or other activities designed to pressure persons to act in a way preferred by the CSE or the Government of Canada.

[84] National Security Agency. (2011 or later). "Fourth Party Opportunities," National Security Agency,

be illegal, and without an obligation to inquire into the source of publicly or commercially available data, leaves how "publicly available information" might be operationalized by the Establishment as deeply problematic. Many commercial markets for personal information are 'grey' markets, where it is by no means clear how the data was acquired (i.e. whether by criminal means or not).

As drafted, there is also a risk that the provision will signal to these private sector actors that the Canadian government is in the market for new kinds of information about Canadians and persons in Canada.[85] These companies—which are already heavily invested in sophisticated methods, sources, and technologies relating to the collection, aggregation and analysis of personal information—could be incentivized to create and collect forms of Canadian data that they would have never previously sought to capture or exploit, but that that could be of particular interest to the CSE. Growing demand from a well-funded agency such as the CSE for commercial available Canadian data could send a signal—including to criminal groups—that it is in the market for such information, however acquired.

Recommendation 40.
Redefine "publicly available information" in the CSE Act so that it is limited in application to commercially available publications and broadcasts.

Recommendation 25.
Amend paragraph 24(1)(a) so that the CSE may only acquire, use, analyze and retain information despite the restrictions in sub-sections 23(1) and (2) if such information falls within a dataset that the Intelligence Commissioner has approved as reasonably necessary to the foreign intelligence or cybersecurity and information assurance aspects of the CSE's mandate.

Recommendation 26.
Amend paragraph 24(1)(a) to remove its application to the "disclosure" of publicly available information or, alternatively, amend section 25 so that it ensures any activities directed at Canadians that would amount to a disclosure of publicly available information may only occur under section 44.

Infrastructure Information

Establishment's activities
24 (1) Despite subsections 23(I) and (2), the Establishment may carry out any of the following activities in furtherance of its mandate:

...

(b) acquiring, using, analysing, retaining or disclosing infrastructure information for the purpose of research and development, for the purpose of testing systems or conducting cybersecurity and

https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0188/45620b38.dir/doc.pdf.

[85] Joshua L. Simmons. (2009). "Buying You: The Government's Use of Fourth-Parties to Launder Data about 'The People'," *Columbia Business Law Review* 2009(3): 950.

information assurance activities on the infrastructure from which the information was acquired;

~

24 (5) **infrastructure information** means information relating to
(a) any functional component, physical or logical, of the global information infrastructure; or
(b) events that occur during the interaction between two or more devices that provide services on a network — not including end-point devices that are linked to individual users — or between an individual and a machine, if the interaction is about only a functional component of the global information infrastructure.

It does not include information that could be linked to an identifiable person.

Paragraph 24(1)(b) of the proposed *CSE Act* permits the CSE to direct its activities at Canadian persons or Canadian infrastructure if acquiring, using, analysing, retaining or disclosing 'infrastructure information' for research and development purposes, to test systems, and to carry out cybersecurity and information assurance activities. Infrastructure information, in turn, is defined at 24(5) as information relating to:

> (a) any functional component, physical or logical, of the global information infrastructure; or
> (b) events that occur during the interaction between two or more devices that provide services on a network — not including end-point devices that are linked
> to individual users — or between an individual and a machine, if the interaction is about only a functional component of the global information infrastructure.
>
> It does not include information that could be linked to an identifiable person.

In relying on this exception to the prohibition on directing its activities at Canadians and Canadian infrastructure, the CSE must remain within its mandate. More specifically, the CSE will be able to acquire information under its foreign intelligence, cybersecurity and information assurance or technical and operational assistance aspects of its mandate when relying on this exception.[86] Worryingly, the CSE will also be able to use Canadian infrastructure information in furtherance of its active and defensive cyber operations mandates or purposes of testing and research and development.

Much as is the case with paragraph 24(1)(a), which permits the CSE to target Canadian persons when interacting with publicly available information, the underlying presumption behind the exception granted in paragraph 24(1)(b) appears to be that 'infrastructure information' is not private in nature, and hence does not require the protections imposed by the *CSE Act* in relation to other types of data. Presumably, the exclusion of information about an identifiable person from the definition of 'infrastructure information' is deemed sufficient to limit the impact Canadian privacy. As such, Canadian 'infrastructure information' is left

[86] As noted with respect to paragraph 24(1)(a) [publicly available information] of the proposed *CSE Act*, paragraph 24(1)(b) will rarely be engaged by the CSE's cyber operation mandates, as these mandates preclude the CSE from acquiring any information. However, in both instances, the CSE may still analyze or use implicated information in real time to carry out cyber operations.

even less protected than 'publicly available information'. Whereas the CSE must undertake measures to protect the privacy of Canadians in 'publicly available information' once obtained (further to section 25) it is under no such obligation with respect to 'infrastructure information'.

However, as is the case with 'publicly available information', the 'infrastructure information' category is defined with sufficient breadth that it can have far-reaching implications for the rights and interests of Canadians. Even information that is not correlated directly to any specific individual, which would implicate the restriction on including information about an identifiable person. However, the CSE may still retain the ability to render this information, once collected, identifiable by other means.

For example, under this exception, the CSE could potentially compile detailed databases of the locations of all WiFi routers in Canada, as well as the IP address and other device or network identifying information associated with these, as that would constitute 'infrastructure information'. Yet, once obtained, this information can be leveraged in highly revealing ways, particularly if the CSE is permitted to leverage such data when relying on its technical and operational assistance mandate to assist domestic law enforcement agencies. For example, one of the CSE's test programs leveraged this type of WiFi location information to predict the movements of specific individuals landing at Canadian airports and was shown sufficiently precise to pinpoint individuals making repeated anonymous phone calls from within a city in Canada.[87] In another example, an NSA program acquired and analyzed detailed 'infrastructure information' about Virtual Private Networks associated with specific institutions (for example, networks associated with some Canadian banking institutions were included) creating a recognizable 'fingerprint' for VPN usage associated with such companies.[88] Once this kind of database is created, it can be used, for example, to track individual representatives of that company in their travels abroad. The CSE (or one of its partners) would only need to search for the 'fingerprint' associated with the VPN in a given locale.

Infrastructure information can also include, for example, include interactions between individuals who are transmitting command and control information to core pieces of the global information infrastructure, including commands to routers or cryptographic certificates needed to secure information as it moves across the Internet. Such information can be used to target and identify Canadian system administrators. Once located (not as individual persons, but as a 'source' of functional information being transmitted to a component of the global information infrastructure. Under 24(1)(b), this information can then be disclosed to the CSE's international partners, it might then be used to target the system administrator for more intrusive operations, potentially undermining the security of the Canadian private network in question.[89] In some instances, infrastructure information

---

[87] Communications Security Establishment. (2012). "IP Profiling Analytics & Mission Impacts," Government of Canada, https://christopher-parsons.com/writings/cse-summaries/#ip-profiling.

