Submission to the Standing Committee on Access to Information, Privacy, and Ethics

Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto), 11 August 2022

For all inquiries related to this submission, please contact:

Dr. Ronald J. Deibert, Director, The Citizen Lab, Munk School of Global Affairs
Professor of Political Science, University of Toronto
r.deibert@utoronto.ca

Contributors to this report (in alphabetical order):

Siena Anstis (Senior Legal Advisor, The Citizen Lab)
Dr. Ronald J. Deibert (Professor of Political Science, University of Toronto; Director, The Citizen Lab)
Angela Yang (Legal Intern, The Citizen Lab)

Introduction

The Citizen Lab wishes to draw the House of Commons' Standing Committee on Access to Information, Privacy, and Ethics attention to the following issues associated with government use of spyware:

(1) The unique technological capabilities of spyware;[1]
(2) The human rights, public, and national security risks associated with spyware and the unregulated nature of the mercenary spyware industry; and,

[1] The RCMP's description of the capabilities of "on-device investigative tools" (ODITs) shows that ODITs have the same or similar capabilities as spyware. We use the term spyware or mercenary spyware in this submission.

(3) The need for public debate and the development of a specific legal framework for the use of spyware by government agencies.

Further, we lay out initial recommendations for how the Canadian government should begin to address the use of spyware by government agencies like the Royal Canadian Mounted Police (RCMP).

The unique technological capabilities of spyware and the unregulated nature of the mercenary spyware industry

<u>The unique technological capabilities of spyware</u>

Spyware is a form of malware that allows an operator to gain access to—or "hack"—a device and extract, modify, or share its contents. Spyware may also sometimes be referred to as "government hacking" technology, "intrusion software," "offensive cyber capabilities," or "access as a service."[2] Spyware relies on the exploitation of flaws in software code that leave widely used applications and operating systems highly vulnerable, such as flaws in WhatsApp or iOS.[3] Devices can be infected with spyware through several different vectors: (1) socially-engineered exploit links which a targeted user has to click on before the device is infected, (2) "zero-click" exploits, which require no user interaction to install the spyware and thus lead to the silent infection of a targeted device, (3) or manual installation, if a device is physically seized.[4]

[2] Winnona DeSombre et al, "Countering Cyber Proliferation: Zeroing in on Access-as-a-Service" (March 2021), *Atlantic Council* <https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/>; Sven Herpig, "Government Hacking: Global Challenges" (Jan 2018), <https://www.stiftung-nv.de/sites/default/files/government_hacking_akt.feb_.pdf>.

[3] The Citizen Lab, "NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases" (Oct 2019), <https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/>; Bill Marczak et al, "FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild" (Sept 2021), <https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/>.

[4] Bill Marczak et al, "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit" (Dec 2020), <https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/> at 2; Bill Marczak et al, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries" (Sept 2018),

Depending on the sophistication of the spyware, an infection may give the perpetrator full access to a target's device. The Citizen Lab has reported that an infection with NSO Group's Pegasus spyware gives operators access to all of the targeted phone's content and passwords, including emails and SMS messages, as well as the ability to download files, listen to telephone calls, track the target's location, and remotely turn on the microphone and camera.[5] These infections can successfully target encrypted calls and messages.[6]

The rapid proliferation of spyware around the world and its use by government agencies is a cause for alarm. In June 2019, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression called for a moratorium on the sale, transfer, and use of spyware.[7] In February 2022, the European Data Protection Supervisor (EDPS) stated that a complete ban of Pegasus or similar spyware was the most effective way to protect fundamental rights and freedoms which are seriously imperiled by this technology.[8] In March 2022, the European Parliament instituted a committee to study potential infringements of EU law through governments' use of Pegasus and related spyware.[9] In July 2022, the United States House of Representatives Permanent Select Committee on Intelligence held a hearing on commercial cybersurveillance and introduced a bi-partisan bill containing new rules further strengthening regulation around the mercenary spyware industry.[10] The US

<https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> at 7.

[5] *Ibid*.

