The Coming Tsunami of Transnational Repression*[1]

Ronald J. Deibert
12 March 2026

My name is Ron Deibert, and I am professor of political science and the founder and director of the Citizen Lab at the University of Toronto's Munk School of Global Affairs and Public Policy.

The mission of the Citizen Lab is to undertake evidence-based investigations into digital security issues that arise out of human rights concerns. For over two decades, our group has published pioneering reports about risks to civil society in the digital sphere, including mapping online censorship, surveillance, influence operations, and cyber espionage campaigns worldwide. These investigations have received widespread global media coverage and have helped trigger litigation, sanctions, criminal charges, regulations, and other international efforts at mitigation. In 2022, I was appointed Officer of the Order of Canada for my work as founder and director of the Citizen Lab.

Background

Transnational repression (TNR) is defined as states reaching across borders to repress dissent. The targets of TNR are primarily diaspora members, including political exiles, asylum seekers, and people with personal connections to a perpetrating state. Digital transnational repression (DTR) is when such conduct is undertaken using the internet or related cyber technologies, such as online harassment, influence operations, geolocation tracking, or the hacking of personal devices. DTR is harmful in its own right, but can also be used as a stepping stone to more serious physical attacks, such as when data on victims' movements or places of residence are acquired to help conduct an assault, kidnapping, or assassination.

TNR and DTR are conceptually distinct from "foreign interference." Foreign interference concerns one government intervening in the domestic affairs of another government, such as through attempted manipulation of election results or cyber espionage against a government agency. Foreign interference is a function of geopolitical competition between states. TNR and DTR are best understood as either subsets of foreign interference or their own distinct category of action. States undertaking TNR and DTR may in fact be agnostic about the specific state in which a target lives, or at most factoring it in only as a function of the perpetrator's risk

[1] Remarks prepared for *The Canadian House of Commons' Subcommittee on International Human Rights of the Standing Committee on Foreign Affairs and International Development*

calculation (i.e., will there be significant political or diplomatic costs of getting caught). The actual target of TNR or DTR is a person living abroad, not the state in which they live. The difference in framing matters because of the ways in which policies flow from each. Foreign interference is typically framed as a national security issue, thus prioritizing the involvement of security agencies and all that goes along with them (e.g., secrecy). Those responses may be counterproductive to what is required to mitigate TNR and DTR. TNR and DTR are ultimately human rights issues.

We first encountered DTR more than 15 years ago, although the term itself did not yet exist. Beginning in the late 2000s and early 2010s, our investigations into cyber espionage targeting civil society uncovered numerous cases of state agencies using highly advanced hacking technology to get inside the phones of dissidents and refugees who had fled abroad for their safety. These surveillance operations were conducted by governments in just about every region of the world, including Bahrain, the U.A.E., Saudi Arabia, China, Russia, Iran, Rwanda, Ethiopia, El Salvador, Thailand, and many others.

Over time, we came to understand that the mercenary spyware industry was a major driver of the spread of authoritarian practices across borders. This largely unregulated sector was placing a new form of stealthy global reach in the hands of autocratic regimes and despots, enabling them to target individuals who had fled to a foreign country. Hacking a target's phone is like slipping inside that target's entire life without them knowing. Once inside a device, an operator can observe everything as if looking at the device through the owner's eyes. It also allows an operator to bypass whatever end-to-end encryption exists to protect communications, as on popular messaging apps like Signal or WhatsApp.

This topic hit close to home in 2018, when we uncovered Saudi espionage against Omar Abdulaziz, a Canadian permanent resident and close confidant of the late *Washington Post* journalist Jamal Khashoggi. Abdulaziz and Khashoggi had been communicating about their activism over an end-to-end encrypted messaging application for months, assuming their conversations were protected. However, our investigation showed that Abdulaziz's device had been successfully hacked and implanted with NSO Group's Pegasus spyware prior to Khashoggi's murder in the Saudi consulate in Istanbul, Turkey. Pegasus allowed Saudi intelligence to eavesdrop on their conversations for months.

Later, forensic analysis by the Citizen Lab and Amnesty International showed that several members of Khashoggi's inner circle also had their devices hacked with Pegasus spyware, including family members, fellow activists and journalists in the U.S., Europe, and the U.K. Thanks to companies like NSO Group, Saudi intelligence was able to cast a transnational surveillance net around Khashoggi's entire private life prior to his brutal execution.