[88] See: Colin Freeze and Christine Dobby. (2015). "NSA trying to map Rogers, RBC communications traffic, leak shows," *Globe and Mail*, https://www.theglobeandmail.com/news/national/nsa-trying-to-map-rogers-rbc-communications-traffic-leak-shows/article23491118/.

[89] National Security Agency. (2012). "I hunt sysadmins (part 2)," Government of the United States of

might even be 'analyzed' and 'used' to track individuals moving within Canada if, for example, their mobile devices are configured as 'hot spots' and, hence, do not fall within the exclusion of 'endpoint devices' in paragraph 24(1)(b). Finally, infrastructure information can be used to undermine anonymous online activity within Canada. Specifically, the unmitigated collection and analysis of infrastructure information within Canada can be used to undermine the privacy of Virtual Private Networks and anonymization networks such as Tor by analyzing the time, size and nature of interactions arriving and existing key functional components of the global information infrastructure within Canada.[90]

Infrastructure information can also be used by the CSE and its international partners to identify vulnerabilities or cryptologic weaknesses in order to either exfiltrate information or establish proxies to mask the Establishment's later activities. Under this exception, the CSE may be able to identify *specific* vulnerabilities on *specific* Canadian networks or computing systems for 'testing' and research purposes, effectively bypassing restrictions imposed on the CSE under the cybersecurity aspect of its mandate, where it is limited from accessing Canadian systems without consent of the system owner and without a designation that said system is 'critical' under subsection 22(1). This specific vulnerability information can also be disclosed to the CSE's foreign partners under paragraph 24(1)(b) for the purpose of testing systems or for research and development purposes. Once disclosed, however, there are no limits on how these vulnerabilities will be used by the foreign partners in question. This can have the net effect of undermining security in Canadian networks, rather than enhancing it.

Finally, paragraph 24(1)(b) could be used to conduct disruptive cyber operations on Canadian infrastructure for testing or research and development purposes. While such activities will be conducted under the auspices of a Ministerial authorization (and accompanying safeguards), it can nonetheless be disruptive of Canadian networks as there is no obligation to limit or tailor the scope and scale of testing operations under this exception.[91] Indeed, in the past, the CSE has carried out wide-ranging 'tests' implicating the data of hundreds of thousands of Canadians in a given city.[92] The CSE's cyber operation powers constitute some of its most disruptive capabilities. Allowing the Establishment free reign to unleash these capabilities on Canadian networks—even if just for testing or research purposes—can have serious implications for the integrity of networks and systems in Canada.

America, https://theintercept.com/document/2014/03/20/hunt-sys-admins/.

[90] National Security Agency. (2012 or later). "Peeling Back the Layers of TOR with EGOTISTICALGIRAFFE," Government of the United States of America, https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH32d5.dir/doc.pdf.

[91] Communications Security Establishment. (2011). "CASCADE: Joint Cyber Sensor Architecture," Government of Canada, https://christopher-parsons.com/writings/cse-summaries/#cse-cascade-joint.

[92] Communications Security Establishment. (2012). "IP Profiling Analytics & Mission Impacts," Government of Canada, https://christopher-parsons.com/writings/cse-summaries/#ip-profiling

Recommendation 24.
Amend paragraph 24(1)(b) so that the activities it authorizes may only occur on electronic information and information infrastructures described in 18(a) of the *CSE Act*, and only in furtherance of its cybersecurity and information assurance mandate.

Testing

Establishment's activities
24 (1) Despite subsections 23(1) and (2), the Establishment may carry out any of the following activities in furtherance of its mandate:

...

(c) testing or evaluating products, software and systems, including testing or evaluating them for vulnerabilities.

Paragraph 23(1)(c) of the proposed *CSE Act* would authorize the CSE to test or evaluate "products, software and systems, including testing or evaluating them for vulnerabilities" even when such activities are directed at Canadian persons or infrastructure in Canada. While this exception does not explicitly authorize the CSE to acquire information (including personal or other information) from the products, software, and systems it tests or evaluates, such acquisition is not expressly precluded. Activities undertaken must be to further is five-part mandate and in light of the nature of the activities in question all five aspects of the CSE's mandate are likely to be engaged. While at face value this exception appears designed to facilitate security of networks and devices, its expansive breadth may also operate to undermine the integrity of communications networks and computing systems.

Paragraph 24(1)(c) introduces many new and undefined terms. At its most limited interpretation, this exception would permit the CSE to interact with a narrow set of software and products to identify security vulnerabilities for the purpose of fixing these devices. This most innocuous interpretation, however, remains concerning for its inclusion of 'systems', a term that, in the context of paragraph 24(1)(b), is clearly refers to networks and systems within the global information infrastructure, i.e. the Internet. This means that the CSE would be empowered to probe Canadian networks and infrastructure remotely and surreptitiously. In effect, this bypasses the requirement for the CSE to obtain consent from a Canadian system operator prior to accessing its network and the limitation on CSE access to Canadian networks not deemed 'critical' under subsection 22(1). However, a plausible reading of 'systems' can be stretched further to include internal networks of Canadian individuals or entities.

When carrying out these probes of either software, products, or systems and doing so remotely or in person, the CSE may engage any aspect of its mandate. This includes the cyber operations aspects of its mandate, which are heavily reliant on the exploitation of network vulnerabilities, and the foreign intelligence aspect of its mandate. As a result, the CSE is not only empowered to avoid disclosure of the vulnerabilities it discovers so

that it might later exploit these[93] but may specifically target a Canadian individual or infrastructure in Canada to test and probe for the express purpose of identifying a vulnerability *in order* to exploit them. This is in spite of the general prohibition imposed on the CSE that limits it from engaging in active cyber operations directed at Canadian infrastructure or persons in Canada. For example, the CSE could target laptops or mobile devices active on airport networks to discover vulnerabilities to be exploited once the individual visitors to Canada have returned home. Further, under the CSE's foreign intelligence mandate, the CSE could rely on 24(1)(c) to intentionally intercept network equipment while it is being shipped through Canada to foreign state for the explicit purpose of evaluating that device for vulnerabilities. If discovered, the CSE would be able to immediately exploit these vulnerabilities as it is not precluded from targeting infrastructure in Canada under its foreign intelligence mandate. In theory, in testing a system in furtherance of the active cyber operations aspect of its network, the CSE could actively disrupt Canadian infrastructure to identify its level of susceptibility and resilience. Even such conduct would fall within the scope of this expansive 'testing' exception as currently framed.

