

**IMMIGRATION DIVISION
IMMIGRATION AND REFUGEE BOARD OF CANADA**

Between:

THE MINISTER OF PUBLIC SAFETY AND EMERGENCY PREPAREDNESS

Applicant

-and-

CHELSEA ELIZABETH MANNING

Respondent

STATEMENT OF RONALD J. DEIBERT

Overview

1. I am a Professor of Political Science and Director of the Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto. I have been asked to provide this statement in the context of Chelsea Manning's inadmissibility proceeding before the Immigration and Refugee Board of Canada.
2. This statement proceeds in four parts. In the first section, I provide background context regarding my professional experience and the Citizen Lab's work. In the second section, I describe the Citizen Lab's research activities in detail and the academic and public interest impacts of those activities. In the third section, I summarize certain events that have threatened or aimed to chill the Citizen Lab's research activities in the past. In the fourth section, I explain the chilling effects that a broad interpretation of section 342.1 of the *Criminal Code* and/or of subsection 16(2) of the *Security of Information Act* ("SOIA") could have on the Citizen Lab's scholarship and on related initiatives.

Background and Credentials

3. I received an B.A. from the University of British Columbia in 1988, an M.A. from Queen's University in 1990, and a PhD from the University of British Columbia in 1995. I have been employed by the University of Toronto Department of Political Science continuously since 1996 as an Assistant Professor (1996-2001), an Associate Professor (2001-2011), and as a full Professor since 2011.
4. I am the founding Director of the Citizen Lab, 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. My research activities are directed primarily through the projects and collaborative partnerships of the Citizen Lab.

5. The Citizen Lab is based at the Munk School of Global Affairs & Public Policy, University of Toronto. It currently employs eighteen full and part-time staff, the majority of whom are researchers in computer science and the social sciences. It is also home to about the same number of fellows, including various affiliated academics, lawyers, and researchers who contribute to the organization's activities.
6. The Citizen Lab is funded by the university and has received funding from various government and private funding institutions, including the Canada Centre for Global Security Studies, Donner Canadian Foundation, Ford Foundation, Hewlett Foundation, HIVOS, The Hopewell Fund, International Development Research Centre (IDRC), John D. and Catherine T. MacArthur Foundation, Oak Foundation, Open Society Foundations, Psiphon Inc., The Sigrid Rausing Trust, Social Sciences and Humanities Research Council of Canada, and the Walter and Duncan Gordon Foundation. The Citizen Lab also receives in-kind donations of investigative tools from various technology companies.
7. I am the co-editor of three major volumes with MIT Press: *Access Denied: The Practice and Policy of Internet Filtering* (2008), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (2010), and *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (2011). I am also the author of *Parchment, Printing, and Hypermedia: Communications in World Order Transformation* (New York: Columbia University Press, 1997), *Black Code: Surveillance, Privacy and the Dark Side of Cyberspace* (Signal/McClelland & Stewart/Random House, 2013), and *Reset: Reclaiming the Internet for Civil Society* (House of Anansi Press, 2020 / September Publishing, UK), which was delivered as part of the 2020 CBC Massey Lecture series.
8. I currently serve on the editorial boards of the journals *International Political Sociology*, *Explorations in Media Ecology*, *Review of Policy Research*, *Journal of Global Security Studies*, and *Astropolitics*. I also have served on the advisory boards of Access Now, Privacy International, the technical advisory groups of Amnesty International and Human Rights Watch, and am currently a member of the advisory boards of PEN Canada and the Design4Democracy Coalition, as well as the Steering Committee of the World Movement for Democracy.
9. My work as the Director of Citizen Lab and as a scholar has received extensive recognition. In particular, I have been awarded the University of Toronto's Outstanding Teaching Award (2002), the Northrop Frye Distinguished Teaching and Research Award (2002), the Carolyn Tuohy Award for Public Policy (2010), and the President's Impact Award (2017). I was a Ford Foundation research scholar of information and communication technologies (2002-2004), named among Esquire Magazine's "Best and Brightest List" of 2007, listed among SC Magazine's 2010 top "IT Security Luminaries", and named one of the top "Humans of the Year" in 2017 by VICE.
10. In 2017, I was included in Foreign Policy Magazine's 2017 "Global Thinkers" list, an honour I shared that year with Chelsea Manning — as well as with French President

Emmanuel Macron, Canadian Foreign Affairs Minister Chrystia Freeland, Chinese artist Ai Weiwei, San Juan mayor Carmen Yulín Cruz, and other notable recipients. I also accepted the Electronic Frontier Foundation Pioneer Award on behalf of the Citizen Lab in 2015, an award which I understand Ms. Manning won two years later. I am also the recipient of the Neil Postman Award for Career Achievement in Public Intellectual Activity (2014), the Advancement of Intellectual Freedom in Canada Award from the Canadian Library Association (2014), and the Canadian Journalists for Free Expression Vox Libera Award (2010).

