Submission of the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) to the National Security and Intelligence Committee of Parliamentarians (NSICOP)

June 30, 2023

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; Director, The Citizen Lab)
Camila Franco (Legal Extern, The Citizen Lab)
Zoe Panday (Research Assistant, The Citizen Lab)

Acknowledgements:

Thank you to Michelle Akim (Legal Intern, The Citizen Lab) and Snigdha Basu (Communications Specialist, The Citizen Lab) for formatting and copy editing.

TABLE OF CONTENTS

Introduction **3**

Mercenary Spyware **4**

Technical Functions and Capabilities 4

Market Features 6

Selected Companies 8

NSO Group 9

Candiru (Saito Tech) 11

Cytrox 11

QuaDream 12

Concerns Raised by Mercenary Spyware **12**

National Security 12

Human Rights 14

Democracy and the Rule of Law 16

US and EU Responses to Mercenary Spyware **18**

United States 18

European Union and Member States 21

The Threat of Mercenary Spyware to Canadian National Security **23**

Threats Arising From Government Use of Spyware 24

Threats Arising From Proliferation of Mercenary Spyware 27

Conclusion and Recommendations **29**

Introduction

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

The Citizen Lab adopts a mixed-method approach to its research which incorporates methods from computer science, law, political science, and area studies. Research areas include investigating digital espionage against civil society; documenting Internet filtering and other technologies and practices that impact freedom of expression online; analysing privacy, security, and information controls of popular publications; and examining transparency and accountability mechanisms relevant to the relationship between state agencies and corporations regarding personal data and other surveillance activities.

Research by the Citizen Lab on the use of spyware by state actors shows that this technology is abused by governments and results in human rights violations and serious risks to national security, democracy, and the rule of law. Spyware abuses are not limited to authoritarian regimes, but are also committed by democratic and quasi-democratic states against journalists, members of the political opposition, human rights defenders (HRDs), lawyers, and civil society.

The Citizen Lab welcomes this opportunity to submit a report to the National Security and Intelligence Committee of Parliamentarians (NSICOP) on the growing threat of mercenary spyware, an issue which has received limited attention by Canadian policymakers to date. The scope of this submission is three-fold:

1. Provide an overview of the technical features of mercenary spyware and key players in the market and highlight relevant sources. This section will identify key concerns around mercenary spyware and challenges in regulating the industry;

2. Review abuses of spyware at the international level, notably its deployment against HRDs, civil society, journalists, and members of political opposition. We will discuss risks related to spyware proliferation, with a particular focus on concerns related to human rights, democracy, the rule of law, and national security. We will examine existing and proposed legislative or policy initiatives (as of May 15, 2023) intended to address spyware proliferation in the European Union (EU) and the United States (US); and,

3. Summarise risks to human rights, democracy, and the rule of law in Canada that arise from the use of spyware by Canadian government agencies and institutions, as well as the national security risks that the Government of Canada has to contend with in the face of the unchecked global proliferation of mercenary spyware.

Mercenary Spyware

Technical Functions and Capabilities

Spyware is a form of malware (i.e., malicious software) that allows an operator—such as a government intelligence agency—to gain access to an electronic device and extract, modify, or share its contents.[1] In Canada, "on-device investigative tools" (ODITs) used by the Royal Canadian Mounted Police (RCMP) have capabilities that are analogous to those of mercenary spyware.[2]

The use of the term "mercenary" in association with spyware indicates the willingness of companies in this market to sell their wares without concern for the potential abuse of such technology, e.g., in human rights abuses. It also underscores the role of the private sector in developing and supplying spyware to government agencies as well as in supporting their use of this technology through system set-up, training, maintenance, support, and upgrades – much like private security companies for hire.[3]

Spyware functions by exploiting flaws in software code (i.e., exploits) that leave popular applications and operating systems vulnerable to attack by a third party (e.g., WhatsApp and iOS).[4] In sophisticated spyware, these exploits are usually "zero-day" exploits, i.e., exploits which have yet to be discovered by the software manufacturer and can be surreptitiously exploited. Spyware like NSO Group's Pegasus spyware, discussed further on, is implanted on a targeted device after one or more exploits is used to gain unauthorised access to the operating system. NSO Group is known for using in-house resources to find exploits that presumably are not being sold on the public market for exploits. The 'exclusive' nature of these exploits is part of the high price tag that comes with mercenary spyware technology.

Electronic devices can be infiltrated through different vectors of infection: (1) socially engineered exploit links that trick a target into interacting with a link, which starts the process of downloading spyware to the device (e.g., clicking on a URL in a WhatsApp message); (2) "zero-click" exploits, which do not require interaction from the targeted user and thus enable

---

[1] Anstis, Siena, Ronald J. Deibert, and Angela Yang (2022), "Submission to the Standing Committee on Access to Information, Privacy and Ethics," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2022/08/Brief-to-the-House-of-Commons-Standing-Committee-on-Access-to-Information-Privacy-and-Ethics.pdf>.

[2] Standing Committee on Access to Information, Privacy and Ethics (2022), "Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues," *The House of Commons* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-e.pdf> at 19–20.

[3] See e.g., "Exhibit 1 through 11: *WhatsApp Inc. v. NSO Group Technologies Limited*" (Filed 10/29/2019) <https://www.courtlistener.com/docket/16395340/1/1/whatsapp-inc-v-nso-group-technologies-limited/> at Exhibit 10.

[4] The Citizen Lab (2019), "NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/>; Marczak, Bill, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ronald J. Deibert (2021), "FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/>.

the silent infection of a device; and (3) manual installation where the spyware is installed after a device is physically seized from the targeted user.[5] In addition to providing spyware and associated exploits, spyware companies may also provide additional services to government operators, such as assistance with hardware installation, systems training, and maintenance and support.[6]

Mercenary spyware provides government bodies with the ability to access and manipulate data on a targeted device.[7] This includes access to account passwords, cloud credentials (e.g., Apple accounts), files, contact lists, emails, calendar events, text messages (including encrypted messages that sit decrypted on the device), and photos.[8] Some spyware products can enable the operator to inject data onto a targeted device, making it possible for a state actor to plant incriminating or defamatory contents into a device remotely, and later rely on this content as evidence against an innocent target.[9] This intrusive technology also has the capability to silently activate a device's microphone and camera, and send live information

[5] Marczak, Bill, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ronald J. Deibert (2020), "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2020/12/great-ipwn-journalists-hacked-suspected-nso-group-imsg-zero-click-exploit/> at 2; Anstis, Siena, Ronald J. Deibert, Émilie LaFlèche, and Jon Penney (2022), "Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of-Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf> at 3–4; Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ronald J. Deibert (2018), "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2018/09/hide-seek-tracking-nso-groups-pegasus-spyware-to-operations-45-countries/> at 7.