The scope of software, products, and systems that the CSE may test under this exception appears to be intentionally broad and near unlimited. These can include: 'smart' vehicles; anything within the growing Internet of Things; the networked lock on someone's front door; medical sensors and equipment -- including, for example, a networked pacemaker; military or defense systems; internet routers; smart grid systems; or electoral system software; just to start. It is likely to most frequently include the full range of laptops, mobile devices, home computing devices, and network devices. Given the presence of software (or digital code) in almost all facets of contemporary products and services, this section would permit the CSE to engage in testing or evaluation of almost all products sold today and all services which contain a digital element. As more products are digitized and adapted to send and receive information from the Internet, this the specific failure to define 'software' would effectively authorize the CSE to examine any and all products and services, and not impose a corresponding onus on the Establishment to subsequently try and ameliorate the vulnerabilities that are discovered. Similar problems exist in relation to 'product' -- it is unclear what would not constitute a product -- and 'system' which currently could be broadly taken to refer to any collection of things which work together.

What is included in 'testing and evaluation' remains equally open ended. Testing and

---

[93] When the CSE and its partners discovered a flaw in how UC Browser, a widely used Chinese web browser, they subsequently developed a way to collect information which leaked from the browser and which could itself be used for testing and research activities. See: Communications Security Establishment, Defense Signals Directorate, Government Communications Headquarters, Government Communications Security Bureau, and National Security Agency. (2012 or later). "Synergising Network Analysis Tradecraft: Network Tradecraft Advancement Team (NTAT)," https://christopher-parsons.com/writings/cse-summaries/#cse-synergising-network; Jakub Dalek; Katie Kleemola; Adam Senft; Christopher Parsons; Andrew Hilts; Sarah McKune; Jason Q. Ng, Masashi Crete-Nishihata, John Scott-Railton; and Ron Deibert. (2015). "A Chatty Squirrel: Privacy and Security Issues with UC Browser," *Citizen Lab*, https://citizenlab.org/2015/05/a-chatty-squirrel-privacy-and-security-issues-with-uc-browser/.

evaluation may involve discovering flaws in how software establishes cryptographic communications or flaws in software design that enable the CSE to disable the associated hardware or otherwise interrupt the software's normal functioning. Tests and evaluations may also involve actively disrupting products, software, or systems in Canada for the purpose of identifying their level of susceptibility and resilience in support of an active cyber operation the CSE plans to conduct outside of Canada. Testing and evaluation is not temporally restricted. The CSE could, on its own initiative and without consent from the owner of the system being targeted in Canada, probe the system repeatedly (i.e. following every system upgrade). It is also possible that in the case of a product or piece of software or system that the CSE has previously tested and discovered a vulnerability, the Establishment could 'test' whether the same vulnerability exists in the same or similar products, software, or systems outside of the Establishment's immediate control. In effect, the non-definition of what testing or evaluating entail leave the CSE unrestricted in the kinds of activities it might undertake.

As we discuss in section II, iii of this document, there is a tension inherent to the CSE's mandate which requires the Establishment to simultaneously improve Canada's cybersecurity while exploiting vulnerabilities in systems to facilitate surveillance as well as engaging in cyber operations against others. The exception encoded in paragraph 24(1)(c) allows the CSE to capitalize on this tension in deeply problematic ways that can have far-reaching implications for the integrity of communications networks and computing systems, and for the rights and interests of Canadians.

Recommendation 27.
Amend paragraph 21(4)(c) to, at minimum, include the full and informed consent of any and all individuals whose software, products or systems are being tested or evaluated.

Recommendation 28.
Amend paragraph 21(4)(c) to, at minimum, limit its use to cybersecurity objectives.

Generally Insufficient Privacy Protections in Section 25

Measures to protect privacy
25 The Establishment must ensure that measures are in place to protect the privacy of Canadians and of persons in Canada in the use, analysis, retention and disclosure of
(a) information related to them acquired in the course of the furtherance of the foreign intelligence and cybersecurity and information assurance aspects of the Establishment's mandate; or
(b) publicly available information related to them acquired under paragraph 24(1)(a).

In carrying out the foreign intelligence and cybersecurity aspects of its mandate, the CSE is currently required to take measures to protect the privacy of Canadians "in the use and retention" of intercepted information (s. 274.64(2)(a)). The proposed *CSE Act* expands this protection in two important ways at section 25. First, it would also encompass the privacy of "persons in Canada" in addition to Canadians. Second, it would specify that measures must be taken to protect privacy "in the use, *analysis*,

retention, and *disclosure*" of information acquired in the furtherance of the foreign intelligence or cybersecurity aspects of the mandate (*CSE Act,* s. 25(a)). Notably—and by design, given the Establishment's dragnet surveillance activities—these requirements do not extend to either the *acquisition* or *collection* of information.

These measures are to be accounted for at the authorization stage of foreign intelligence and cybersecurity activities (*CSE Act*, 35(2)(c), 35(3)(d)). However, these provisions are drafted in a manner that could incentivize willful blindness as to whether or not information acquired by the CSE relates to Canadians and persons in Canada. The provisions which impose privacy measures on foreign intelligence and cybersecurity and information assurance authorizations limit the protection only to information that "is identified as relating to a Canadian or a person in Canada" (see s. 35(2)(c), 35(3)(d)). In the absence of affirmative identification by the Establishment, privacy protections would seemingly not be required. This language contrasts with broader language elsewhere in the Bill which sets out circumstances when "information that could be used to identify a Canadian or a person in Canada" may be disclosed by the Establishment.

The privacy measures referred to in section 25 also do not apply to information acquired in the course of the assistance mandate (as this would fall under the legal framework of the requesting agency, such as CSIS, the RCMP, or the Canadian Forces), nor information acquired in the course of either cyber operations aspects of the mandate (*CSE Act*, s. 25). Section 25 appears not to apply to the active or defensive cyber operations activities because one of the conditions for their authorization is that the Minister must have reasonable grounds to believe "that no information will be acquired under the authorization except in accordance with an authorization issued under subsection 27(1) or 28(1) or (2) or 41(1)" (*CSE Act*, s. 35(4)). In other words, where information is acquired in the course of those activities, a separate authorization is required, and the privacy measures will (theoretically) be accounted for through that framework. However, even this system fails to address broader concerns about the impacts of the CSE's activities on the privacy of Canadians and persons in Canada (as well as the privacy rights of individuals worldwide more generally). As described elsewhere in this report, the CSE's operations have the potential to impact the security of the global information infrastructure in ways that dramatically jeopardize the privacy rights, freedom of expression, and security of individuals both in Canada and abroad. Section 25 is not drafted in a manner which would in any way limit the CSE from interfering with or undermining secure communications technology, encryption software, or anonymity tools used by the general public—despite the fact that doing so *inherently* threatens the privacy rights of users.