11. In 2019, I received an honorary Doctor of Laws from the University of Guelph. In 2020, I was awarded two ISA (International Studies Association) awards: the ISA Canada Distinguished Scholar award and the STAIR Distinguished Scholar ‘Transversal Acts’ award. In 2013, I 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.”

The Citizen Lab’s Activities and Impact

12. For over a decade, the Citizen Lab has used a mixed methods approach that combines techniques from network measurement, information security, law, and the social sciences to research and document information controls — including Internet censorship and surveillance — that impact the openness and security of digital communications and pose threats to human rights.
13. As Director of the Citizen Lab, I have overseen and been a contributing author to more than 120 reports¹ covering path-breaking research on cyber espionage, commercial spyware, Internet censorship, and human rights. The following are a few examples of Citizen Lab reports with a technical² dimension:
 - a. **Tracking Ghostnet (2009)**, which uncovered an espionage operation that infiltrated the computer networks of hundreds of government offices, NGOs, and other organizations, including those of the Dalai Lama;³

¹ A complete list of the Citizen Lab’s publications, including research reports, articles, book chapters, resources and external submissions to government and international bodies is available online: <https://citizenlab.ca/publications/>.

² For a summary of what is meant by “technical” research, a summary of some of the general tools and methods employed by Citizen Lab researchers is provided at paragraph 28.

³ Information Warfare Monitor, “Tracking GhostNet: Investigating a Cyber Espionage Network” (Information Warfare Monitor, Munk School of Global Affairs, University of Toronto, Toronto, ON, 2009); see also Bill Marczak, Adam Hulcoop, Etienne Maynier, Bahr Abdul Razzak, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert. “Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits,” Citizen Lab Research Report No. 123, University of Toronto, September 2019.

- b. **China’s Great Cannon (2015)**, which exposed an offensive tool used to hijack digital traffic through Distributed Denial of Service attacks, demonstrating the Chinese government’s ability to enforce censorship by weaponizing users;⁴
- c. **The Million Dollar Dissident (2016)**, which revealed the use of a zero-day iPhone exploit by NSO Group against the UAE human rights defender Ahmed Mansoor;⁵
- d. **Tainted Leaks (2017)**, which investigated manipulated leaks and the discovery of a phishing operation targeting over 200 people, including a former Russian Prime Minister, members of cabinets, ambassadors, high ranking military officers, CEOs of energy companies, and members of civil society;⁶
- e. **The Reckless Series (2017-2019)**, which investigated the abuse of NSO Group’s “Pegasus” spyware to target journalists, anti-corruption advocates, and public health officials in Mexico, as well as their family members;⁷
- f. **Bad Traffic (2018)**, which uncovered the apparent use of Sandvine/Procera Networks Deep Packet Inspection technology to redirect hundreds of users in Turkey and Syria to nation-state spyware, as well as its use to hijack Egyptian Internet users’ unencrypted web connections for profit;⁸
- g. **The Kingdom Came to Canada (2018)**, which investigated how Omar Abdulaziz, a Canadian permanent resident, Saudi dissident, and colleague of murdered journalist Jamal Khashoggi was targeted with NSO Group’s spyware by an operator linked to Saudi Arabia;⁹

⁴ Bill Marczak (Lead), Nicholas Weaver (Lead), Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald Deibert, Vern Paxson, “China’s Great Cannon,” Citizen Lab Research Report No. 52, University of Toronto, April 2015.

⁵ Bill Marczak and John Scott-Railton. “The Million Dollar Dissident: NSO Group’s iPhone Zero-Days used against a UAE Human Rights Defender,” Citizen Lab Research Report No. 78, University of Toronto, August 2016.