[6] See e.g., "Exhibit 1 through 11: *WhatsApp Inc. v. NSO Group Technologies Limited,*" (Filed 10/29/2019) <https://www.courtlistener.com/docket/16395340/1/1/whatsapp-inc-v-nso-group-technologies-limited/> at Exhibit 10.

[7] Anstis, Siena, Ronald J. Deibert, Émilie LaFlèche, and Jon Penney (2022), "Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of-Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf> at 4; Anstis, Siena, Ronald J. Deibert, and Angela Yang (2022), "Submission to the Standing Committee on Access to Information, Privacy and Ethics," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2022/08/Brief-to-the-House-of-Commons-Standing-Committee-on-Access-to-Information-Privacy-and-Ethics.pdf> at 3.

[8] Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ronald J. Deibert (2018), "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2018/09/hide-seek-tracking-nso-groups-pegasus-spyware-to-operations-45-countries/> at 7.

[9] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ronald J. Deibert (2021), "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf> at 5; Scott-Railton, John, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, and Ronald J. Deibert (2022), "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru," *Citizen Lab, (Munk School of Global Affairs, University of Toronto)* <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/> at 25 (For example, a recent case in India involved the alleged planting of incriminating evidence into the device of an Indian activists who was accused of terrorism).

regarding the user's location.[10] Such capabilities effectively turn any infected mobile device into a portable surveillance tool that can transmit conversations happening within the target's vicinity, as well as other intimate and personal information of the device owner and/or those persons communicating with them.[11]

Market Features

The mercenary spyware market operates in a business-to-government framework where private companies sell products to government clients such as intelligence, law enforcement, and security agencies.[12] The industry has thrived over the last decade, as the shift toward an increasingly digitally networked society has been paralleled by an increasing appetite (and funding) among government agencies to buy and use surveillance technologies for counter-terrorism objectives.[13] In 2016, there were reportedly "over five hundred companies developing, marketing and selling [digital surveillance] products to government purchasers."[14] By 2022, the industry was valued at an estimated USD 12 billion.[15]

---

[10] Anstis, Siena, Ronald J. Deibert, Émilie LaFlèche, and Jon Penney (2022), "Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of-Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf> at 4–5.

[11] Anstis, Siena, Ronald J. Deibert, Émilie LaFlèche, and Jon Penney (2022), "Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of-Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf> at 4–5.

[12] Anstis, Siena, Ronald J. Deibert, and Jon Penney (2019), "Submission of the Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto) to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Surveillance Industry and Human Rights," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2019/02/Submission-to-the-UN-Special-Rapporteur-on-the-promotion-and-protection-of-the-right-to-freedom-of-opinion-and-expression-on-the-surveillance-industry-and-human-rights-2.pdf> at 11.

[13] Ronald J. Deibert (2022), "Protecting Society From Surveillance Spyware," *Issues in Science and Technology* 2(38) <https://issues.org/surveillance-spyware-uso-group-pegasus-citizen-lab/>; United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism (2023), "Position paper on Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach," *United Nations Special Procedures of the Human Rights Council* <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf> at 17.

[14] 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 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement> at para 6.

[15] Ronan Farrow (2022), "How Democracies Spy on Their Citizens," *The New Yorker* (April 18 2022) <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>.

Despite its proliferation, nearly every aspect of the mercenary spyware industry is cloaked in secrecy: from who buys surveillance products,[16] to the secret trade shows where they are promoted,[17] to the names of spyware companies and the nature of their operations.[18] Complex sales structures—such as multiple corporate entities that operate from various countries—make it difficult to monitor a company's compliance with applicable legislation such as export licence requirements.[19] This secrecy extends to corporate policies and standards.[20] Even for publicly known companies, there is generally little substantive information published on how they comply with the *United Nations Guiding Principles on Business and Human Rights* (UNGPs), how they address the human rights impacts of the spyware they develop and sell, whether they have a human rights due diligence system in place that leads to verifiable results, or if they have implemented grievance systems, for example.[21]

The lack of transparency in the spyware market is facilitated by an absence of state regulation, which allows the industry to operate with little to no effective public or government oversight.[22] The close link between the spyware industry and government bodies that are

---

[16] See e.g., Merlin Delcid (2022), "El Salvador Denies Responsibility for Hacking Journalists After Report Finds Pegasus Spyware on their Phones," *CNN* (January 13 2022) <https://www.cnn.com/2022/01/13/americas/el-salvador-pegasus-spyware-intl/index.html>; Justin Spike (2021), "Hungarian Official: Government Bought, Used Pegasus Spyware," *AP News* (November 4, 2021) <https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0>; Vanessa Gera (2022), "Polish Leader Admits Country Bought Powerful Israeli Spyware," *AP News* (January 7 2022) <https://apnews.com/article/technology-business-software-spyware-jaroslaw-kaczynski-0c41a504e8fbdbb6b9b06f6869848a4>; Panu Wongcha-um (2022), "Thailand Admits to Using Phone Spyware, Cites National Security," *Reuters* (July 20 2022) <https://www.reuters.com/world/asia-pacific/thailand-admits-using-phone-spyware-cites-national-security-2022-07-20/>; Joseph Wilson (2022), "Catalan: Spain Spy Chief Admits Legally Hacking Some Phones," *AP News* (May 5 2022) <https://apnews.com/article/technology-europe-barcelona-spain-hacking-38dcf5392b273f8e8447b0a9f62ed2f5>.

[17] See e.g., Ilya Lozovsky (2021), "Where NSO Group Came From—And Why It's Just the Tip of the Iceberg," *Organized Crime and Corruption Reporting Project* <https://www.occrp.org/en/the-pegasus-project/where-nso-group-came-from-and-why-its-just-the-tip-of-the-iceberg>.

[18] See e.g., Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ronald J. Deibert (2021), "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf> at 2.

[19] Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (2021), "Operating from the Shadows: Inside NSO Group's Corporate Structure," *Amnesty International* <https://www.amnesty.org/en/documents/doc10/4182/2021/en/>; Ronald J. Deibert (2022), "Subversion Inc: The Age of Private Espionage," *Journal of Democracy* 2(33) at 34.

[20] Anstis, Siena, Ronald J. Deibert, and Jon Penney (2019), "Submission of the Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto) to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Surveillance Industry and Human Rights," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2019/02/Submission-to-the-UN-Special-Rapporteur-on-the-promotion-and-protection-of-the-right-to-freedom-of-opinion-and-expression-on-the-surveillance-industry-and-human-rights-2.pdf> at 11.

[21] Anstis, Siena, Ronald J. Deibert, and Jon Penney (2019), "Submission of the Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto) to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Surveillance Industry and Human Rights," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2019/02/Submission-to-the-UN-Special-Rapporteur-on-the-promotion-and-protection-of-the-right-to-freedom-of-opinion-and-expression-on-the-surveillance-industry-and-human-rights-2.pdf> at 17.