As to what the "measures" contemplated in section 25 might entail, the answer is left unclear. The proposed *CSE Act* would leave these measures entirely to regulation set by the Governor-in-Council rather than subject to rigorous public debate, democratic scrutiny, or oversight by the Privacy Commissioner (*CSE Act*, s 61(b)). As a result, there is a risk that these measures will ultimately remain vague, superficial, and deferential to the internal and secretive decisions of the Establishment itself. We would also note that there is another major problem with section 61 of the *CSE Act*, which is that it allows the Governor-in-Council to amend "the definition of any term defined in section 2 or

subsection 24(5) or 45(3) to respond, directly or indirectly, to any technological change" (s. 61(c)). In other words, this provision would allow the Executive to completely redefine essential terms of the *CSE Act* in a manner that could profoundly redesign the legal framework governing the CSE (and corresponding human rights implications) while bypassing public debate or accountability to Parliament. It is also not clear whether it is constitutionally sound for Parliament to delegate its authority to amend a statute to the Governor-in-Council.

Recommendation 39.
Amend the *CSE Act* to remove section 61(c).

Finally, the proposed CSE Act does not account in any manner for the privacy rights of foreigners, despite the fact that this is a major outstanding issue in the area of international human rights law. Questions have also been raised about whether the *Personal Information Protection and Electronic Documents Act* could lose its "adequacy" standing under the European Union's General Data Protection Regulation (GDPR).

Recommendation 42.
Ensure that the complete set of measures referred to in section 25 and adopted in regulation under section 61(b) to protect the privacy of Canadians and persons in Canada are made available to the public for comment and analysis.

Recommendation 43.
Require the Office of the Privacy Commissioner of Canada to annually evaluate the protections for Canadians and persons in Canada under section 25, and to be able to provide recommendations to the CSE and the Intelligence Commissioner.

iv. Purpose and Tension Between Aspects of the Mandate

The proposed *CSE Act* raises fundamental issues about what it means to engage in "cybersecurity" on behalf of a state and about the broader purpose of agencies like the CSE in the 21st century. As Ron Deibert has written:

> "What do we mean when we say "cyber security?" What is it, exactly, that we are securing? And for whom? Are we securing the Internet as a whole — that vast global information infrastructure that envelops the planet, from the code to satellites, the handheld devices, and everything in between?
>
> Or, instead, do we mean 'we protect our nation's cyberspace first and others second, if at all'? Do we regard other nations' networks as fair game to be "exploited" in order to gain competitive advantage?
>
> The tension between these points of view is not unique to cyber security, but reflects a deeper tension at the heart of global politics today: between a slowly emerging sense of

> global responsibility and citizenship on the one hand, and the old Westphalian nation-state system on the other."[94]

This unresolved tension is at the heart of the legal framework governing the CSE in Bill C-59, and the proposed *CSE Act* is an explicit reflection of that latter, older worldview. Yet in a global technological ecosystem which is highly interdependent, immeasurably complex, and upon which the human rights of individuals worldwide depend, such a position is not only archaic but is actively counterproductive to Canada's broader security interests.

National Borders as Inadequate Boundaries

Paragraph 23(2)(a) of the *CSE Act* indicates that activities carried out by the Establishment in support of the defensive or active cyber operations aspects of its mandate are not to be "directed at any portion of the global information infrastructure that is in Canada." The lack of protection in this provision of the *CSE Act* for foreign individuals, their rights or their infrastructure—alongside the view that the security interests of Canadians and persons in Canada are neatly confined to our physical borders—is indicative of that "Westphalian" worldview.

This territorial limitation does help to constrain the impact and scope of the CSE's cyber operations activities. However, whether or not a portion of the global information infrastructure is physically "in" Canada is not, in itself, determinative of the degree to which access or interference may impact the security, privacy, or other Charter-protected rights of Canadians and persons in Canada. For example, efforts to weaken, circumvent or otherwise detrimentally affect aspects of the global information infrastructure used by Canadians to facilitate encrypted or anonymous communications which are not physically "in" Canada may have significant collateral impacts on their human rights and on global security more broadly. Interference with, or attacks on, parts of the Tor network located outside of Canada would be just one example of such a situation (notably, Tor is responsible for protecting the anonymity of those working for military and intelligence agencies just as it does for human rights defenders, researchers and journalists worldwide).[95] In some cases Canadian *Charter* rights may also be impacted—including but not limited to those guaranteed under section 2(b) (which protects freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication), section 7 (the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice), and section 8 (the right to be secure against unreasonable search and seizure).

The limitation in s. 23(2)(a) provides only weak protections to the rights of Canadians

---

[94] Ron Deibert (2014). "The Cyber Security Syndrome," *OpenCanada*, https://www.opencanada.org/features/the-cyber-security-syndrome/.

[95] The Tor Project is free software and an open network that helps users defend against traffic analysis, preserve online anonymity, and circumvent Internet censorship. Tor is a distributed, anonymous network, which routes data through "nodes" that are located in many different countries. See: The Tor Project, at: https://www.torproject.org/.

and persons in Canada. Simultaneously, it ignores the rights and interests of individuals—including Canadians—abroad and may create the conditions for the CSE to run afoul of Canada's international human rights obligations in the course of its active and defensive cyber operations activities. Coupled with the narrow and poorly defined limitations on the exercise of these powers in section 33 of the *CSE Act* (as described above), there is a strong likelihood that the CSE will engage in activities that ultimately jeopardize Canada's international interests, threaten human rights, and compromise the security of the global information infrastructure.

No activities — global information infrastructure in Canada or without authorization

23(2) Activities carried out by the Establishment in furtherance of the defensive cyber operations or active cyber operations aspects of its mandate

(a) must not be directed at any portion of the global information infrastructure that is in Canada; ...

CSE vs CSE

There is a deep tension between several aspects of the CSE's mandate, which requires that the Establishment simultaneously improve Canada's cybersecurity while exploiting vulnerabilities in systems to facilitate surveillance, and to defend information and infrastructure while engaging in offensive operations against others. As Deibert writes:

> "The same agencies one might expect and hope to be at the forefront of patching software bugs, are simultaneously coveting, stockpiling, and even purchasing them...as weapons. Agencies like the NSA are tasked with defending critical infrastructures on the one hand, while fueling a multi-million dollar industry of products and services to exploit them on the other. Protecting the integrity of communications systems is a mission imperative, but so is building "back doors" — a kind of insecurity-by-design — programs designed to proactively weaken information security are justified on the basis of strengthening national security."[96]

For example, the CSE contributes its expertise in international cryptographic standards bodies in the course of providing cybersecurity and information assurance advice, guidance, and services. With a host of other international experts, the CSE is expected to identify deficiencies in proposed standards, suggest improvements, and play a significant role in setting standards ultimately adopted by the Government of Canada as well as private-sector infrastructure owners and operators.