⁶ Adam Hulcoop, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ron Deibert. “Tainted Leaks: Disinformation and Phishing with a Russian Nexus,” Citizen Lab Research Report No. 92, University of Toronto, May 2017.

⁷ See first report in series (and links to subsequent reports): John Scott-Railton, Bill Marczak, Claudio Guarnieri, and Masashi Crete-Nishihata. “Bitter Sweet: Supporters of Mexico’s Soda Tax Targeted With NSO Exploit Links,” Citizen Lab Research Report No. 89, University of Toronto, February 2017.

⁸ Bill Marczak, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert. “Bad Traffic: Sandvine’s PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?,” Citizen Lab Research Report No. 107, University of Toronto, March 2018.

⁹ Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ron Deibert. “The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil,” Citizen Lab Research Report No. 115, University of Toronto, October 2018.

- h. **Can't Picture This (2018)** and **Can't Picture This 2 (2019)**, which analyzed real-time automatic censorship of chat images on WeChat (the most popular chat app in China), documenting censorship of political content, sensitive text, and images pertaining to government, social resistance, and current events;¹⁰
- i. **Stopping the Press (2020)**, which showed that *New York Times* journalist Ben Hubbard had been targeted with NSO Group's Pegasus spyware by the same Saudi Arabia linked operator that targeted Saudi dissidents including Omar Abdulaziz, Ghanem al-Masarir, and Yahya Assiri;¹¹
- j. **Dark Basin (2020)**, which exposed a hack-for-hire group that has targeted thousands of individuals and hundreds of institutions on six continents, including journalists, elected and senior government officials, hedge funds, and multiple industries, as well as advocacy groups, environmental activists, and net neutrality activists;¹²
- k. **Hooking Candiru (2021)**, which revealed spyware infrastructure belonging to a mercenary spyware vendor called Candiru and — in collaboration with Microsoft Threat Intelligence Center — discovered two vulnerabilities (then patched by Microsoft) that were used to target at least 100 victims throughout the Middle East and beyond;¹³
- l. **FORCEDENTRY (2021)**, which exposed a zero-day zero-click exploit against Apple's iMessage which put all Apple iOS, MacOS and WatchOS users at risk and was used by NSO Group to remotely exploit and infect the latest Apple devices with Pegasus spyware (then patched by Apple);¹⁴

¹⁰ Jeffrey Knockel, Lotus Ruan, Masashi Crete-Nishihata, and Ron Deibert. “(Can't) Picture This: An Analysis of Image Filtering on WeChat Moments,” Citizen Lab Research Report No. 112, University of Toronto, August 2018. Jeffrey Knockel and Ruohan Xiong. “(Can't) Picture This 2: An Analysis of WeChat's Realtime Image Filtering in Chats,” Citizen Lab Research Report No. 122, University of Toronto, July 2019.

¹¹ Bill Marczak, Siena Anstis, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert. “Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator,” Citizen Lab Research Report No. 124, University of Toronto, January 2020.

¹² John Scott-Railton, Adam Hulcoop, Bahr Abdul Razzak, Bill Marczak, Siena Anstis, and Ron Deibert. “Dark Basin: Uncovering a Massive Hack-For-Hire Operation,” Citizen Lab Research Report No. 128, University of Toronto, June 2020.

¹³ Bill Marczak, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert. “Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus,” Citizen Lab Research Report No. 139, University of Toronto, July 2021.

¹⁴ Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert, “FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild,” Citizen Lab Research Report No. 140, University of Toronto, September 2021.

14. These reports have been cited widely in global media, garnering more than 25 front page exclusives in *The New York Times*, *Washington Post*, and other leading outlets, and have been cited by policymakers, academics, and civil society as foundational to the understanding of digital technologies, human rights, and global security.
15. The Citizen Lab's research is subject to rigorous ethical protocols, including, where required, approval from the relevant University of Toronto Research Ethics Board (REB), guidance from the Citizen Lab's Senior Legal Advisor, and review by University and/or external legal counsel. The Citizen Lab routinely works with vulnerable and at-risk individuals in the course of its research activities, including human rights defenders, journalists, refugees and asylum-seekers, and dissidents in high-risk countries. In many cases, these individuals have collaborated with the Citizen Lab on an anonymous or confidential basis in order to protect their safety and the safety of their collaborators and families. The Citizen Lab and its researchers take considerable precautions to protect these individuals.
16. In other words, the Citizen Lab ensures that its activities are carried out with the highest degree of professionalism, ethics, and integrity and has implemented numerous policies and procedures to ensure these standards are consistently met. This said, its research regularly relates to sensitive or rapidly developing political issues and operates in an emerging area of scholarship where norms are sometimes unclear. As is the case for all public interest technologists and security researchers, the Citizen Lab's research is therefore never entirely "risk free".