[22] Anstis, Siena, Ronald J. Deibert, and Angela Yang (2022), "Submission to the Standing Committee on Access to Information, Privacy, and Ethics," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)*

purchasing spyware means there is likely a perceived mutual benefit to this lack of transparency, which further contributes to a lack of regulation.[23] Finally, there is less external pressure requiring transparency in the context of business transactions where governments are the primary clientele and the public has limited awareness of what is happening.[24]

Selected Companies

There are a growing number of companies developing and selling mercenary spyware.[25] This section focuses on four entities that the Citizen Lab has recently published on: NSO Group, Candiru, Cytrox, and QuaDream. However, other firms which have likewise been implicated in the sale of spyware to government agencies, and which Citizen Lab has addressed in technical

<https://citizenlab.ca/wp-content/uploads/2022/08/Brief-to-the-House-of-Commons-Standing-Committee-on-Access-to-Information-Privacy-and-Ethics.pdf> at 6.

[23] See Hagar Shezaf and Jonathan Jacobson (2018), "Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays," *Haaretz* (October 20 2018) <https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000> (Discussing the close relationship between the private companies manufacturing surveillance technology and state military and defense in Israel).

[24] Anstis, Siena, Ronald J. Deibert, and Jon Penney (2019), "Submission of the Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto) to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Surveillance Industry and Human Rights," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2019/02/Submission-to-the-UN-Special-Rapporteur-on-the-promotion-and-protection-of-the-right-to-freedom-of-opinion-and-expression-on-the-surveillance-industry-and-human-rights-2.pdf> at 18.

[25] See for e.g., UN Human Rights Council (2023) "Human Rights Implications of the Development, Use and Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism," 52nd Sess, UN Doc A/HRC/52/39 <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/reports/A-HRC-52-39-AdvanceEditedVersion.docx> at para 47.

reports, include Gamma Group,[26] FinFisher GmbH,[27] Cyberbit,[28] Amesys (now "Nexa Technologies"),[29] Qosmos, DarkMatter, WiSpear, and Hacking Team (now "Memento Labs").[30]

NSO Group

NSO Group is an Israeli-based spyware company founded in 2010 with connections to Israeli military intelligence.[31] NSO Group's spyware, **Pegasus**, has both one-click and zero-click

---

[26] Siena Anstis (2018), "Litigation and other Formal Complaints Related to Mercenary Spyware," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/#GammaGroup> (Gamma Group is an international manufacturer of surveillance systems headquartered in the UK, purporting to provide consulting services to law enforcement agencies. Gamma Group created a line of spyware products called FinFisher/FinSpy, which it alleges that it stopped selling after 2012).

[27] Siena Anstis (2018), "Litigation and other Formal Complaints Related to Mercenary Spyware," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/#FinFisher> (FinFisher GmbH is a German-based company selling FinFisher/FinSpy since 2013). Marczak, Bill, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune (2015), "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/> (FinFisher spyware has been implicated in numerous surveillance abuses. Citizen Lab has identified 33 likely government users of FinFisher in 32 countries. For example, Bahrain's government used FinFisher between 2010–2012 to monitor law firms, journalists, activists, and political opposition. Ethiopian dissidents in exile in the UK and the US have also been infected with FinFisher spyware). See also on this point Marquis-Boire, Morgan, Bill Marczak, Claudio Guarnieri, and John Scott-Railton (2013), "You Only Click Twice: FinFisher's Global Proliferation," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/>.

[28] Marczak, Bill, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ronald J. Deibert (2017), "Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/> (Cyberbit is an Israeli-based company established in 2015, marketed to intelligence and law enforcement agencies. Its software, PC Surveillance System, has been used to target Ethiopian dissidents in several countries including the US and the UK).

[29] Paul Sonne and Margaret Coker (2011), "Firms Aided Libyan Spies," *Wall Street Journal* (August 30, 2011) <http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html> (Nexa Technologies, formerly "Amesys," is a French company involved in supplying spyware to the Libyan and Egyptian governments used to surveil, track, torture and forcibly disappear activists during the regimes of Gaddafi and al-Sisi, respectively); Fédération internationale pour les droits humains (2022), "France: Court of Appeal Confirms Indictment of Amesys & Its Executives over Allegations of Complicity of Torture in Libya," *Business & Human Rights Resource Centre* <https://www.business-humanrights.org/en/latest-news/france-court-of-appeal-confirms-indictment-of-amesys-its-executives-over-allegations-of-complicity-of-torture-in-lybia/> (Executives of Nexa and Amesys have been indicted by the Paris Court of Appeal for their complicity in providing technology used in relation to these crimes).

[30] Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton (2014), "Mapping Hacking Team's "Untraceable" Spyware," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/>; Anstis, Siena, Ronald J. Deibert, and Jon Penney (2019), "Submission of the Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto) to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Surveillance Industry and Human Rights," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2019/02/Submission-to-the-UN-Special-Rapporteur-on-the-promotion-and-protection-of-the-right-to-freedom-of-opinion-and-expression-on-the-surveillance-industry-and-human-rights-2.pdf> at 11 (Memento Labs is an Italian-based company providing "offensive technology" to worldwide law enforcement and intelligence communities. Citizen Lab reports in 2014 and 2015 documented that their spyware, Remote Control System (RCS), attempted to target employees of the Ethiopian Satellite Television Service, an independent media outlet run by members of the Ethiopian diaspora. The Citizen Lab mapped the suspected use of RCS by governments including Azerbaijan, Colombia, Egypt, Ethiopia, Hungary, Italy, Kazakhstan, Korea, Malaysia, Mexico, Morocco, Nigeria, Oman, Panama, Poland, Saudi Arabia, Sudan, Thailand, Turkey, UAE, and Uzbekistan).

[31] Ronen Bergman and Mark Mazzetti (2022), "The Battle for the World's Most Powerful Cyberweapon," *The New York Times* (January 28 2022) <https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html>; Al Jazeera (2022),

capabilities that turn targeted devices into sophisticated tracking and surveillance tools.[32] The Citizen Lab has published numerous reports documenting state deployment of Pegasus spyware against a broad range of individuals, such as HRDs, civil society actors, journalists, scientists, lawyers, and politicians, that would likely not be justified under international human rights law.[33] In 2018, the Citizen Lab identified 45 countries where Pegasus operators may be conducting surveillance operations.[34] This includes Canada, where the Citizen Lab discovered that Omar Abdulaziz, a Saudi dissident and permanent resident of Canada, had been targeted with Pegasus spyware likely by a Saudi operator.[35] In June 2022, NSO Group representatives testified before the European Parliament that Pegasus has been used by states to target 12,000–13,000 people per year.[36]

"Pegasus: What You Need to Know About Israeli Spyware," *Al Jazeera* (February 8 2022) <https://www.aljazeera.com/news/2022/2/8/what-you-need-to-know-about-israeli-spyware-pegasus>.

[32] Anstis, Siena, Ronald J. Deibert, Émilie LaFlèche, and Jon Penney (2022), "Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of-Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf> at 3–4.