While highly intrusive, spyware is only one tool in the autocrat's toolkit for undertaking DTR. There are numerous techniques and services that enable perpetrators to put victims under surveillance from abroad, including exploits targeting the mobile telecom ecosystem's weakly secured signalling protocols, advertising intelligence (ADINT) derived from real-time data

brokerages, facial recognition systems, and forensic data extraction tools. As many of our investigations and those of other groups have shown, these systems are now being actively employed by authoritarian governments to engage in domestic and international repression, ranging from harassment campaigns to enforced disappearances.

Throughout our years researching DTR, we have observed perpetrators combining tactics across multiple domains. Highly sophisticated mercenary spyware may be used to infiltrate a victim's device, while other sources of data – such as information obtained through compelled platform disclosures or advertising brokerages – can help build a detailed intelligence dossier on that target. These dossiers may include victims' places of residence and employment, common transit routes, religious affiliations, social relationships, and more. In the most serious of cases, they can be used in combination with physical attacks, such as assaults, kidnappings or murders. All of these systems are commercially available to perpetrators today, many of them developed by ethically-dubious firms that lack public accountability.

Data from these sources can also feed highly personalized harassment, trolling, disinformation, and influence operations designed to belittle or discredit regime opponents. These types of online harassment campaigns have become increasingly easy to mount, thanks to advances in Large Language Models (LLMs) and AI systems that have revolutionized the generation of inauthentic images, audio, and videos. Free versions of online AI platforms, such as X's Grok, can be summoned with a few prompts and within seconds can create a plausible looking video of a target doing incriminating and embarrassing things. It can also be employed to create harmful nonconsensual sexualized content. Unfortunately, most of the social media platforms through which these campaigns take place have rolled back, or eliminated entirely, fact checkers and trust and safety teams whose mission has been to mitigate such abuses.

Victims' Experiences

Beginning in the late 2010s, we started systematically interviewing victims of DTR to better understand their lived experiences. These interviews were conducted under an approved University of Toronto research ethics protocol, and lasted several hours with each victim. We published two major reports: one on DTR victims in Canada (*Psychological and Emotional War: Digital Transnational Repression in Canada*, 2022) and a second that featured a much larger set of DTR victims spread across the world, with a special focus on gender and DTR (*No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression*, 2024).

These interviews surfaced common experiences. Victims who had suffered torture and other types of repression and who had fled from one country to another for their safety soon realized that they were not truly safe at all. Their sense of sanctuary was shattered when the governments they had fled from reached across borders to harass, surveil, and track them. Victims described not knowing where to turn or receiving little help when they reported their experiences to authorities. Formal complaints submitted to law enforcement typically went nowhere, with local officials either unable to determine who was responsible or, when it was

clear, unable to hold foreign governments accountable because they were shielded by distance and sovereign immunity protections. Worst of all were instances when victims reported being approached by members of their host country's security services, such as CSIS in Canada; victims described feeling like they were being treated more like potential intelligence assets for the host country's security agencies than people deserving compassion and help.

DTR has had major chilling effects on civil society. We observed many victims retreating into isolation, too afraid to speak up or engage with members of their fellow diaspora communities. Paranoia was common, and for understandable reasons. Victims reported being unable to properly evaluate whether their devices, social media platforms, or applications were safe to use with some deciding to abandon them altogether out of an abundance of caution. Victims reported describing the internet and social media as threatening and toxic, nullifying any positive social or networking effects they may have once provided.

We found that women and sexual minorities experience DTR differently than men. Misogynistic campaigns vilifying transgender and queer communities are common in patriarchal authoritarian regimes. Women and those who identify as LGBTQ+ often face sexualized harassment and threats of gendered violence, especially as authoritarian regimes systematically promote patriarchal norms and discredit "woke" ideologies as part of their strongman political repertoire and then carry those themes into their DTR campaigns. Some of this sexualized harassment is outsourced to private actors and then fed into swarms of misogynic trolls on social media platforms which, in at least the case of X, actually seem to encourage such behaviour.

The Good News

Thanks to the work of a growing number of groups focused on DTR, there have been some positive developments. Fifteen years ago, we lacked the terminology to describe what we were witnessing. Today, TNR and DTR are widely recognized phenomena, and the language is familiar to policymakers and stakeholders around the world. That alone is significant, because naming a problem is the first step toward addressing it.