Yet in the past, the CSE has collaborated with the National Security Agency to knowingly propagate a pseudorandom number generator (PRNG) called Dual EC DRBG at international forums as well as within Canada—despite the fact that it was known to be deficient.[97] By propagating this standard, the CSE and its Five Eyes allies were able to subtly interfere with the security of communications which used this standard, as were other unintended parties

[96] Ron Deibert (2014). "The Cyber Security Syndrome," *OpenCanada*, https://www.opencanada.org/features/the-cyber-security-syndrome/.

[97] Christopher Parsons and Tamir Israel. (2015). "Canada's Quiet History Of Weakening Communications Encryption," *Citizen Lab*, https://citizenlab.ca/2015/08/canadas-quiet-history-of-weakening-communications-encryption/.

who identified the vulnerability. Researchers raised issues about flaws in the standard before the interference was confirmed in the Snowden revelations, but that did not stop Dual EC DRBG from being adopted, standardized, and introduced into commercial tools over the course of years.[98]

This example underscores the tensions that arise between the cybersecurity and the foreign intelligence (or, potentially, the active and defensive cyber operations) aspects of the CSE's mandate. The fact that CSE was complicit in deliberately weakening tools that it subsequently recommended the Government of Canada and private industry adopt raises fundamental questions about when, and whether, the advice provided is in the service of a cybersecurity or foreign intelligence objective, and how the Establishment reconciles tensions between the two. Canada's intelligence allies have even more problematic track record of interfering with security technologies: programs like the NSA's Bullrun and the GCHQ's Edgehill[99] have been explicitly designed to interfere with, weaken, and undermine the protections afforded by encryption tools.

This tension is likely exacerbated by the newly introduced defensive and active cyber operations aspects of the mandate. The defensive cyber operations aspect of the CSE's mandate would have it test and evaluate "products, software and systems, including testing or evaluating them for vulnerabilities" (*CSE Act,* s. 24(1)(c)), but there is no requirement to publicly disclose the results of such tests. The broad range of activities envisioned as part of the active cyber operations aspect of the mandate will not only involve taking advantage of such vulnerabilities, but will allow the Establishment to take offensive measures in a manner that may ultimately escalate tensions, provoke retaliation, or otherwise compromise Canada's security and public safety interests.

Revelations that intelligence agencies have historically worked to interfere with the security of communications tools have led to great skepticism in situations where these same agencies have sought to provide advice to international standards bodies and private sector actors alike.[100] This mistrust weakens the CSE's credibility in its efforts to ensure that the best and most secure standards and practices are adopted in Canada and internationally. Secret collusion between intelligence agencies and private sector actors also diminish public and consumer trust in commercially available technologies for communications and storage. As an example, the increasing perception that national-level computer emergency response teams (CERTs) are acting as "instruments of state competition" limits information sharing, compromises rapid threat response, and undercuts coordination efforts by institutions meant

---

[98] Matthew Green. (2015). "Hopefully the last post I'll ever write on Dual EC DRBG," *A Few Thoughts on Cryptographic Engineering*, https://blog.cryptographyengineering.com/2015/01/14/hopefully-last-post-ill-ever-write-on/.

[99] See e.g., James Ball, Julian Borger and Glenn Greenwald. (2013). "Revealed: how US and UK spy agencies defeat internet privacy and security," *The Guardian*, https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; Jeff Larson. (2013). "Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security," *ProPublica*, https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

[100] Joseph Menn. (2017). "Distrustful U.S. allies force spy agency to back down in encryption fight," *Reuters*, http://mobile.reuters.com/article/amp/idUSKCN1BW0GV.

to be apolitical.[101]

Elsewhere, Citizen Lab researchers have argued that these activities not only interfere with the security of the global information infrastructure directly, but also have significant downstream impacts. Legislation such as C-59 which provides an enabling framework for mass surveillance and offensive, state-sponsored hacking sets a problematic example for the international community by encouraging a "race to the bottom" for global security. Such a race has troubling impacts for those living in countries unconstrained by the rule of law or unsheltered by effective human rights protections. The trend toward the kinds of activities captured by section 32 of the proposed *CSE Act*—such as disruption, hacking, interference, and illicit data modification—will serve to encourage and legitimize the international market for spyware and hacking tools which invariably end up in the hands of abusive state actors, criminal organizations, and other malicious actors despite being marketed toward intelligence agencies and law enforcement agencies.[102]

Minimizing the tension between the CSE as a guarantor of security and offensive actor in cyberspace may entail either moving the CSE's cybersecurity and information assurance mandate to another organization—effectively separating the CSE's security and intelligence operations—or amending proposed legislation to limit the Establishment's ability to work at cross-purposes. But even such a modification will not fully resolve the tension that the Government of Canada is involved in both offensive and defensive operations, nor would it serve to delegitimize the growing market of spyware and hacking tools that are routinely used to target journalists, legislators, human rights defenders, or lawyers.

Recommendation 35.
Require Parliament to undertake a study regarding the benefits, challenges, and feasibility of separating the CSE into two distinct agencies, one of which is tasked exclusively with cybersecurity, information assurance and defence; the other which is exclusively responsible for foreign intelligence and any cyber operations activities.

v. Absence of a Formal Vulnerabilities Equities Process

As part of its cybersecurity and information assurance mandate, the CSE is tasked with identifying threats to electronic information and information infrastructure controlled by the Government of Canada as well as equivalent threats to systems of importance to the Government of Canada (*NDA*, s. 273.64 (1)(b), *CSE Act*, s. 18). In part, this means that when the CSE identifies security vulnerabilities or weaknesses in aspects of the global information infrastructure, it is expected to provide advice, guidance, or services to assist the Government of Canada or parties operating systems of importance to the Government of Canada on how

[101] See reference to comments by Yuri Ito at the 2013 Bali Internet Governance Forum in: Ron Deibert (2014). "The Cyber Security Syndrome," *OpenCanada,* https://www.opencanada.org/features/the-cyber-security-syndrome/.