[33] Siena Anstis (2018), "Litigation and other Formal Complaints Related to Mercenary Spyware," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/> (For more information on NSO Group, including a non-exhaustive list of resources on spyware companies compiled by the Citizen Lab and a list of reports on the following targets: Emirati human rights defender Ahmed Mansoor, Saudi dissidents Omar Abdulaziz and Ghanem Al-Masarir, as well as another Saudi activist, Salvadorian journalists from *El Faro*, Jordanian human rights defenders, lawyers, and journalists, civil society in Palestine, pro-democracy protestors in Thailand, Mexican journalists, politicians, and civil society, Catalonian civil society, and a *New York Times* journalist).

[34] Anstis, Siena, Ronald J. Deibert, Émilie LaFlèche, and Jon Penney (2022), "Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of-Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf> at 6.

[35] Marczak, Bill, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ronald J. Deibert (2018), "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/>.

[36] European Parliament: Multimedia Centre (2022), "Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware," *European Parliament* <https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20220621-1500-COMMITTEE-PEGA>; United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism (2023), "Position paper on Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach," United Nations Special Procedures of the Human Rights Council <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf> at 21.

Candiru (Saito Tech)

Founded in 2014 and based in Israel, Candiru markets "untraceable" spyware exclusively to government customers.[37] Candiru appears to be currently registered as Saito Tech Ltd.[38] Candiru products enable clients to exfiltrate files, extract messages from encrypted apps, and steal cookies and passwords.[39] The spyware allows clients to send messages directly from an infected device by accessing logged-in email or social media accounts, making it appear as though the messages were sent by the spyware target.[40] The Citizen Lab has documented hundreds of websites linked to Candiru that use fake domains to pose as advocacy organisations and hack targets.[41] Several abuses have been identified, including the targeting of journalists in the Middle East[42] and of civil society in Spain.[43]

Cytrox

Cytrox is a Macedonian company with operations in Hungary and Israel purporting to provide "cyber intelligence systems designed to offer security" to governments.[44] Yet Cytrox's spyware, **Predator**, has been used in the hacking of Egyptian politicians critical of the Sisi regime,[45] and

[37] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ronald J. Deibert (2021), "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf> at 14.
[38] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ronald J. Deibert (2021), "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf> at 2; see also Sam Levin (2021), "Israeli Spyware Firm Linked to Fake Black Lives Matter and Amnesty Websites," *The Guardian* (July 15 2021) <https://www.theguardian.com/technology/2021/jul/15/spyware-company-impersonates-activist-groups-black-lives-matter>.
[39] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ronald J. Deibert (2021), "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf> at 7.
[40] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ronald J. Deibert (2021), "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf> at 7.
[41] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ronald J. Deibert (2021), "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf> at 10.
[42] Emma McGowan (2022), "New Candiru Attack Targets Journalists in the Middle East," *Avast* (July 28 2022) <https://blog.avast.com/candiru-targeting-journalists-middle-east>.
[43] Scott-Railton, John, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, and Ronald J. Deibert (2022), "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru," *Citizen Lab, (Munk School of Global Affairs, University of Toronto)* <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>.
[44] Marczak, Bill, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ronald J. Deibert (2021), "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2021/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-spyware/> (Cytrox forms part of the "Intellexa alliance" which is a marketing label for a range of mercenary surveillance vendors that emerged in 2019 and is made up of a consortium of companies, including Nexa Technologies, which are purportedly seeking to compete against prominent players in the market such as NSO Group).
[45] Marczak, Bill, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ronald J. Deibert (2021), "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2021/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-spyware/>.

in the ongoing domestic surveillance scandal in Greece.[46] In 2012, Meta removed around 300 accounts on Facebook and Instagram that were linked to Cytrox and reported that numerous Meta users around the world have been targeted by Cytrox, including politicians and journalists.[47]

QuaDream

QuaDream is an Israeli firm selling digital offensive technology to government customers.[48] Their spyware, **Reign**, utilizes zero-click exploits to infect the devices of persons of interest.[49] A 2023 investigative report by the Citizen Lab identified operators of QuaDream in Bulgaria, Czech Republic, Hungary, Ghana, Israel, Mexico, Romania, Singapore, United Arab Emirates and Uzbekistan.[50] The investigation found that the spyware was deployed against targets such as journalists, political opponents, and NGO workers.[51] Recent reports suggest that QuaDream wound operations down in April 2023, after months of financial strain and the publication of the Citizen Lab's report.[52]

Concerns Raised by Mercenary Spyware

National Security

Spyware poses a significant risk to national security. Spyware is, by its nature, highly intrusive, constantly evolving, and difficult to detect. This creates risks that are hard for governments to address and mitigate, particularly given that there is limited insight into the

---

[46] Georgios Samaras (2022), "Greece's 'Watergate' Explained: Why the European Parliament is Investigating Over a Wiretapping Scandal," *The Conversation* (November 8 2022) <http://theconversation.com/greeces-watergate-explained-why-the-european-parliament-is-investigating-over-a-wiretapping-scandal-192537>.

[47] Dvilyanski, Mike, David Agranovich, and Nathaniel Gleicher (2021), "Threat Report on the Surveillance-for-Hire Industry," *Meta* <https://about.fb.com/wp-content/uploads/2021/12/nThreat-Report-on-the-Surveillance-for-Hire-Industry.pdf>.

[48] Gur Megiddo (2021), "Secretive Israeli Cyber Firm Selling Spy-tech to Saudi Arabia," *Haaretz* (June 8 2021) <https://www.haaretz.com/israel-news/tech-news/2021-06-08/ty-article/.highlight/the-secret-israeli-cyber-firm-selling-spy-tech-to-saudia-arabia/0000017f-df07-d856-a37f-ffc724f80000>.

[49] Marczak, Bill, John Scott-Railton, Astrid Perry, Noura Al-Jizawi, Siena Anstis, Zoe Panday, Emma Lyon, Bahr Abdul Razzak, and Ronald J. Deibert (2023), "Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/> .

[50] Marczak, Bill, John Scott-Railton, Astrid Perry, Noura Al-Jizawi, Siena Anstis, Zoe Panday, Emma Lyon, Bahr Abdul Razzak, and Ronald J. Deibert (2023), "Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/> .

[51] Marczak, Bill, John Scott-Railton, Astrid Perry, Noura Al-Jizawi, Siena Anstis, Zoe Panday, Emma Lyon, Bahr Abdul Razzak, and Ronald J. Deibert (2023), "Sweet QuaDreams A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/> .

[52] Omer Benjakob (2023), "Israeli Spyware Maker QuaDream Closes, Fires All Employees," *Haaretz* (April 16 2023) <https://www.haaretz.com/israel-news/security-aviation/2023-04-16/ty-article/.premium/offensive-israeli-cyber-firm-quadream-closes-and-fires-all-employees/00000187-8b5c-d484-adef-ebdc048c0000>; Howard Solomon (2023), "Commercial Spyware-maker QuaDream to Close, Say Reports," *IT World Canada* (April 17 2023) <https://www.itworldcanada.com/article/commercial-spyware-maker-quadream-to-close-say-reports/536543> (reporting that QuaDream terminated all but two of its employees the week following Citizen Lab's 2023 publication).

market as a whole and a lack of transparency regarding the origin of spyware and identity of end-users.[53]

These risks are compounded by the proliferation of this technology, giving any country willing to pay unprecedented surveillance capabilities.