[6] The Citizen Lab, "Would You Click?" (2022), <https://catalonia.citizenlab.ca/>.

[7] OHCHR, "UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools" (June 2019), <https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance>.

[8] EDPS, "Preliminary Remarks on Modern Spyware" (Feb 2022), <https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf> at 9.

[9] PEGA Committee, "About" (2022), <https://www.europarl.europa.eu/committees/en/pega/about>.

[10] US House Intelligence Committee, "Chairman Schiff Delivers Opening Statement at House Intelligence Committee Open Hearing on Commercial Cyber Surveillance" (July 2022), <https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=1211>; US House Intelligence

Biden Administration has already taken several measures to try and curb the industry, including placing NSO Group and Candiru, another mercenary spyware firm, on the Department of Commerce's Entity List.[11]

The unregulated nature of the mercenary spyware industry

The mercenary spyware industry is characterized by private actors selling spyware products and services to clients that include government intelligence, law enforcement, and security services. From the little we know publicly, the industry appears to have thrived over the course of the last decade, as states are increasingly buying and using surveillance technology.[12] At the same time, almost every aspect of this industry is cloaked in secrecy, from who buys and sells the products,[13] to the secret trade shows

Committee, "Chairman Schiff, Ranking Member Turner Laud Passage of 2023 Intelligence Authorization Act" (July 2022), <https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=1209>; Amendment in the Nature of a Substitute to H.R. 8367 (Jul 2022), <https://intelligence.house.gov/uploadedfiles/iaa_ans_xml.pdf>.

[11] US Department of Commerce, "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities" (Nov 2021), <https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list>; "United States Makes Efforts to Curb Misuse of Surveillance Technology" (2022) 116:2 AJIL 426.

[12] Ronan Farrow, "How Democracies Spy on Their Citizens," *The New Yorker* (April 2022), <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>; UN Human Rights Council (2019), "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," 41st Sess, UN Doc A/HRC/41/35 at para 6; Ron Deibert, "Protecting Society From Surveillance Spyware" (2022) 38:2 Issues Sci & Tech <https://issues.org/surveillance-spyware-uso-group-pegasus-citizen-lab/>.

[13] See e.g. Merlin Delcid, "El Salvador Denies Responsibility for Hacking Journalists After Report Finds Pegasus Spyware on their Phones," *CNN World* (Jan 2022) <https://www.cnn.com/2022/01/13/americas/el-salvador-pegasus-spyware-intl/index.html>; Justin Spike, "Hungarian official: Government bought, used Pegasus spyware" (Nov 2021), *AP News,* <https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0>; Vanessa Gera, "Polish leader admits country bought powerful Israeli spyware" (Jan 2022), *AP News,* <https://apnews.com/article/technology-business-software-spyware-jaroslaw-kaczynski-0c41a504e8fbdbb6b9b06f6869848a48>; Panu Wongcha-um, "Thailand admits to using phone spyware, cites national security" (July 2022), *Reuters* <https://www.reuters.com/world/asia-pacific/thailand-admits-using-phone-spyware-cites-national-security-2022-07-20/>; Joseph Wilson, "Catalan: Spain spy chief admits legally hacking some phones" (May 2022), *AP News*

which promote the spyware,[14] to the names of the spyware companies.[15] Companies who sell spyware tend to operate using complex sales structures including multiple corporate entities operating from a range of countries, making it difficult to monitor and report on their activities, in particular where companies are applying for and receiving export licences.[16]

Spyware companies typically deflect criticism by framing their technology as tools to combat terrorism and crime.[17] NSO Group has repeatedly stated that they sell their product exclusively to governments for use against terrorists and major criminals as both a justification and a marketing tactic.[18] However, reports by the Citizen Lab, civil society organizations, technology platforms, and journalists paint a different picture: hundreds of journalists, opposition politicians, lawyers, activists, and family members have been routinely and repeatedly hacked.[19] NSO Group is not the only spyware

<https://apnews.com/article/technology-europe-barcelona-spain-hacking-38dcf5392b273f8e8447b0a9f62ed2f5>.