This growing awareness has triggered government policy responses. For example, in the United States under the Biden administration, many federal agencies began to develop policies and programs addressing both TNR and DTR. The FBI publicly defined TNR as a priority area, detailing tactics such as stalking, cyberhacking, harassment, and threats used by foreign governments against dissidents and diaspora communities. The DOJ pursued criminal charges and indictments against individuals acting on behalf of foreign governments for schemes that included threats, intimidation, and spying on individuals within the United States.

The U.S. government also focused on the enabling technologies, issuing Executive Order 14093, which prohibited the procurement of commercial spyware by U.S. agencies from mercenary spyware firms when it can be demonstrated their technology has posed counterintelligence, national security, or human rights risks. The U.S. Treasury Department

sanctioned firms and individuals while the State Department put in place visa restrictions against individuals involved in the abusive deployment of spyware. I will return to what is currently happening in the United States later in my testimony.

In the United Kingdom, the government has also made some efforts to address TNR and DTR, though these efforts could also be strengthened. There has been some progress in ensuring that victims of DTR are able to access a legal remedy through civil litigation. In January 2026, the High Court of England and Wales ordered Saudi Arabia to pay more than £3 million in damages to London-based Saudi dissident Ghanem Al-Masarir after finding evidence that his phones had been hacked with NSO Group's Pegasus spyware and that he was subsequently physically attacked in London. The case dates back to 2018, when the Citizen Lab first discovered that Al Masir's device had been hacked with NSO Group's Pegasus spyware, showing what one pathway from investigation to justice may look like and ensuring that sovereign immunity does not bar the way.

In Canada, the federal government has explicitly recognized TNR as a real threat and condemned both physical and digital methods used by foreign states, most notably in the June 2025 G7 Leaders Statement. Global Affairs Canada also houses the Rapid Response Mechanism (RRM), a G7 coordination center based in Canada that helps democracies detect and respond to foreign disinformation and interference campaigns; the RRM has produced useful bulletins on these topics. Along with several other governments and nonprofit organizations, Canada has contributed to the Common Cyber Good fund whose aim is to "sustain nonprofit organizations whose work strengthens the public-interest cybersecurity ecosystem" – an endeavour that, if successful, would help protect victims of DTR. The Canadian government has also established a foreign interference watchdog, which may ensure continued high-level attention to the topic.

But our impression, based on extensive conversations with victims across the country, is that actions have lagged behind words in Canada. Certainly the Canadian government has not put anywhere near the effort the United States did to target the abuse of mercenary surveillance technologies under the Biden administration, such as bans, sanctions and visa restrictions. And many victims still describe poor or nonexistent support among local authorities when reporting cases. We are aware of at least one exception: The York Regional Police has developed an extensive framework and set of programs to deal with TNR and DTR. Their efforts are a model and I encourage you to look more closely at what they have done.

The Bad News

In spite of positive developments, there are at least three reasons to believe that TNR and DTR will expand dramatically in the coming months and years: the sudden descent into authoritarianism in the United States; the rapid development and widespread use of artificial intelligence (AI) technologies; and Prime Minister Carney's adoption of a realist-inspired "variable geometry" foreign policy for Canada.

The Authoritarian Turn in the United States

We have all witnessed the spectacle unfolding south of the border, and as Canadians we hear clearly the threats to our sovereignty. Among the many things that can be said about that sad situation is its impact on the topic of this hearing.

The United States has suddenly pivoted from a state that was developing a sensible and helpful approach to combatting TNR and DTR to becoming a major enabler of them instead. A key pillar of the Trump regime's domestic agenda is its cruel and unprecedented assaults on immigrants and refugees and its open embrace of white nationalist and fascist rhetoric. Its Immigrations and Customs Enforcement (ICE) agency has become, for all intents and purposes, a secret paramilitary police force. Its recruitment materials employ neo-Nazi memes and symbols. Many of its agents have been poorly vetted and trained, and reportedly include far-right insurrectionists and white nationalists. They roam the streets without identification, outfitted in battlefield fatigues, heavily armed, and routinely kidnap people or break into their homes without warrants or probable cause. ICE agents have murdered U.S. citizens for no legitimate cause and yet were not held accountable for their actions. They have built or are in the process of building massive concentration camps to house detainees before deporting them to countries where the prospect of torture or other types of persecution is very high. This includes sending Russians, Iranians, Chinese, and others back to jurisdictions from which they had once fled to the United States for sanctuary.