The mercenary spyware industry introduces a new tier of spyware players. The existence of this unregulated market has provided a growing number of countries—including countries hostile to Canada or with a history of human rights abuses—access to highly intrusive surveillance technology. The availability of spyware equips governments to engage in cross-border cyber espionage, whether against other states or against diaspora members or their own resident dissidents.

States with advanced spyware capabilities are able to use this technology to strategically shape global political, military, economic, and ideological power.[54] There have been several documented instances of spyware being used against government officials in ways that pose risks to national security. Examples include spyware infections of UK government networks (notably the Prime Minister's Office and the Foreign Commonwealth and Development Offices),[55] the devices of Spanish Prime Minister Pedro Sánchez and Defense Minister Margarita Robles,[56] as well as the devices of at least 50 US government officials in 10 different countries.[57]

The Pegasus Project, an international investigation into government cyber espionage led by a consortium of 17 media organisations, revealed that the phone numbers of 14 heads of state as well as those of diplomats, military chiefs, and senior politicians from 34 countries were

---

[53] Marczak, Bill, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ronald J. Deibert (2020), "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2020/12/great-ipwn-journalists-hacked-suspected-nso-group-imsg-zero-click-exploit/>; Duncan B. Hollis (2011), "An e-SOS for Cyberspace," *Harvard International Law Journal* 2(52) <https://harvardilj.org/wp-content/uploads/sites/15/2011/07/HILJ_52-2_Hollis1.pdf>.

[54] European Union Agency for Cybersecurity (2021), "ENISA Threat Landscape 2021," *European Union Agency for Cybersecurity* <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021> at 21.

[55] Ronald J. Deibert (2022), "UK Government Officials Infected with Pegasus," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/>.

[56] Vincent Manancourt (2022), "Hack of Spanish PM's Phone Deepens Europe's Spyware Crisis," *POLITICO* (May 2 2022) <https://www.politico.eu/article/pegasus-hacking-spyware-spain-government-prime-minister-pedro-sanchez-margarita-robles-digital-espionage-crisis/>.

[57] Ellen Nakashima, Tim Starks (2023), "At Least 50 U.S. Government Employees Targeted with Phone Spyware Overseas," *The Washington Post* (March 27 2023) <https://www.washingtonpost.com/national-security/2023/03/27/spyware-diplomats-us-pegasus/>; Peter Guest (2023), "Spyware Finally Got Scary Enough to Freak Lawmakers Out—After It Spied on Them," *Bloomberg* (January 24 2023) <https://www.bloomberg.com/news/features/2023-01-24/nso-group-s-pegasus-spyware-focus-of-us-eu-investigations>; Katie Benner, David E. Sanger, and Julian E. Barnes (2021), "Israeli Company's Spyware Is Used to Target U.S. Embassy Employees in Africa," *The New York Times* (December 3 2021) <https://www.nytimes.com/2021/12/03/us/politics/phone-hack-nso-group-israel-uganda.html>.

contained in a leaked database of potential spyware targets.[58] The infected devices of HRDs, journalists, or activists may also be used to surveil meetings with government officials. For example, Carine Kanimba, a US-Belgian activist, met with officials from the US, Belgium, UK, and the EU Parliament while her phone was infected with Pegasus.[59]

Human Rights

Governments and international organisations have increasingly recognized the incompatibility of mercenary spyware with fundamental human rights.[60] As observed by the European Data Protection Supervisor (EDPS) and current and former United Nations (UN) Special Rapporteurs, spyware—by facilitating complete access to a device's contents—infringes on human rights, including the rights to freedom of speech, association, and assembly, the right to privacy, the right to life, liberty and security of the person, data protection law, and other individual rights, and poses a persistent threat to civil society institutions.[61]

While human rights can sometimes be infringed on by government actors under the framework of international human rights law, such infringements must be prescribed by law, serve a legitimate purpose, and be necessary and proportionate.[62] There is extensive evidence that spyware is used in a manner that results in unjustified human rights violations. For example, it has been used to target journalists and HRDs who are critical to civil society institutions and to maintaining democratic and rights-respecting norms. Targeting these actors impedes their ability to engage in human rights advocacy or undertake investigative

[58] Angelique Chrisafis, Dan Sabbagh, Stephanie Kirchgaessner, and Michael Safi (2021), "Emmanuel Macron Identified in Leaked Pegasus Project Data," *The Guardian* (July 20 2021) <https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data>.

[59] Stephanie Kirchgaessner (2021), "Hotel Rwanda Activist's Daughter Placed under Pegasus Surveillance," *The Guardian* (July 19 2021) <https://www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance>.

[60] European Data Protection Supervisor (2022), "Preliminary Remarks on Modern Spyware," *European Data Protection Supervisor* <https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf> at 8 (The European Data Protection Supervisor concludes that spyware is likely incompatible with *EU Charter of Fundamental Rights*, since "the level of interference with the right to privacy is so severe that the individual is in fact deprived of it" and that the use of this technology "cannot be considered proportionate – irrespective of whether the measure can be deemed necessary to achieve the legitimate objectives of a democratic state" since it affects the "essence" of the right to privacy).

[61] European Data Protection Supervisor (2022), "Preliminary Remarks on Modern Spyware," *European Data Protection Supervisor* <https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf> at 2; UN Human Rights Council (2013), "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," 23rd Sess, UN Doc A/HRC/23/40 <https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf> at para 24 ("[t]he right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas"); UN Human Rights Council (2015), "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," 29th Sess, UN Doc A/HRC/29/32 <https://www.refworld.org/docid/5576dcfc4.html> at paras 6–10 (discussing the relationship between privacy and freedom of opinion and expression in the context of the debate over encryption and anonymity).

[62] Dunja Mijatović (2023), "Highly Intrusive Spyware Threatens the Essence of Human Rights," *Commissioner for Human Rights* <https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights>.

journalism and undermines fundamental rights like freedom of expression and opinion and the right to privacy.[63] As the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (the "Special Rapporteur on human rights and counter terrorism") recently underlined in her report discussing spyware:

> The impact of surveillance on multiple human rights is considerable. The Special Rapporteur highlights that the right to privacy functions as a gateway right protecting and enabling many other rights and freedoms, and its protection is intimately related to the existence and advancement of a democratic society. She therefore sees the escalation in the use of secret surveillance and the collection of content information and metadata for purposes of countering terrorism, combined with the runaway development of underregulated new technologies, as a significant threat to democratic societies.[64]

In addition to the states that operate and use spyware in violation of international human rights law, mercenary spyware companies—who are willing to sell their technology to countries with poor human rights records—operate in a non-transparent environment[65] and in contravention of human rights norms outlined in the UNGPs.[66] The unregulated nature of the industry facilitates governments' ability to obtain spyware and use it widely against targets in violation of international human rights law.[67]

---

[63] UN Human Rights Council (2013), "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," 23rd Sess, UN Doc A/HRC/23/40 <https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf> at paras 24–26.