[14] Ilya Lozovsky, "Where NSO Group Came From – And Why It's Just the Tip of the Iceberg," *OCCRP* (July 2021) <https://www.occrp.org/en/the-pegasus-project/where-nso-group-came-from-and-why-its-just-the-tip-of-the-iceberg>.

[15] See e.g. Bill Marczak et al, "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus," (2021), <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/> ("Candiru" has changed its name to "DF Associates Ltd.," "Grindavik Solutions Ltd.," "Taveta Ltd.," and "Saito Tech Ltd.").

[16] *Ibid* (Candiru "makes efforts to keep its operations, infrastructure, and staff identities opaque to public scrutiny."); Amnesty International, Privacy International & the Centre for Research on Multinational Corporations, "Operating from the Shadows: Inside NSO Group's Corporate Structure" (May 2021), <https://www.amnesty.org/en/documents/doc10/4182/2021/en/>; Ronald J Deibert, "Subversion Inc: The Age of Private Espionage" (2022) 33:2 J Democracy 28.

[17] The Citizen Lab, *supra* note 3; Bill Marczak et al, "Mapping Hacking Team's 'Untraceable' Spyware" (2014), <https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/>.

[18] Frank Bajak, "Probe: Journalists, activists among firm's spyware targets" (July 2021), *AP News* <https://www.cbc.ca/news/world/spyware-journalists-activists-1.6108070>.

[19] The Citizen Lab, "Targeted Threats Archives", <https://citizenlab.ca/tag/targeted-threats/>; Amnesty International, "Pegasus Project: Rwandan Authorities Chose Thousands of Activists, Journalists and Politicians to Target with NSO Spyware" (2021), <https://www.amnesty.org/en/latest/news/2021/07/rwandan-authorities-chose-thousands-of-activists-journalists-and-politicians-to-target-with-nso-spyware/>.

company with significant discrepancies between their affirmation for human rights and business practices.[20]

There is very little regulation of the mercenary spyware industry at domestic or international levels, allowing this sector to operate largely without scrutiny. The main regulatory requirement in Canada and a number of other jurisdictions is that companies should apply for licenses to export dual-use technology.[21] However, export controls have been criticized as inadequate in addressing human rights concerns associated with spyware.[22] For example, Israeli dual-use export controls appear to be focused less on minimizing harm and misuse than on promoting strategic interests.[23]

Beyond the regulation of dual-use exports, there is no specific regime addressing the international trade of spyware and few countries have adopted domestic legislation that specifically covers the use of spyware by government bodies such as law enforcement and intelligence agencies.[24] In recent years, civil society has argued that

[20] See e.g. Alex Hern, "Hacking Team Hack Casts Spotlight on Murky World of State Surveillance" (July 2015), *The Guardian* <https://www.theguardian.com/technology/2015/jul/11/hacking-team-hack-state-surveillance-human-rights>.

[21] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, "Public Documents: Volume II, List of Dual-Use Goods and Technologies and Munitions List" (Dec 2021), <https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-II-2021-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-2021.pdf>.

[22] Sarah McKune & Ron Deibert, "Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking" (March 2017), <https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf>; Heejin Kim, "Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue" (2021) 70:2 ICLQ 379 at 380; Siena Anstis & RJ Reid, "The Adverse Human Rights Impacts of Canadian Technology Companies: Reforming Export Control with the Introduction of Mandatory Human Rights Due Diligence" (2021) CJLT, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3894947>.

[23] Ronen Bergman & Mark Mazzetti, "Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia" (March 2022), *New York Times* <https://www.nytimes.com/2022/03/23/us/politics/pegasus-israel-ukraine-russia.html>; Ronen Bergman & Mark Mazzetti, "The Battle for the World's Most Powerful Cyberweapon" (Jan 2022), *New York Times* <https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html>.

[24] See e.g. Kim, *supra* note 22; Jonathon W Penney & Bruce Schneier, "Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group" (2022) 36:1 BTLJ 469.

governments–including democratic ones–need to adopt specific rules for the use of spyware because of its susceptibility for abuse and its unique and powerful technological capabilities.[25]

There are serious human rights, public, and national security risks associated with government use of spyware and the mercenary spyware industry.