Previous Threats Against Citizen Lab

17. The nature of the Citizen Lab's work means that its activities are often considered adversarial by large, powerful corporations (such as those that develop surveillance and censorship technology) as well as by governments, including authoritarian regimes. A number of the Citizen Lab's research publications have also been critical of threats to *Charter*-protected rights posed by the Canadian federal government, as well as of Canadian administrative bodies, law enforcement agencies, and intelligence services.¹⁵
18. In other words, there is no shortage of actors who might prefer that the Citizen Lab not engage in the work that it does.

¹⁵ See e.g., Cynthia Khoo, Kate Robertson, and Yolanda Song. "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada," Citizen Lab and International Human Rights Program (Faculty of Law, University of Toronto), Research Report No. 131, September 2020; Petra Molnar and Lex Gill. "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System," Citizen Lab and International Human Rights Program (Faculty of Law, University of Toronto) Research Report No. 114, University of Toronto, September 2018; Jakub Dalek, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft, and Ron Deibert. "Planet Netsweeper," Citizen Lab Research Report No. 108, University of Toronto, April 2018.

19. Indeed, the Citizen Lab has been threatened with legal action to silence its work in the past. In January 2016, a company called Netsweeper Inc. filed a defamation suit before the Ontario Superior Court of Justice naming the University of Toronto and myself as defendants and seeking over \$3,500,000 in damages. The lawsuit pertained to an October 2015 Citizen Lab report which confirmed that Netsweeper Inc.'s Internet filtering products were being used to facilitate censorship amidst an armed conflict in Yemen under the direction of a group that has committed serious human rights violations.¹⁶
20. Had Netsweeper not discontinued its claim in its entirety in April 2016, we would have sought a stay of proceedings under Ontario's then newly-enacted *Protection of Public Participation Act* (PPPA), which protects defendants from litigation meant to intimidate or threaten public interest activities — sometimes called “strategic litigation against public participation” or “SLAPP suits”. The University, our counsel, and I nonetheless spent extensive time and resources preparing our statement of defence and other aspects of what we anticipated would be full legal proceedings.¹⁷ This was a costly, disquieting, and extremely stressful process that took up considerable time and resources in early 2016.
21. The Netsweeper litigation was also not the first time a company contemplated legal action regarding the Citizen Lab's work. Based on emails posted to Wikileaks in 2015 following a breach of the company's servers,¹⁸ we know that the Italian spyware vendor Hacking Team contacted a law firm to evaluate whether it would be possible to “hit [Citizen Lab] hard” — seeking to threaten the organization with damages, compel the removal of a research report, and force the identification of an anonymous source. The report which provoked these events analyzed certain Hacking Team's products and built upon previous work showing that so-called “lawful interception” technology is often used against political targets by repressive regimes, rather than against legitimate security threats.¹⁹
22. The Citizen Lab and its researchers have also faced other, non-legal threats. In 2019, for example, John Scott-Railton, a senior researcher at Citizen Lab, was targeted by an undercover agent which the *New York Times* linked to the Israeli private intelligence firm Black Cube. Bahr Abdul Razzak, another Citizen Lab researcher, had a similar encounter shortly before that incident.²⁰

The Criminal Code and the Security of Information Act

¹⁶ Jakub Dalek, Ronald Deibert, Sarah McKune, Phillipa Gill, Naser Noor, and Adam Senft. “Information Controls during Military operations: The case of Yemen during the 2015 political and armed conflict,” Citizen Lab Research Report No. 66, University of Toronto, October 2015.

¹⁷ See Ronald Deibert, “On Research in the Public Interest (A Statement from Professor Ronald Deibert), July 26, 2016.

¹⁸ Note that these leaks have no relation to Ms. Manning or her case.