[64] UN Human Rights Council (2023), "Human Rights Implications of the Development, Use and Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism," 52nd Sess, UN Doc A/HRC/52/39 <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/reports/A-HRC-52-39-AdvanceEditedVersion.docx> at para 45.

[65] Directorate-General for External Policies, Policy Department, European Parliament (2015), "Surveillance and Censorship: The Impact of Technologies on Human Rights," *European Parliament* <https://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf> at 29; Cindy Cohn, Trevor Timm, and Jillian C. York (2012), "Human Rights and Technology Sales: How Corporations Can Avoid Assisting Repressive Regimes," *Electronic Frontier Foundation* <https://www.eff.org/document/human-rights-and-technology-sales> at 4–5.

[66] UN Commission on Human Rights (2011), "Guiding Principles on Business and Human Rights," *United Nations Commission on Human Rights*, Doc HR/PUB/11/04 <https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf>.

[67] United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism (2023), "Position paper on Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach," *United Nations Special Procedures of the Human Rights Council* <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf> at 22–23 (on the various violations of international human rights law, including: violations of the right to life and exposure to physical risk; disproportionate interference with privacy; disproportionate interference with freedom of expression, peaceful assembly, association, and religion; harms to women and LGBTQI+ persons; impact on fair trial and due process; impact on effective remedies).

Democracy and the Rule of Law

Spyware poses a significant threat to democracy and the rule of law.[68] It has been used by repressive regimes to limit or control political dissent, the media, the courts, and other institutions of civil society.[69] Governments have used spyware to enable repression, manipulation, and defamation campaigns. Key figures in the public sphere, including journalists, opposition politicians, and activists, have been targets of spyware. However, spyware violations occur not only in authoritarian regimes, but also in democracies.[70] Spyware has been used to interfere with the electoral process, through manipulation and smear campaigns against political opposition members, in countries as wide-ranging as Saudi Arabia,[71] India,[72] Poland,[73] Hungary,[74] Greece, and Spain.[75]

Spyware threatens the quality of democratic political participation by preventing people from engaging in certain political issues, expressing their sincerely held views, and developing political and professional networks.[76] For example, it has been used against government critics and pro-democracy protesters in the United Arab Emirates,[77] Thailand,[78] Saudi Arabia,[79]

---

[68] European Data Protection Supervisor (2022), "Preliminary Remarks on Modern Spyware," *European Data Protection Supervisor* <https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf> at 9.

[69] Ronald J. Deibert (2022), "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy," *Foreign Affairs* 1(102).

[70] See e.g., European Union Agency for Cybersecurity (2021), "ENISA Threat Landscape 2021," *European Union Agency for Cybersecurity* <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021> at 16 (the European Union Agency for Cybersecurity listed state-sponsored cyber espionage as a major risk in this report).

[71] Stephanie Kirchgaessner (2021), "Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests," *The Guardian* (July 18 2021) <https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus>.

[72] Human Rights Watch (2021), "India: Spyware Use Violates Supreme Court Privacy Ruling," *Human Rights Watch* <https://www.hrw.org/news/2021/08/26/india-spyware-use-violates-supreme-court-privacy-ruling>.

[73] Agence France-Presse (2021), "Claims Polish Government Used Spyware is 'Crisis for Democracy', Says Opposition," *The Guardian* (December 28 2021) <https://www.theguardian.com/world/2021/dec/28/poland-pegasus-spyware-donald-tusk>.

[74] Shaun Walker (2021), "Viktor Orbán Using NSO Spyware in Assault on Media, Data Suggests," *The Guardian* (July 18 2021) <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>.

[75] Scott-Railton, John, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, and Ronald J. Deibert (2022), "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru," *Citizen Lab, (Munk School of Global Affairs, University of Toronto)* <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>.

[76] Sartor, Giovanni, and Loreggia Andrea (2022), "The Impact of Pegasus on Fundamental Rights and Democratic Processes," *European Parliament's Committee of Inquiry to investigate the Use of Pegasus and Equivalent Surveillance Spyware (PEGA)* <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf> at 27.

[77] Marczak, Bill, and John Scott-Railton (2016), "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender," *Citizen Lab, (Munk School of Global Affairs, University of Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/96976/1/Report%2378--Million-Dollar-Dissident.pdf> at 8.

[78] Scott-Railton, John, Bill Marczak, Irene Poetranto, Bahr Abdul Razzak, Sutawan Chanprasert, and Ronald J. Deibert (2022), "GeckoSpy: Pegasus Spyware Used against Thailand's Pro-Democracy Movement," *Citizen Lab, (Munk School of Global Affairs, University of Toronto)* <https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/>.

[79] Stephanie Kirchgaessner (2021), "Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests," *The Guardian* (July 18 2021) <https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus>.

and Hungary.[80] Spyware also undermines the rule of law, having been used against judicial officials and civil society organisations that seek to hold governments accountable. Examples include Argentina,[81] Mexico,[82] Spain,[83] and Poland,[84] where lawyers have been targeted.

Journalists have also been a key target of spyware, which is a severe breach of democratic foundations, the rule of law, and freedom of the press.[85] Spyware compromises the confidentiality of journalistic sources and the functioning and credibility of free access to information, media freedom, and media pluralism. This is particularly concerning since independent media is a pillar of democratic societies.[86] Recent examples include the targeting of journalists reporting on Greece,[87] Hungary,[88] Mexico,[89] El Salvador,[90] the Dominican Republic,[91] and Saudi Arabia.[92] One prominent example is the targeting of various individuals close to Saudi dissident and journalist Jamal Khashoggi, who was brutally killed by the Saudi regime in Turkey.[93]