To equip its domestic security apparatus, the Trump administration has allocated an enormous $85 billion to ICE, making it the highest-funded law enforcement agency in the country. A sizable proportion of this massive budget has gone to equipping ICE with the latest surveillance gear, including contracts with mercenary spyware firms, cellphone forensic data extraction companies, advertising intelligence (ADINT) firms, facial recognition companies, and data fusion and analysis platforms. Ominously, almost all of the U.S.-based technology platforms have publicly praised the Trump administration's MAGA agenda, with many of them donating to his inauguration and venal White House ballroom project. Under Trump, an executive branch-controlled techno-fascist fusion appears to be developing, which can be used to monitor and neutralize political dissent as well as train ICE on marginalized and vulnerable communities for mass deportation. Apart from all of the other immediate harms, the sudden injection of large amounts of financing into the surveillance sector will enrich ethically dubious companies and give them a U.S. procurement "seal of approval," which will help market their wares to authoritarian governments abroad.

The Trump administration has also unleashed politically motivated investigations and other attacks on universities, philanthropies, media, law firms, judges, political opposition figures, and civil society organizations supporting refugees and immigrants. Once nominally independent from the executive, the DOJ has become a weapon in the administration's arsenal of domestic repression, and has trained itself on outlawing those that resist its deportation regime and other programs. Those who have opposed ICE's actions – including citizens exercising their First

Amendment rights to film ICE operations – have been labelled "domestic terrorists." The U.S. government has cut back or eliminated funding for agencies that promote democracy abroad and help support immigration and refugee resettlement, including those that have helped raise awareness about TNR and DTR, and has withdrawn from dozens of international organizations that could be employed to coordinate mitigation efforts. Law enforcement resources that were earmarked for combatting TNR and DTR have also been diverted to focus on the deportation program or hunting "domestic terrorists."

On top, the Trump regime's corruption is unprecedented, which may help prejudice U.S. government responses to combatting TNR and DTR. Trump family members and business associates act as policy advisors and conflict negotiators in the Middle East and Europe at the same time as they are enriching themselves in business ventures with Gulf sheikdoms and other oligarchs that also happen to be some of the world's worst perpetrators of TNR and DTR, such as the U.A.E. and Saudi Arabia. As an illustration of how such ties can prejudice the government's response, in a November 2025 White House meeting with Saudi Crown Prince Mohamed bin Salman, Trump responded to a reporter's question about the Khashoggi murder by suggesting he may have deserved it and reprimanded the reporter for daring to ask about the case.

The U.S. military has also embarked on a series of unprecedented and aggressive military adventures, including kidnapping a head of state and assassinating another in clear violation of both international law and constitutional rules requiring congressional approval for acts of war. An explicit aim of the Trump regime appears to be a "world without rules," as Oona Hathaway and Scott Shapiro have called it. It is one in which there are no "constraints on the exercise of state power," which is precisely the type of world order favourable to dictators, despots, oligarchs and their mercenary benefactors. Reflecting this cynical approach to world affairs, Trump has formed an Orwellian-named "Board of Peace" whose members are made up entirely of governments that have been routinely flagged for human rights abuses. According to Nate Schenkkan, formerly of the U.S.-based Freedom House – an organization that helped raise alarms about TNR and DTR but which has also been targeted with budget cuts under the Trump regime – we are now entering into a "golden age of transnational repression."

This momentous shift of the world's most powerful country will have major direct and indirect consequences for TNR and DTR. It will normalize state repression and thus embolden dictators all over the world who now have a model for crackdowns on political opposition. With its domestic security agencies now focused on deportation and political repression, refugees and immigrants and other marginalized populations who once looked to authorities for help are now hiding from the state's goon squads that are hunting them down instead. The U.S. government's spending spree on surveillance systems will help legitimize government procurement of services from mercenary firms all over the world, which will invariably be further deployed to target and repress dissidents abroad in new high-tech ways.

Artificial Intelligence

Over the last several years, artificial intelligence has shifted from basic systems that can categorize or predict within narrow parameters to models that can now generate language, images, videos, and code across numerous domains at lightning speed, enabled in part by a massive increase in the power of computer processing used during training. At the same time, these systems have moved from research settings into widely used products and services, touching billions of users within months. Although it is too early to say what the comprehensive implications of AI will be, there is no doubt that it will be massively transformative of nearly every facet of life, TNR and DTR included.