Spyware poses serious risks to human rights

Both authoritarian and democratic governments use spyware in a manner that violates human rights through the targeting of human rights defenders, activists, journalists, and members of the political opposition.[26] In April 2022, the Citizen Lab uncovered that spyware was used to target or infect the phones of at least 65 Catalan activists and politicians as well as their friends, families, and associates between 2015 and 2020.[27] Pegasus spyware was also used to infect the devices of Polish government critics.[28] Spyware has been deployed by the Greek government to track journalists and a politician.[29]

[25] See e.g. EDPS, *supra* note 8; Privacy International, "Hacking Necessary Safeguards," <https://privacyinternational.org/demand/government-hacking-safeguards>; Amnesty International, "Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology" (July 2021), <https://www.amnesty.org/en/documents/doc10/4516/2021/en/>.

[26] Marczak et al, "Hide and Seek", *supra* note 4 at 8-10; Amnesty International, *supra* note 19.

[27] John Scott-Railton et al, "CatalanGate: Extensive Mercenary Spyware Operation Against Catalans Using Pegasus and Candiru" (2022), <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>.

[28] Stephanie Kirchgaessner, "More Polish Opposition Figures Found to Have Been Targeted by Pegasus Spyware" (Feb 2022), *The Guardian* <https://www.theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware>.

[29] International Press Institute, "Greece: Journalist Thanasis Koukakis surveilled for 10 weeks with powerful new spyware tool" (Apr 2022), <https://ipi.media/greece-journalist-thanasis-koukakis-surveilled-for-10-weeks-with-powerful-new-spyware-tool/>; France 24, "Surveillance of opposition leader was 'unacceptable': Greek PM" (Aug 2022), *France 24* <https://www.france24.com/en/live-news/20220808-surveillance-of-opposition-leader-was-unacceptable-greek-pm>.

These cases–which provide just a snapshot into the human rights harms associated with spyware–show that this technology is susceptible to abuse in all political contexts. Its use against political opposition, human rights defenders, journalists, and activists is particularly troubling and presents a serious threat to human rights, democracy, and rule of law. The possibility of abuse in the hands of the RCMP is real, in particular in light of the institution’s history of surveillance abuses and discriminatory practices.[30]

Spyware poses serious risks to national and public security

Spyware is not only used against civil society by government agencies. Spyware is also used by governments to spy on other governments, presenting significant national and international security risks. French President Emmanuel Macron and a device in Prime Minister Boris Johnson’s office were targeted by Pegasus spyware.[31] In May 2022, it was reported that the devices of Spanish Prime Minister Pedro Sánchez and Defense Minister Margarita Robles were infected with Pegasus. Moreover, spyware intended for government use does not always remain in the hands of governments. Reports by *The Guardian* indicate that some Mexican government officials helped Mexican drug cartels procure mercenary spyware, including spyware by NSO Group and Hacking Team.[32]

[30] See e.g. Catharine Tunney, “Watchdog finds RCMP's policing of anti-pipeline protesters reasonable — but sees gaps in surveillance policies” (Dec 2020), *CBC* <https://www.cbc.ca/news/politics/crcc-pipeline-protest-surveillance-1.5841752>; Catharine Tunney, “RCMP's use of facial recognition tech violated privacy laws, investigation finds” (June 2021), *CBC* <https://www.cbc.ca/news/politics/rcmp-clearview-ai-1.6060228>; Standing Committee on Public Safety and National Security, “Systemic Racism in Policing in Canada” (June 2021), <https://www.ourcommons.ca/Content/Committee/432/SECU/Reports/RP11434998/securp06/securp06-e.pdf>.

[31] Daniel Boffey, “EU Data Watchdog Calls for Pegasus Spyware Ban” (Feb 2022), *The Guardian* <https://www.theguardian.com/world/2022/feb/15/eu-data-watchdog-calls-for-pegasus-spyware-ban>; Ron Deibert, “UK Government Officials Infected with Pegasus” (2022), *The Citizen Lab* <https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/>.