---

[80] Justin Spike (2021), "Hungarian Official: Government Bought, Used Pegasus Spyware," *AP News* (November 4 2021) <https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0>.
[81] Scott-Railton, John, Morgan Marquis-Boire, Claudio Guarnieri, and Marion Marschalek (2015), "Packrat: Seven Years of a South American Threat Actor," *Citizen Lab, (Munk School of Global Affairs, University of Toronto)* <https://citizenlab.ca/2015/12/packrat-report/> at 9–10.
[82] Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ronald J. Deibert (2017), "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," *Citizen Lab, (Munk School of Global Affairs, University of Toronto)* <https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/>.
[83] Scott-Railton, John, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, and Ronald J. Deibert (2022), "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru," *Citizen Lab, (Munk School of Global Affairs, University of Toronto)* <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>.
[84] Agence France-Presse (2021), "Claims Polish Government Used Spyware is 'Crisis for Democracy', Says Opposition," *The Guardian* (December 28 2021) <https://www.theguardian.com/world/2021/dec/28/poland-pegasus-spyware-donald-tusk>.
[85] Saskia Bricmont, Claudia Rothe, and Georg McCutcheon (2022), "In the Name of National Security: How Spyware Threatens the EU's Democratic Foundations," *Heinrich Böll Stiftung The Green Political Foundation* <https://www.boell.de/en/2022/12/14/name-national-security-how-spyware-threatens-eus-democratic-foundations>.
[86] Dunja Mijatović (2023), "Highly Intrusive Spyware Threatens the Essence of Human Rights," *Commissioner for Human Rights* (January 27 2023) <https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights>.
[87] George Georgiopoulos (2022), "Greek Intelligence Service Admits Spying on Journalist," *Reuters* (August 3 2022) <https://www.reuters.com/world/europe/greek-intelligence-service-admits-spying-journalist-sources-2022-08-03/>.
[88] Shaun Walker (2021), "Viktor Orbán Using NSO Spyware in Assault on Media, Data Suggests," *The Guardian* (July 18 2021) <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>.
[89] Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ronald J. Deibert (2017), "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," *Citizen Lab, (Munk School of Global Affairs, University of Toronto)* <https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/>.
[90] Scott-Railton, John, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Al-Jizawi, Salvatore Solimano, and Ronald J. Deibert (2022), "Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware," *Citizen Lab, (Munk School of Global Affairs, University of Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123609/1/Report%23148--project-torogoz.pdf> at 5–9.
[91] Amnesty International (2023), "Dominican Republic: Pegasus Spyware Discovered on Prominent Journalist's Phone," *Amnesty International* <https://www.amnesty.org/en/latest/news/2023/05/dominican-republic-pegasus-spyware-journalists-phone/>.
[92] Marczak, Bill, John Scott-Railton, Siena Anstis, Bahr Abdul Razzak, and Ronald J. Deibert (2021), "Breaking the News: New York Times Journalist Ben Hubbard Hacked with Pegasus after Reporting on Previous Hacking Attempts," *Citizen Lab, (Munk School of Global Affairs, University of Toronto)* <https://citizenlab.ca/2021/10/breaking-news-new-york-times-journalist-ben-hubbard-pegasus/>.
[93] Stephanie Kirchgaessner (2021), "Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests," *The Guardian* (July 18 2021)

US and EU Responses to Mercenary Spyware

United States

The US has pursued various regulatory responses to threats posed by spyware.[94] US lawmakers have increasingly called for inquiries into the use of spyware and measures to protect against the national security and human rights risks it raises.[95] Congressman Jim Himes, along with 14 colleagues, has emphasised the need for concerted action to protect US citizens and residents from becoming spyware targets.[96] Congressman Adam Schiff, former chair of the House Intelligence Committee, has called on the head of the Drug Enforcement Administration (DEA) to provide details about its deployment of Graphite spyware, noting the "potential implications for US national security" and suggesting that its use could "run contrary to efforts to deter the broad proliferation of powerful surveillance capabilities to autocratic regimes and others who may misuse them."[97] The US House Intelligence Committee also held a hearing on "combatting the threats to U.S. national security from the proliferation of foreign commercial spyware" in July 2022.[98] These calls for action have prompted various legislative, regulatory, and policy changes at the federal level.

The Biden Administration has made several recent efforts to counter the proliferation and misuse of commercial spyware.[99] This includes hosting an event on Advancing Technology for Democracy as part of the Summit for Democracy 2023. During the Summit, the US adopted a Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware along with ten other countries, including Canada, to promote international cooperation on spyware regulation.[100]

<https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus>.

[94] Ronald J. Deibert (2022), "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy," *Foreign Affairs* 1(102).

[95] Mark Mazzetti and Ronen Bergman (2022), "Lawmakers Signal Inquiries Into U.S. Government's Use of Foreign Spyware," *The New York Times* (December 28 2022) <https://www.nytimes.com/2022/12/28/us/politics/spyware-israel-dea-fbi.html>.

[96] Representative James A. Himes, et. al. to Secretary Antony Blinken and Secretary Gina M. Raimondo, memorandum, September 29, 2022, <https://himes.house.gov/_cache/files/f/1/f1a6daf0-9ee6-4936-9cb4-25de81cd7d74/D34AB1A35CAEAA423C986A74FDD68A97.letter-concerning-the-unethical-uses-of-foreign-commercial-spyware-29sept-.pdf>.

[97] Representative Adam B. Schiff to Hon. Anne Milgram, memorandum, December 22, 2022, <https://int.nyt.com/data/documenttools/schiff-letter-on-israeli-spyware-companies/a514c9b78dd75959/full.pdf>.

[98] House Select Intelligence Committee, "House Hearing on Foreign Spyware," 2022, C-SPAN <https://www.c-span.org/video/?522013-1/house-hearing-foreign-spyware>; Tim Starks (2022), "Congress Joins the Fight over Foreign Spyware," *Washington Post* (July 25 2022) <https://www.washingtonpost.com/politics/2022/07/25/congress-joins-fight-over-foreign-spyware/>; Permanent Select Committee on Intelligence, "Full Committee Hearing on Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware, Before the Permanent Select Committee on Intelligence," 117th Cong. (2022) <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=115048>.

[99] The White House (2023), "FACT SHEET: Advancing Technology for Democracy," *The White House Briefing Room* <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/29/fact-sheet-advancing-technology-for-democracy-at-home-and-abroad/>.

[100] The White House (2023), "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware," *The White House Briefing Room*

This has been complemented by domestic measures put in place through an Executive Order (the "Order") signed by President Biden on March 27, 2023. The Order prohibits the US government from using commercial spyware that "pose[s] significant counterintelligence or security risks to the U.S. Government or significant risks of improper use by a foreign government or foreign person, including to target Americans or enable human rights abuses."[101] The prohibition applies to various federal government institutions and agencies, including law enforcement, defence, and intelligence agencies.[102] It also responds to mounting pressure to address the serious threats posed by spyware, establishing key counterintelligence, security, and improper use factors as risk indicators to engage the prohibition.[103] The Order was signed amid revelations that at least 50 US government officials overseas have been targeted with spyware.[104]

The Order builds upon and is consistent with items included in the *2023 National Defence Authorization Act* (*NDAA*).[105] The *NDAA*, which was signed into law on December 23, 2022, introduced measures to mitigate counterintelligence threats from the proliferation and use of foreign commercial spyware.[106] The statement of policy included in the new provisions underlines the government's commitment to "act decisively against counterintelligence threats" posed by commercial spyware and individuals who participate in that market.[107] The *NDAA* mandates that the US intelligence community report to Congress with an assessment of

<https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/>.

[101] The White House (2023), "FACT SHEET: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security," *The White House Briefing Room* <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/>.