[102] Sarah McKune and Ron Deibert. (2017). "Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking," *Citizen Lab,* https://citizenlab.ca/2017/03/whos-watching-little-brother-checklist-accountability-industry-behind-government-hacking/.

to mitigate or respond to those risks. The CSE is also able to disclose threats and vulnerabilities to the manufacturers or developers responsible for producing or maintaining the means by which electronic information is encoded or information infrastructure is secured. In the absence of a clear framework for how, when and whether vulnerabilities are disclosed, there is no way for industry or the public to understand under what conditions the CSE would decide to keep such discoveries secret for its own purposes. For example, a security vulnerability which is not known to the public or the developers and which allows the CSE to circumvent protection provided by encryption could be exploited to facilitate the collection of foreign intelligence. However, a decision to retain—and not to disclose—these kinds of vulnerabilities also raises the prospect that adversaries, including both foreign states and criminal parties, will exploit them too.

The United States Government has established a Vulnerabilities Equities Process (VEP) that is "charged with balancing whether to disclose vulnerability information to the vendor with expectation that they will patch the vulnerability, or temporarily restrict knowledge of the vulnerability so that it can be used for national security or law enforcement purposes."[103] Multiple US federal government agencies are involved in the process of evaluating whether a vulnerability should be retained and used, or disclosed and closed by the responsible vendors or developers. The American VEP system is not required in legislation, but has emerged as part of transparency efforts in response to concerns that the NSA has unduly stockpiled vulnerabilities in the past, and that such vulnerabilities can and do wreak havoc when and if foreign actors gain access to and disseminate them.[104]

The CSE currently operates a VEP program but the details of its operation remain secret.[105] The framework that governs who evaluates whether the CSE will retain or disclose vulnerabilities, the parties who are to be involved in the VEP process, and the types of vulnerabilities or technical deficiencies that will prompt a VEP evaluation to take place are entirely outside of public view. As a result, it is impossible for industry actors or the public to understand the nature of the calculations being made by the CSE when it discloses a vulnerability (or fails to do so), or to hold the Establishment accountable if policies which inappropriately restrict responsible disclosure fail to serve the public interest. To retain the public's trust that the CSE is actively involved in providing fulsome advice, guidance, and services whilst fulfilling its cybersecurity and information assurance mandate, Bill C-59—or some other form of clear, public, detailed, and up-to-date policy document—should clarify this system. Furthermore, the CSE should be required to report outcomes under this

---

[103] Rob Joyce. (2017). "Improving and Making the Vulnerability Equities Process Transparent is the Right Thing to Do," The White House, https://www.whitehouse.gov/blog/2017/11/15/improving-and-making-vulnerability-equities-process-transparent-right-thing-do.

[104] Jason Healey. (2016). "The U.S. Government and Zero-Day Vulnerabilities," *Journal of International Affairs* (November 2016); Brad Smith. (2017). "The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack," *Microsoft*, https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/.

[105] Matt Braga. (2017). "When do Canadian spies disclose the software flaws they find? There's a policy, but few details," *CBC News*, http://www.cbc.ca/news/technology/canada-cse-spies-zero-day-software-vulnerabilities-1.4276007.

framework on a regular basis, including the rate at which vulnerabilities of various classes are withheld and disclosed, and these reports—to the extent possible—should not only be provided to NSIRA, but also to the general public.

Recommendation 49.
Require the establishment of a Vulnerabilities Equities Program for the CSE that includes a requirement that evaluation criteria for disclosure be made completely public.

Recommendation 50.
Require that VEP criteria should specify the need to prioritize the public interest and public safety over the CSE's intelligence-gathering or disruption-related operational objectives. Enable the Intelligence Commissioner and/or independent non-governmental experts to advance these public interest concerns.

Recommendation 51.
Require public reporting on the Vulnerabilities Equities Program, including disclosure with regard to the frequency at which the CSE discloses vulnerabilities to Computer Emergency Response Teams, public institutions, private organizations, and other entities.

vi. Arrangements with Foreign and International Bodies

In order to further its mandate, the CSE has historically entered into various "arrangements" with entities that have powers and duties similar to its own, including both domestic entities and foreign intelligence agencies alike. The proposed *CSE Act* would acknowledge, and provide a legal framework for, these kinds of arrangements, specifying that they may include information sharing and other forms of cooperation (*CSE Act*, s. 55). Under the proposed model, arrangements with "institutions of foreign states or that are international organizations of states or institutions of those organizations" must be approved by the Minister, who is required to consult the Minister of Foreign Affairs prior to approval (*CSE Act,* s. 55(2)). The Minister of Foreign Affairs does not, however, have to consent to the arrangement, nor do arrangements require any form of oversight or approval by the Intelligence Commissioner.

Arrangements can be made with respect to any aspect of the Establishment's mandate. In cases where either legislation or the scope of authorizations approved by the Intelligence Commissioner impose limits on the CSE's activities or the information it can collect, arrangements with foreign agencies could nonetheless create an avenue for the Establishment to circumvent those barriers. In collaborating with foreign parties the CSE may be able to gain access to information or networks that it would otherwise lack the in-house technical capabilities to acquire. Arrangements could also allow the CSE to develop interoperable and interconnected systems—such as networks of sensors—with foreign entities, which could then be leveraged by foreign actors to conduct activities that violate international human rights norms, or which would be unlawful for the CSE to undertake itself. Information sharing arrangements with foreign entities are also potentially a cause for concern in that they may allow the CSE to acquire, collect, use, or analyze information

that the Establishment, if acting on its own, would have never been allowed to lawfully acquire—including information acquired in a manner that would not only raise legal issues, but international human rights concerns as well. Furthermore, while the CSE may use information sharing arrangements to prohibit foreign partners from sharing information that was obtained by foreign surveillance activities directed at Canadians and persons in Canada, information obtained incidentally about Canadians and persons in Canada likely remains an issue.

The CSE may collect publicly available information about Canadians and persons in Canada subject to paragraph 24(1)(a) of the proposed *CSE Act,* in addition to the Establishment's bulk collection activities, which are also likely to capture information about Canadians or persons in Canada. The *CSE Act* includes a requirement that the CSE establish measures to protect the privacy of Canadians or persons in Canada whose information is collected as part of the CSE's foreign intelligence and cybersecurity aspects of the mandate or which is collected subject to the "publicly available information" exception at section 24(1)(a). The framework for arrangements should also be read alongside the provisions related to disclosure of information at sections 44 to 47 and the limitations on directing activities at Canadians included in section 23 of the proposed *CSE Act*. Section 44 authorizes the CSE to disclose Canadian identifying information used, analyzed or retained through a foreign intelligence authorization to persons designated under section 47 if the CSE deems disclosure to be essential to international affairs, defence, security or cybersecurity. Section 45 authorizes the CSE to disclose information that has been acquired, used or analysed in the course of activities carried out under the cybersecurity and information assurance aspect of its mandate, with the inclusion of intercepted private communications and the existence thereof expressly permitted (s. 45(2)) if the CSE finds it is reasonably necessary to do so to achieve the objectives of its cybersecurity and information assurance mandate. However, beyond the limitations imposed by that section, it appears that any information under the control or in the possession of the CSE could be subject to an information sharing arrangement under section 55. It should be noted that historically, measures intended to limit the disclosure of Canadian information to third parties have not always been effective.[106]

Recommendation 44.