[32] Cecile Schilis-Gallego & Nina Lakhani, “’It’s a Free-for-All’: How Hi-Tech Spyware Ends up in the Hands of Mexico’s Cartels” (Dec 2020), *The Guardian* <https://www.theguardian.com/world/2020/dec/07/mexico-cartels-drugs-spying-corruption>; “The Pegasus project part 3: cartels, corruption and cyber-weapons” (July 2021), (podcast) *The Guardian* <https://www.theguardian.com/news/audio/2021/jul/21/the-pegasus-project-part-3-cartels-corruption-and-cyber-weapons-podcast>.

There are also public security risks associated with the mercenary spyware market. The mercenary spyware industry is founded on the discovery and exploitation of software flaws that software vendors themselves are unaware of or have not patched.[33] These software flaws exist in applications and operating systems that are widely used across the world, and thus leave millions of people vulnerable to illegal surveillance. Further, the uncontrolled proliferation of this technology fuels a global market that prioritizes collective digital insecurity.[34]

There needs to be a public debate on the use of this technology by government agencies and the elaboration of a specific legal framework.

Research and investigations by the Citizen Lab and other organizations have revealed that governments around the world have purchased and used spyware against their citizens. The covert adoption of this technology and the discovery of countless cases of abuse has caused a loss of public confidence, and led to the resignation of or dismissal of several government officials.[35] The highly intrusive nature of this technology and the threat it poses to human rights, democracy, and rule of law calls for public debate in Canada on whether its use is appropriate in a democratic society and, if so, what limitations must be enacted.[36]

Initial recommendations to the Canadian government

[33] See e.g. Marczak et al, *supra* note 3; Marczak et al, *supra* note 15 .

[34] Jonathan Berr, ""WannaCry" ransomware attack losses could reach $4 billion" (May 2017), *CBC* <https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/>.

[35] See e.g. Belén Carreño & Inti Landauro, "Spain's spy chief sacked over Pegasus case" (May 2022), *Reuters* <https://www.reuters.com/world/europe/spains-spy-chief-sacked-over-pegasus-case-el-pais-reports-2022-05-10/>; Tasos Kokkinidis, ""Greece's Intelligence Chief Resigns Amid Phone-Tapping Scandal" (Aug 2022), *Greek Reporter* <https://greekreporter.com/2022/08/05/greece-spy-chief-resigns-phone-tapping-fiasco/>.

[36] Privacy International, *supra* note 25; UN Human Rights Council, *supra* note 12; EDPS, *supra* note 8; Amnesty International, *supra* note 25.

1. Issue statements at the highest levels that Canada takes seriously the threat to democracy and rule of law posed by spyware and its associated industry.
2. Hold public hearings on the risks and threats of spyware and its associated industry to Canadian society and fundamental rights and freedoms.
3. Mandate privacy impact assessments by government agencies who want to use new surveillance technologies and make these assessments public.
4. If there is consensus–after public debate–that government agencies like the RCMP are going to use spyware, develop a legal framework for the use of this technology that is compliant with the *Charter*/international human rights law and is calibrated to its highly invasive nature and the risks it entails.
5. Ensure that government agencies are subject to independent oversight in the procurement, use, and deployment of spyware.
6. Ensure a high-level of transparency in government use of spyware in order to facilitate public accountability.
7. Ensure that Canadian surveillance technology is not exported to jurisdictions that may abuse these technologies.
8. Mandate greater transparency in Canada's export of surveillance technologies through proactive disclosure of what Canadian companies are exporting and to what jurisdictions.
9. Impose regulatory penalties on mercenary spyware firms that are known to facilitate human rights bans abroad.
10. Impose a lifetime ban for those who have worked in the Canadian intelligence and law enforcement agencies from working with mercenary spyware firms.

About the Citizen Lab

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, 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.[37]

[37] The Citizen Lab, <https://citizenlab.ca/>.