¹⁹ Morgan Marquis-Boire, John Scott-Railton, Claudio Guarnieri, and Katie Kleemola, “Police Story: Hacking Team's Government Surveillance Malware,” Citizen Lab Research Report No. 41, University of Toronto, June 2014; Wikileaks, “Re: URGENT: Yet another Citizen Labs' attack” [Jun 24, 2014 email thread], Hacking Team Archive, 8 July 2015.

²⁰ See Ronen Bergman and Scott Shane, “The Case of the Bumbling Spy: A Watchdog Group Gets Him on Camera”, *The New York Times*, 28 January 2019.

i. The Criminal Code

23. I understand that one of the equivalent provisions cited by the Minister in Ms. Manning’s immigration proceedings is section 342.1 of the *Criminal Code*, “unauthorized use of a computer”.²¹
24. I have no personal knowledge of the facts of Ms. Manning’s case. However, I understand that she used a common software utility called Wget to download documents that were available to her and that she was authorized to access in the course of her work, but that this particular method of access was found to be prohibited by the applicable computer use policy.
25. As explained below, if section 342.1 of the *Criminal Code* (and in particular the phrase “fraudulently and without colour of right”) is interpreted to apply to actions like those undertaken by Ms. Manning, it could create serious practical uncertainties for technical researchers and chill public interest research, including that undertaken by the Citizen Lab.
26. This is because this interpretation would almost necessarily turn the violation of any corporate policy or contract into a criminal offence.
27. To understand the full consequences of this problem, it is important to understand that almost all commercial software is governed by some form of end-user license agreement (EULA), Terms of Use (ToU) or Terms of Service (ToS) document or similar contract. These documents are the primary tool governing the use of any given piece of software or technology. A few basic observations about these agreements:
 - a. They are generally subject to change and do in fact change frequently, generally at the unilateral discretion of the technology’s owner;

²¹ **Unauthorized use of computer**

- 342.1 (1)** Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction who, fraudulently and without colour of right,
- o (a) obtains, directly or indirectly, any computer service;
 - o (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system;
 - o (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system; or
 - o (d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c).

- b. They are often lengthy, drafted in extremely broad or vague language, and make reference to general principles that are open to many different reasonable interpretations;
 - c. They often include blanket provisions prohibiting almost any use of the technology in question other than for a narrowly, opaquely, or entirely undefined “intended” purpose;
 - d. They are rarely litigated or interpreted by courts, leaving their meaning generally indeterminate or uncertain;
 - e. They are sometimes drafted by unsophisticated actors or by parties that have marginal interest in producing a coherent legal document;
 - f. They are often drafted pursuant and subject to the laws of foreign jurisdictions, including jurisdictions that Canadians would generally consider as having authoritarian governments or weak human rights protections; and,
 - g. They often incorporate the law of foreign jurisdictions.
28. Most technical research involves the use of multiple programs, tools, and technologies to observe and analyze a system, sometimes in complex, overlapping, and interacting ways. Many of these technologies are designed and developed by third parties. For example, researchers at the Citizen Lab routinely make use of technologies such as:
- a. Network monitoring technologies and techniques, measurement tools, and software used to analyze traffic and detect suspicious or irregular activity on a network;
 - b. Various programs, scripts, and software in order to automate tasks, such as the collection of images, text and data from the web in bulk, some of which are analogous to Wget;
 - c. Programs that perform various tests to determine how a computer system, mobile application or website responds to particular inputs and external factors;
 - d. Anonymity and circumvention technology, which allows researchers to study Internet filtering and censorship and better understand what the Internet looks like to users elsewhere in the world.
29. Without these technologies — which are common, ubiquitous, beneficial, and used by computer scientists and researchers worldwide — the Citizen Lab’s work would simply not be possible.
30. As mentioned above, the Citizen Lab conducts extensive due diligence in relation to its research activities. However, the reality of the contractual ecosystem described above means that researchers can almost *never* be certain that their actions will not be opportunistically interpreted as a violation of a company’s standard form agreement in order to intimidate or discourage future research.

31. As a result, any interpretation of section 342.1 of the *Criminal Code* which would define a violation of a policy or contractual as “fraudulent” or “without colour of right” would inject extraordinary risk and indeterminacy into the Citizen Lab’s work. It would also allow any number of private actors to accuse the Citizen Lab of a criminal offence or discredit the organization on the basis of dubious allegations of contractual breach in order to prevent the organization from doing its important work.

ii. The Security of Information Act

32. I would also like to briefly comment on the *SOIA* issue in this case and its implications for the Citizen Lab’s work. I understand that the other equivalent provision cited by the Minister in Ms. Manning’s immigration proceedings is subsection 16(2) of *SOIA*.²² I understand that unlike other provisions of *SOIA*, there is no “public interest” or “whistleblower” defence or exception for this provision.