Amend section 55 of the *CSE Act* to require that the Minister seek the approval of the Intelligence Commissioner for all arrangements with institutions of foreign states or that are international organizations of states or institutions of those organizations.

Recommendation 45.

Amend section 55 such that the CSE is prohibited from knowingly entering into arrangements with institutions of foreign states or other entities suspected of engaging in torture.

[106] Office of the Communications Security Establishment Commissioner. (2015). *2014-2015 Annual Report*. Government of Canada, https://www.ocsec-bccst.gc.ca/s21/s20/eng/2014-2015-annual-report; see also: Tamir Israel and Christopher Parsons. (2016). "Why We Need to Reevaluate How We Share Intelligence Data With Allies," *Just Security*, https://www.justsecurity.org/29138/reevaluate-share-intelligence-data-allies/.

Recommendation 46.

Amend section 55 of the CSE Act to require that the Commissioner, when approving an arrangement, ensures that all activities to be undertaken in the the furtherance of the CSE's mandate pursuant to the arrangement (including for the purposes of information sharing or other forms of cooperation) are lawful, constitutional, reasonably necessary, and proportional.

Recommendation 47.

Amend section 55 of the *CSE Act* to include a framework for review and renewal of all arrangements entered into by the CSE on a periodic basis. In the case of arrangements with institutions of foreign states or that are international organizations of states or institutions of those organizations, the renewal process should include the consent of the Minister of Foreign Affairs and the approval of the Intelligence Commissioner.

Section III - Recommendations

Review, Oversight, Control and Accountability

1. Amend section 9 of the *National Security and Intelligence Review Agency Act* to clarify that the NSIRA is entitled to access documents in the possession or under the control of any department, including all documents originating from foreign governments, their respective intelligence agencies, and international bodies—despite any limitation imposed by those foreign bodies or by "originator control."
2. Amend section 48 of the *National Security and Intelligence Review Agency Act* to prohibit the secretariat from engaging in direct hiring from intelligence and national security agencies, and to impose a reasonable time limitation for prospective secretariat employees who have been employed by those agencies in the past.
3. Amend section 4(3) of the *Intelligence Commissioner Act* to require, or at least provide the option for, a full-time Intelligence Commissioner.
4. Amend section 4(4) of the *Intelligence Commissioner Act* so that remuneration of the Intelligence Commissioner is set in relation to the salary of a judge of the Federal Court under paragraph 10(d) of the *Judges Act* (if the Commissioner remains part-time, this amount can be pro-rated).
5. Amend the *Intelligence Commissioner Act* and the *CSE Act* so that the Intelligence Commissioner has the ability to impose conditions on approved authorizations; the obligation to rule on the legality, constitutionality, reasonable necessity, and proportionality of any activity undertaken by the CSE; and order-making powers to prevent the CSE from carrying out any activities that are either illegal, unconstitutional, disproportionate or not reasonably necessary.
6. Amend section 21(a) of the *Intelligence Commissioner Act* to require the Commissioner to issue written reasons when approving the authorization, amendment or determination mentioned in that section.
7. Amend the *Intelligence Commissioner Act* to grant the Intelligence Commissioner all powers granted to commissioners under Part II of the *Inquiries Act*, as subsection 273.63(4) of the *NDA* grants the current CSE Commissioner.
8. Create a mechanism for challenging or appealing decisions rendered by the Intelligence Commissioner.
9. Require both approval of the Intelligence Commissioner and consent of the Minister of Foreign Affairs for all active and defensive cyber authorizations under sections 30 and 31.
10. Require both approval of the Intelligence Commissioner and authorization by the Minister for activities undertaken further to the technical and operational assistance aspect of the CSE's mandate.
11. Amend the *CSE Act* to require that any emergency authorization under section 41 be reviewed *ex post* by the Intelligence Commissioner.
12. Require that both authorizations made by the Minister and decisions made by the Intelligence Commissioner be made public to the greatest extent possible.
13. Introduce some form of security-cleared *amicus* or other manner of adversarial input

in the authorization process for activities under the foreign intelligence, cybersecurity, and cyber operations aspects of the mandate.

14. Require the CSE to proactively provide the NSIRA with any internal legal interpretations it adopts that are novel or which have been subject to substantial change.

Scope of Mandate and Powers

15. Redefine "foreign intelligence" so that it retains within its scope information and intelligence regarding the capabilities, intentions or activities of foreign terrorist groups, foreign states and their agents as these relate to international affairs, defence or security, but limits inclusion of information or intelligence relating to the capabilities, intentions or activities of foreign individuals to situations that pose a threat to the security of Canada, as defined in the *CSIS Act*.
16. Amend sub-sections 23(3) and (4) so that activities carried out in furtherance of the foreign intelligence and cybersecurity and information assurance aspects of the CSE's mandate may only incidentally affect or relate to a Canadian or a person in Canada if carried out further to an authorization under subsections 27(1), 28(1) or (2) and 41(1).
17. Amend the triggering threshold for the CSE to seek an authorization from "must not contravene any other Act of Parliament unless…" (*CSE Act*, at ss. 23(3), 23(4)) to also include breaches of provincial law and common law.
18. Clarify that, under its foreign intelligence mandate, the CSE is prohibited from acquiring, using or analysing information relating to events that occur during an interaction between two or more portions of the global information infrastructure known or likely to be end-point devices located within Canada.
19. Amend sub-section 23(2) of the proposed *CSE Act* so that the CSE is precluded from directing activities carried out in furtherance to the foreign intelligence aspect of its mandate at any portion of the global information infrastructure that is in Canada.
20. Amend the *CSE Act* to include the criteria used by the Minister to designate electronic information, information infrastructures or classes of electronic information or information infrastructures as "of importance to the Government of Canada" under subsection 22(1) of the *CSE Act*.
21. Amend subsection 22(1) of the *CSE Act* such that encoded criteria ensure the designated electronic information and information infrastructures can only be those of "*critical* importance."
22. Amend the *CSE Act* to allow any federal institution, as defined in s. 2, to submit a written request to the Minister in order to opt-out of cybersecurity advice, monitoring, and other services provided by the CSE, including but not limited to any of the CSE's activities which could otherwise be authorized under s. 28.
23. Require a written request to carry out the activity from the federal institution in question in order for an authorization to be issued under subsection 28(1), analogous to the provision set out in subsection 34(3) for authorizations under 28(2).
24. Amend paragraph 24(1)(b) so that the activities it authorizes may only occur on electronic information and information infrastructures described in 18(a) of the *CSE*

Act, and only in furtherance of its cybersecurity and information assurance mandate.