In the current political and economic context, in which authoritarianism is ascendent and the tech platforms are eliminating or scaling back safeguards, it is inevitable that AI is going to be used for malicious purposes, including for TNR and DTR. Indeed, our research has already shown AI tools being deployed in phishing campaigns and influence operations, and among police and customs and border patrol agencies in Canada. AI platforms themselves have disclosed misuses of their systems to enable cyber crime, cyber espionage, influence operations, disinformation, and in cases that appear connected to TNR and DTR operations. In this context, while such disclosures in the public interest are laudable, it raises the question of to what extent AI platforms, which collect voluminous amounts of highly personalized information about their users, may be complying with secretive government orders to turn over that data to be used for state repression.

Some mercenary surveillance firms, whose technology has been extensively documented in connection with DTR, have started advertising their services to include AI components to help make them more efficient. It is certain that AI will increase the scale, speed, and precision of TNR and DTR, and allow states to monitor, profile, and target individuals across borders more rapidly and with greater precision than ever before. AI can be used to speedily synthesize large amounts of disparate data coming from multiple sources, including hacked systems and open-source information. Research has shown that LLMs can be used to rapidly and effectively deanonymize social media users, which may create retroactive risks for activists who spoke publicly in the past about a regime using pseudonyms. We are already witnessing AI systems being widely used as part of coordinated inauthentic disinformation and trolling campaigns. These techniques will make DTR more psychologically harmful and harder to refute.

Ominously, AI platforms have also sought and obtained huge contracts for services with defense and intelligence agencies. It is telling that even while one firm, Anthropic, resisted U.S. pressure to use its systems in ways that crossed ethical red lines, the company's CEO still explained its overall mission as broadly supportive of U.S. military might and national security interests. Anthropic's technology was reportedly used to help identify targets in the U.S. strikes on Iran, some of which have resulted in extensive civilian casualties and the destruction of non-military infrastructure. Anthropic is currently suing the U.S. government after it designated Anthropic a "supply chain risk" as punishment for not complying with U.S. military and intelligence uses.

Regardless of the outcome of that litigation, however, the case will likely be remembered for showing the private sector the costs of not going along with a government's demands. One can only imagine what deals have been struck between defense and intelligence agencies and some AI platforms without even a modicum of this type of publicly articulated, but modest, example of self restraint.

It is highly concerning, therefore, that the Canadian government, led by its Minister of AI and Innovation Evan Solomon, appears to be broadly enthusiastic about AI and has, according to an open letter signed by 160 civil society organizations and experts, failed to properly acknowledge and deal with AI-associated harms. It has signed a memorandum of understanding to strengthen collaboration with the U.A.E., one of the world's worst human rights abusing autocratic regimes with a long track record of supporting unethical surveillance ventures and engaging in DTR. The Canadian government has openly acknowledged that its government departments will be widely deploying AI to improve efficiency even while our research and that of other groups has shown when AI is used in predictive policing and immigration cases it can further entrench preexisting prejudices and racial biases. This is not an administration prepared to deal with the coming flood of AI-enabled repression methods.

Variable Geometry

Canadian Prime Minister Mark Carney received widespread praise for his remarks at the World Economic Forum Annual Meeting 2026 in Davos, where on January 20, 2026, he outlined a new foreign policy vision for Canada. In the speech, titled "Principled and Pragmatic: Canada's Path," Carney described an approach combining "values-based realism" with a pragmatic strategy of "variable geometry," meaning the formation of different international coalitions depending on the issue and the alignment of values and interests. Although he was applauded for speaking plainly in response to the Trump administration's aggressively unilateralist posture, some, including this author (alongside my colleague Jason Stanley), criticized the Prime Minister for not clearly underlining our country's commitment to human rights and the rule of law.

These concerns have been borne out since Carney's speech. In January and February 2026, the Prime Minister went on state visits and entered into partnership with two major perpetrators of foreign interference and TNR/DTR: China and India. The memorandum with China included a commitment to "combatting crimes," even though political dissent is considered a crime in China. It also will include strengthening police cooperation, which would be highly concerning in light of the fact that China's own law enforcement is a major perpetrator of TNR and DTR on Canadian soil. Meanwhile, Prime Minister Carney's trip to India was meant as a "reset" to relations even though the Canadian government and the RCMP stated publicly they found evidence linking agents of the Government of India to serious criminal activities in Canada, including the murder of Canadian citizen Hardeep Singh Nijjar in June 2023.