33. Counsel for Ms. Manning have informed me that it is possible that the Minister will take the position that Wikileaks was, at the relevant time, a “foreign entity or terrorist group”. I have no direct, personal knowledge on that issue.

34. However, I have been asked to comment on the Minister’s alternative argument that communicating protected information directly to the public or providing it to a third party (such as a journalist) who then publishes that information would be sufficient to constitute communication “to a foreign entity or to a terrorist group” — the logic being that those individuals could then access the information through public channels.

35. In addition to the obvious implications for press freedom, this interpretation would be the source of considerable concern and apprehension among the Citizen Lab’s staff and affiliates, who sometimes use, rely on, analyze, and communicate leaked or sensitive documents in the course of their legitimate research activities.

36. For example, individuals employed by or affiliated with the Citizen Lab have, in the course of their research activities, republished and linked to leaked documents disclosed by the American whistleblower Edward Snowden.²³ These documents constitute essential

²² **Communicating safeguarded information**

(2) Every person commits an offence who, intentionally and without lawful authority, communicates to a foreign entity or to a terrorist group information that the Government of Canada or of a province is taking measures to safeguard if

(a) the person believes, or is reckless as to whether, the information is information that the Government of Canada or of a province is taking measures to safeguard;

and

(b) harm to Canadian interests results.

Punishment

(3) Every person who commits an offence under subsection (1) or (2) is guilty of an indictable offence and is liable to imprisonment for life.

²³ See e.g., *Canadian SIGINT Summaries*, analysis of Canadian documents related to the Communications Security Establishment prepared by Dr. Christopher Parsons:

primary materials for researchers in the areas of national security law, international relations, political science, surveillance studies, and other fields directly related to the Citizen Lab's work.

37. I should note that some of the documents in the Snowden archive originated from the Canadian government, and in particular from the Communications Security Establishment (CSE). At least some of these documents are classified as “top secret” — in other words, they would have been considered “information that the Government of Canada or of a province is taking measures to safeguard” under *SOIA*.
38. The Citizen Lab is also sometimes consulted by the press to understand the technical aspects and legal issues associated with leaked documents. For example, I have been consulted to review documents leaked by Edward Snowden and obtained by CBC News in the past prior to publication. I reviewed these documents — as have presumably countless people who downloaded them from the public web or from a news website like the CBC — and I communicated about them to the press and the public when providing commentary and analysis.²⁴
39. I understand that for the above-mentioned activities to attract criminal liability under the provision in question — even under the extreme interpretation that may be offered by the Minister — “harm to Canadian interests” would need to result. However, this concept appears to be defined in extremely broad and ambiguous terms in the law.²⁵ It is therefore

<https://christopher-parsons.com/writings/cse-summaries/> and *Lux ex Umbra*, the blog of Citizen Lab fellow Bill Robinson: <https://luxexumbra.blogspot.com/>.

²⁴ See for example: Greg Weston, “CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents”, *CBC News*, 30 January 2014, link to document published by CBC: https://www.cbc.ca/news2/pdf/airports_redacted.pdf; Dave Seglins, “CSE tracks millions of downloads daily: Snowden documents”, *CBC News*, 2 April 2015, link to document published by CBC: <https://www.documentcloud.org/documents/1510163-cse-presentation-on-the-levitation-project.html>.

²⁵ **Prejudice to the safety or interest of the State**

3 (1) For the purposes of this Act, a purpose is prejudicial to the safety or interests of the State if a person

- (a) commits, in Canada, an offence against the laws of Canada or a province that is punishable by a maximum term of imprisonment of two years or more in order to advance a political, religious or ideological purpose, objective or cause or to benefit a foreign entity or terrorist group;
- (b) commits, inside or outside Canada, a terrorist activity;
- (c) causes or aggravates an urgent and critical situation in Canada that
 - (i) endangers the lives, health or safety of Canadians, or
 - (ii) threatens the ability of the Government of Canada to preserve the sovereignty, security or territorial integrity of Canada;
- (d) interferes with a service, facility, system or computer program, whether public or private, or its operation, in a manner that has significant adverse impact on the health, safety, security or economic or financial well-being of the people of Canada or the functioning of any government in Canada;

difficult to understand with any degree of certainty what kind of communication might eventually be considered illegal under the *SOIA*. Indeed, in my experience, the full spectrum of potential consequences of any given news story, public comment, or research report are often impossible to predict in advance.