25. Amend paragraph 24(1)(a) so that the CSE may only acquire, use, analyze and retain information despite the restrictions in sub-sections 23(1) and (2) if such information falls within a dataset that the Intelligence Commissioner has approved as reasonably necessary to the foreign intelligence or cybersecurity and information assurance aspects of the CSE's mandate.
26. Amend paragraph 24(1)(a) to remove its application to the "disclosure" of publicly available information or, alternatively, amend section 25 so that it ensures any activities directed at Canadians that would amount to a disclosure of publicly available information may only occur under section 44.
27. Amend paragraph 21(4)(c) to, at minimum, include the full and informed consent of any and all individuals whose software, products or systems are being tested or evaluated.
28. Amend paragraph 21(4)(c) to, at minimum, limit its use to cybersecurity objectives.
29. Specify that data acquired further to the CSE's foreign intelligence and cybersecurity and information assurance aspects of its mandate cannot be used, analyzed or disclosed when carrying out activities under the technical and operational assistance aspects of its mandate.
30. When providing technical or operational assistance to domestic law enforcement and other agencies, restrict the CSE from providing access to capabilities or information developed by its international partners—in other words, the assistance aspect of the mandate should be limited to the provision of "in house" expertise.
31. Amend section 33 of the *CSE Act* to apply across all aspects of the mandate, and to the entirety of the CSE's activities (with the potential exclusion of activities undertaken subject to the assistance aspect of the mandate).
32. Amend section 33(1) of the *CSE Act* to add:

    ....

    (c) violating the sexual integrity of an individual;

    (d) subjecting an individual to torture or cruel, inhuman or degrading treatment or punishment, within the meaning of the Convention Against Torture;

    (e) detaining an individual; or

    (f) causing the loss of, or any serious damage to, any property if doing so would endanger the safety of an individual;

    (g) engaging in activities which are likely to undermine the integrity of communications technologies, networks, and services used by the general public, including by weakening or interfering with security standards and protocols.
33. Amend section 33(1)(b) to read, "wilfully attempt in any manner to obstruct, pervert or defeat the course of justice or democracy, including by willfully attempting to obstruct, pervert, or defeat the course of *any judicial proceeding or of any electoral process, directly or indirectly*."

34. Amend the *CSE Act* so that emergency authorizations may only be issued in truly exigent circumstances.
35. Require Parliament to undertake a study regarding the benefits, challenges, and feasibility of separating the CSE into two distinct agencies, one of which is tasked exclusively with cybersecurity, information assurance and defence; the other which is exclusively responsible for foreign intelligence and any cyber operations activities.
36. Require Parliament to undertake a study which addresses (1) the division of labour and separation of roles between the CSE and the Canadian Forces with regard to cyber operations, and the division of labour and separation of roles between the CSE and CSIS with regard to foreign intelligence activities.

Issues with Defined (and Undefined) Terms

37. Amend the *CSE Act* to clarify that the words "intercept", "analysis", "interception" and "acquisition" have the same meaning in the *CSE Act* as in Part VI of the *Criminal Code*.
38. Define the words "acquire," "use", "analyze" and "collect" in the *CSE Act* so that what constitutes an incidence of "acquisition" and an incidence of "collection" is explicit, and so that there is a clear distinction between the analysis and use of information already acquired, and the analysis and use of information that the CSE has not already acquired.
39. Amend the *CSE Act* to remove section 61(c).
40. Redefine "publicly available information" in the *CSE Act* so that it is limited in application to commercially available publications and broadcasts.
41. Amend section 44 to exclude the term "cybersecurity," which is not defined in the *CSE Act* and is not otherwise mentioned in relation to the CSE's foreign intelligence activities.
42. Ensure that the complete set of measures referred to in section 25 and adopted in regulation under section 61(b) to protect the privacy of Canadians and persons in Canada are made available to the public for comment and analysis.
43. Require the Office of the Privacy Commissioner of Canada to annually evaluate the protections for Canadians and persons in Canada under section 25, and to be able to provide recommendations to the CSE and the Intelligence Commissioner.

Arrangements

44. Amend section 55 of the *CSE Act* to require that the Minister seek the approval of the Intelligence Commissioner for all arrangements with institutions of foreign states or that are international organizations of states or institutions of those organizations.
45. Amend section 55 such that the CSE is prohibited from knowingly entering into arrangements with institutions of foreign states or other entities suspected of engaging in torture.
46. Amend section 55 of the *CSE Act* to require that the Commissioner, when approving an arrangement, ensures that all activities to be undertaken in the furtherance of the CSE's mandate pursuant to the arrangement (including for the purposes of information sharing or other forms of cooperation) are lawful, constitutional,

reasonably necessary, and proportional.

47. Amend section 55 of the *CSE Act* to include a framework for review and renewal of all arrangements entered into by the CSE on a periodic basis. In the case of arrangements with institutions of foreign states or that are international organizations of states or institutions of those organizations, the renewal process should include the consent of the Minister of Foreign Affairs and the approval of the Intelligence Commissioner.

Reporting and Transparency Measures

48. Require the Government of Canada to publicly report, on an annual basis, the foreign intelligence and cybersecurity priorities it establishes for the CSE.
49. Require the establishment of a Vulnerabilities Equities Program for the CSE that includes a requirement that evaluation criteria for disclosure be made completely public.
50. Require that VEP criteria should specify the need to prioritize the public interest and public safety over the CSE's intelligence-gathering or disruption-related operational objectives. Enable the Intelligence Commissioner and/or independent non-governmental experts to advance these public interest concerns.
51. Require public reporting on the Vulnerabilities Equities Program, including disclosure with regard to the frequency at which the CSE discloses vulnerabilities to Computer Emergency Response Teams, public institutions, private organizations, and other entities.
52. Require public reporting on the frequency at which the CSE provides technical and operational assistance to other entities, as well as reporting about which agencies receive that assistance, in the CSE's annual review documents.
53. Require the NSIRA to review, on a regular basis, the structure and information provided by the CSE in its annual report and be authorized to recommend the CSE include specific information in future reporting, including periodic inclusion of statistical information regarding the nature and scope of its activities.
54. Require public reporting on the frequency of defensive and active cyber operations.