There have been other troubling patterns evident from Carney's variable geometry. After the U.S. imposed sanctions on International Criminal Court jurist and Canadian citizen Kimberly

Prost, the Canadian government remained quiet. Notably, former Canadian Ambassador to the United Nations, Bob Rae, issued a statement calling the sanctions "disgraceful" before quickly deleting the statement. While there are hopefully quiet diplomatic efforts afoot, the public silence invites similar assaults on international organizations that Canada has built and ultimately depends on for our own national security.

After the U.S. and Israel launched a war on Iran, Prime Minister Carney issued a statement that condemned Iran and encouraged respect for civilians but failed to call out the flagrant violation of international law and the lack of any attempt to seek UN Security Council approval for the war. Indeed, the statement said the Government of Canada "supports the United States acting to prevent Iran from obtaining a nuclear weapon and to prevent its regime from further threatening international peace and security." The protection of citizens from TNR and DTR ultimately rests on a foundation of international human rights law, which Canada has traditionally supported; Prime Minister Carney's recent foreign policy shift signals a potential softening of that stance, especially by what is left out. That may come back to haunt Canadians.

Recommendations

In light of all the above, it is my belief that there will be a tsunami of new TNR and DTR related incidents in Canada. There is also a high likelihood that the U.S. government will pressure Canada to assist with repressive efforts that violate our Charter protections and other principles and values. With that in mind, I make the following recommendations:

- ***Keep the momentum up and expand it.*** The Canadian government and various local agencies have now publicly condemned TNR and DTR and policymakers have been vocal about the need to address it. Recommendations have been made by many experts and stakeholders about what to do, and in some cases (like the York Regional Police and RRM) action has been taken. But, there is still a lot of work to do to translate words into practice. Above all else, the Canadian government must engage more deeply with diaspora members and communities most closely affected by TNR and DTR to understand their concerns and needs and build responses tailored to those at a grassroots level. Government representatives, including law enforcement, must be trained in regional geopolitics, local languages, and contextual knowledge to better understand victims' experiences. Victims must have an easy to use hotline to report cases, and expect some immediate and meaningful response. It is therefore very disappointing to see that the Canadian government has financially cut various forms of immigration and refugee support at the very time it is going to be needed most. These cuts should be immediately reversed and community-level TNR and DTR support systems bolstered against what is likely to be a major wave of cases.

- ***Turn pledges into action.*** In spring 2023, the Canadian government signed onto a pledge alongside nearly two dozen other countries to better regulate the mercenary spyware industry, which is a major enabler of DTR. However, the Canadian government

has done very little to carry through on that pledge. Unlike the United States under the Biden administration, the Canadian government has not put in place export controls or procurement restrictions against mercenary surveillance firms, nor has it held individuals who have helped engineer human rights abuses accountable with visa restrictions and sanctions. The time is long overdue for Canada to contribute to this space, especially in light of the fact that the U.S. government itself may be abandoning its commitments to the area. Canadian authorities must also devote resources to investigating perpetrators of TNR and DTR, and open up legal avenues for victims to hold them accountable in Canadian courts.

- ***Regulate AI.*** The government must squarely and soberly address the huge potential for widespread harm associated with LLMs and AI systems, as well as social media platforms which are connected to them. Although there are many potential economic and other benefits associated with these systems, the current political and economic context all but assures there will also be major harms emanating from their use and abuse. The government should cease any cooperation with governments on AI that are known perpetrators of TNR and DTR. It should engage in meaningful public consultation with affected communities on how these systems have begun to negatively affect peoples' lives, as called for by the People's Consultation on AI. And it should find ways to regulate AI uses, particularly among public agencies, to mitigate harms and ensure equitable outcomes. Part of this regulation must include independent due diligence audits of all tech platforms in a transparent and accountable manner consistent with Charter of Human Rights protections on freedom of speech and access to information.

- ***Review the Canada-US Safe Third Country Agreement***. In a recent publication, which echoes many of the themes of my written testimony, Citizen Lab colleagues recommended that the Canadian government review the Canada-US Safe Third Country Agreement, which designates the United States as a safe third country because its "refugee status determination system offers a high degree of protection to refugee protection claimants" and because the country "meets a high standard with respect to the protection of human rights." Clearly these determinations are now out of date and will need rethinking, alongside a more comprehensive consideration of the risks of TNR and DTR emanating from south of the border. Unlike the United States, which is shaping itself into a white ethnonationalist regime, Canada has always prided itself on its multiculturalism and commitment to the rule of law. We must contrast our approach more forcefully, not only with words but with deeds to match.

.