40. This is compounded by the fact that the provision contains other vague and indeterminate language, such as the phrase “information that the Government of Canada or of a province is taking measures to safeguard”. It is also unclear how this definition would apply to situations where the government has “taken measures to safeguard” information but has ultimately failed to protect it — such as where public interest researchers disclose a vulnerability in the government’s technical infrastructure that exposes the public to risk.

-
- (e) endangers, outside Canada, any person by reason of that person’s relationship with Canada or a province or the fact that the person is doing business with or on behalf of the Government of Canada or of a province;
 - (f) damages property outside Canada because a person or entity with an interest in the property or occupying the property has a relationship with Canada or a province or is doing business with or on behalf of the Government of Canada or of a province;
 - (g) impairs or threatens the military capability of the Canadian Forces, or any part of the Canadian Forces;
 - (h) interferes with the design, development or production of any weapon or defence equipment of, or intended for, the Canadian Forces, including any hardware, software or system that is part of or associated with any such weapon or defence equipment;
 - (i) impairs or threatens the capabilities of the Government of Canada in relation to security and intelligence;
 - (j) adversely affects the stability of the Canadian economy, the financial system or any financial market in Canada without reasonable economic or financial justification;
 - (k) impairs or threatens the capability of a government in Canada, or of the Bank of Canada, to protect against, or respond to, economic or financial threats or instability;
 - (l) impairs or threatens the capability of the Government of Canada to conduct diplomatic or consular relations, or conduct and manage international negotiations;
 - (m) contrary to a treaty to which Canada is a party, develops or uses anything that is intended or has the capability to cause death or serious bodily injury to a significant number of people by means of
 - (i) toxic or poisonous chemicals or their precursors,
 - (ii) a microbial or other biological agent, or a toxin, including a disease organism,
 - (iii) radiation or radioactivity, or
 - (iv) an explosion; or
 - (n) does or omits to do anything that is directed towards or in preparation of the undertaking of an activity mentioned in any of paragraphs (a) to (m).

Harm to Canadian interests

- (2) For the purposes of this Act, harm is caused to Canadian interests if a foreign entity or terrorist group does anything referred to in any of paragraphs (1)(a) to (n).

41. The potential breadth, uncertainty, and indeterminacy of this provision is, of course, all the more chilling given that it carries a risk of life imprisonment.

Consequences of the Minister's Interpretation

42. The mere possibility that either of the *SOLA* or *Criminal Code* provisions discussed above could apply to individuals engaged in the kind of public interest research I have described in my statement would doubtlessly impact the Citizen Lab's activities and its approach to legal threats. While the organization anticipates a certain degree of risk arising from foreign actors and the private sector, the threat of criminal sanction from our own government would raise distinct and serious concerns for academic freedom, freedom of the press, and research in the public interest.
43. Indeed, even the most unfounded criminal investigation or criminal charge in relation to the Citizen Lab's work would result in a significant financial and administrative burden that the organization is ill-equipped to bear. Depending on the context, developments of this nature could also jeopardize the Citizen Lab's continued funding and professional standing in the research community. In all cases, it would result in lost research time and significant distress. In some cases, the continued operation and long-term survival of the Citizen Lab could even be at stake.
44. In addition to the additional administrative and legal burden these new forms of criminal liability would impose on the Citizen Lab, it is essential to note that our ability to conduct certain forms of research would be directly threatened. Based on my professional experience, vulnerable individuals, sources, and informants would be far less likely to contact the Citizen Lab if they believed their involvement could give rise to criminal proceedings. Many of the Citizen Lab's most valuable sources and collaborators reside in or come from countries with authoritarian governments that routinely persecute civil society actors like scholars and journalists. To operate effectively, the Citizen Lab must be in a position to unambiguously and confidently reassure these individuals that they will be protected.
45. Additionally, the Citizen Lab routinely collaborates with other civil society groups (like Amnesty International, Human Rights Watch, Forbidden Stories, and the Open Observatory of Network Interference) and industry partners (such as the Microsoft Threat Intelligence Center). The Citizen Lab also receives in-kind donations of investigative tools from companies like RiskIQ/PassiveTotal, HYAS, VirusTotal, Cisco's AMP Threat Grid Team, and others. In a context where the risk of these technologies for public interest research could plausibly give rise to criminal sanctions, many of the Citizen Lab's collaborations and industry partnerships could dry up.
46. The chilling effect caused by these new risks would not be limited to our organization. Though distinct, the work that the Citizen Lab engages in is similar in some respects to the work carried out by investigative journalists. In my view, it is therefore difficult to see how any increased risk of criminal liability for Citizen Lab researchers would not also translate to greater risks for members of the press.

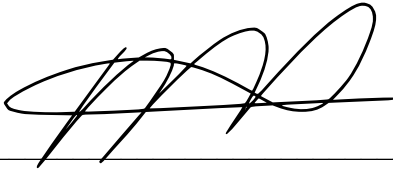
47. Additionally, there are several other organizations that engage in public interest technology research using methods similar to those employed by the Citizen Lab. The Citizen Lab is nonetheless one of the most established and well-resourced organizations of this nature worldwide. If it is understood that technical researchers in Canada are not safe from criminal sanction by their own government, I believe that this message would reverberate in other jurisdictions, giving credibility to states that use the criminal law to threaten scholars, dissidents, journalists, and human rights defenders.
48. As Director of the Citizen Lab, I am also aware that certain members of our community face even greater harm if they were to be subject to a criminal charge or investigation in relation to their work. For example:
- a. Not all researchers associated with the Citizen Lab are Canadian citizens. Over the years, some individuals have worked with the organization on study visas through the University of Toronto. Others are permanent residents or refugees or in the process of seeking refugee status in Canada. I understand that a criminal charge could jeopardize an individual's ability to remain in Canada, sometimes at great personal risk.
 - b. Former students, employees, and affiliates of the Citizen Lab have gone on to work for the Canadian government, including in roles associated with national security and intelligence. I understand that a criminal charge or association with an organization that has been linked to criminal conduct can compromise an individual's ability to secure employment or the necessary clearances required to work for the government or certain contractors.
 - c. The Citizen Lab has hosted several law students and has several fellows who are former or current practicing lawyers. I understand that lawyers are subject to "good character" requirements and are generally required to report criminal charges against them to their professional association. I also understand that a criminal charge can carry serious professional consequences for these individuals, and in some cases threaten their ability to practice.
49. As Director of the Citizen Lab, I feel responsible to these individuals and decisions about organizational and research risk are taken with these constraints in mind.
50. I also believe deeply in the importance of free, open, and independent scholarship that contributes to pursuit of knowledge and the public interest. It is essential that scholars in Canada and around the world can contribute to the advancement of their respective disciplines without fear of legal or extralegal interference, intimidation, or reprisal, whether by the state or private actors. These principles are affirmed and protected by the Canadian *Charter* and under international human rights law.
51. The Citizen Lab remains unwaveringly committed to its academic and public interest research mandate. However, it must be acknowledged that the Citizen Lab does not have unlimited resources and that prior experiences have made our organization more cautious. In recent years, significant administrative resources have been marshaled to ensure that

research activities are reviewed and controlled for the risk of strategic litigation and extralegal threats intended to silence or intimidate researchers — in some cases adding significant cost, complexity, and delay to the research process.

52. If the *Criminal Code* or the *SOIA* were interpreted by administrative decision-makers or the courts in a manner that criminalized public interest technical research and reporting — or even interpreted in a manner that caused significant legal uncertainty about the lawfulness of those activities — there is no doubt that it would have an impact on our organization.

53. In some scenarios, it could even mean that certain public interest research would be abandoned, that some projects would become financially out of reach, or that important stories would remain untold. Practically speaking, such a development would represent a victory for autocrats, censors, and the vendors of rights-violating technology everywhere, who might prefer that their activities remain unexamined by organizations like ours.

And I have signed on this 16th day of October, 2021*

A handwritten signature in black ink, consisting of several loops and a long horizontal stroke at the end, positioned above a solid horizontal line.

Dr. Ronald J. Deibert

*Statement of September 21st, 2021 revised to correct minor error at paragraph 10.