[102] The White House (2023), "FACT SHEET: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security," *The White House Briefing Room* <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/>; See also Tim Starks (2023), "Biden's Spyware Executive Order Gets Mostly Good Reviews,"*The Washington Post* (March 28 2023) <https://www.washingtonpost.com/politics/2023/03/28/bidens-spyware-executive-order-gets-mostly-good-reviews/>.

[103] U.S., Congress, House, Committee on Transportation and Infrastructure, *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, H.R.7776, 117th Cong. (2022) <https://www.congress.gov/bill/117th-congress/house-bill/7776/text>.

[104] Tim Starks and Ellen Nakashima (2023), "At Least 50 U.S. Government Employees Targeted with Phone Spyware Overseas," *The Washington Post* (March 27 2023) <https://www.washingtonpost.com/national-security/2023/03/27/spyware-diplomats-us-pegasus/>.

[105] U.S., Executive Office of The President, "Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security," Executive Order 14093 (March 27 2023) <https://www.federalregister.gov/documents/2023/03/30/2023-06730/prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to>; U.S. Congress, House, Committee on Armed Services, *National Defense Authorization Act for Fiscal Year 2023*, H.R.7900, 117th Congress <https://www.congress.gov/bill/117th-congress/house-bill/7900>.

[106] Access Now (2022), "U.S. Congress Takes Additional Steps to Combat Spyware," *Access Now* <https://www.accessnow.org/spyware-ndaa-2023/>; U.S. Congress, House, Committee on Armed Services, *National Defense Authorization Act for Fiscal Year 2023*, H.R.7900, 117th Congress <https://www.congress.gov/bill/117th-congress/house-bill/7900>.

[107] U.S., Congress, House, Committee on Transportation and Infrastructure, *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, H.R.7776, 117th Congress <https://www.congress.gov/bill/117th-congress/house-bill/7776/text> at §6318(b)(1).

counterintelligence threats and other risks to US national security posed by the proliferation of foreign commercial spyware.[108] It also allows the Director of National Intelligence to prohibit any element of the intelligence community from "procuring, leasing, or otherwise acquiring on the commercial market, or extending or renewing a contract to procure, lease, or otherwise acquire, foreign commercial spyware."[109]

The US has also taken measures to address the national security threat of ex-intelligence community officials working with mercenary spyware companies. For example, after it was revealed that ex-US intelligence officials were working for companies linked to the United Arab Emirates,[110] the US established restrictions on former intelligence community officials seeking employment with foreign governments or companies, including foreign commercial spyware entities.[111] The *NDAA* brought additional changes to employment restrictions in §6301, which creates a permanent ban on working in covered post-service positions for designated foreign countries and has been implemented through a recent *Intelligence Community Directive*.[112]

Export and trade have been key areas of spyware regulation, highlighting the US government's interest in addressing spyware as both a national security concern and a threat to human rights.[113] US Secretary of Commerce, Gina M. Raimondo, explained that the US was committed to "aggressively using export controls to hold companies accountable that develop, traffic, or use technologies to conduct malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials, and organisations here and abroad."[114]

---

[108] U.S., Congress, House, Committee on Transportation and Infrastructure, *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, H.R.7776, 117th Congress <https://www.congress.gov/bill/117th-congress/house-bill/7776/text> at §6318(c)(b).

[109] U.S., Congress, House, Committee on Transportation and Infrastructure, *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, H.R.7776, 117th Congress <https://www.congress.gov/bill/117th-congress/house-bill/7776/text> at §6318.

[110] Christopher Bing and Joel Schectman (2019), "Inside the UAE's Secret Hacking Team of American Mercenaries," *Reuters* (January 30 2019) <https://www.reuters.com/investigates/special-report/usa-spying-raven/>.

[111] U.S., Congress, House, Committee on Transportation and Infrastructure, *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, H.R.7776, 117th Congress <https://www.congress.gov/bill/117th-congress/house-bill/7776/text> at §6301; Representative James A. Himes, et. al. to Secretary Antony Blinken and Secretary Gina M. Raimondo, memorandum, September 29, 2022, <https://himes.house.gov/_cache/letter-concerning-the-unethical-uses-of-foreign-commercial-spyware-29sept-.pdf>.

[112] U.S., Congress, House, Committee on Transportation and Infrastructure, *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, H.R.7776, 117th Congress <https://www.congress.gov/bill/117th-congress/house-bill/7776/text> at §6301; U.S. Office of the Director of National Intelligence, *Requirements for Certain Employment Activities by Former Intelligence Community Employees*, Intelligence Community Directive 712 (March 23 2023) <https://www.dni.gov/files/documents/ICD/ICD_712.pdf>; Baumohl, Chris, John Davisson, Jake Wiener, and Ben Winters (2023), "Privacy, Surveillance, and AI in the FY'23 National Defense Authorization Act (NDAA)" *Electronic Privacy Information Center* <https://epic.org/privacy-surveillance-and-ai-in-the-fy23-national-defense-authorization-act-ndaa/>.

[113] U.S. Department of Commerce, Bureau of Industry and Security, *Export Administration Regulations (EAR)* 15 C.F.R., March 16, 2021 <https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear> at §730.3; Office of Public Affairs (2021), "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities," *U.S. Department of Commerce* <https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list>.

[114] Office of Public Affairs (2021), "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities," *U.S. Department of Commerce*

In November 2021, the US Commerce Department's Bureau of Industry and Security (BIS) released a final rule adding a number of technology companies—including Candiru and NSO Group—to the Export Administration Regulations' (EAR) "Entity List," which restricts designees from accessing US-origin products or technology.[115] In May 2022, BIS published a final rule implementing new restrictions on cybersecurity items that can be used for malicious cyber activities.[116] As part of the US-EU Trade and Technology Council, the US has also underlined a commitment to "counter the proliferation of foreign commercial spyware and hacking tools by actors that misuse them to target human rights defenders and others, and to promote accountability for companies that are complicit in enabling human rights abuses."[117]

European Union and Member States

The EU and its Member States have also begun to recognize the risks posed by spyware. For example, the European Union Agency for Cybersecurity (ENISA) listed state-sponsored cyber espionage as a major risk in their 2021 Threat Landscape Report.[118] The Catalan government implemented a moratorium on the use of Pegasus spyware in 2023, making it the first European territory to enact such a measure.[119]

Much of the recent discussion around spyware in the EU has focused on establishing how to regulate unlawful state spyware use against EU residents and citizens. The European Parliament launched the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware ("PEGA Committee") in 2022. The PEGA Committee has undertaken an extensive investigation into the use of Pegasus, among other spyware, by the

<https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list>.

[115] U.S., Department of Commerce, Bureau of Industry and Security, *Addition of Certain Entities to the Entity List,* 86(211), FR Doc. 2021-24123, Final rule, November 4, 2021 <https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2021/file> at 60759; Capito, Charles, Brandon L. Van Grack, and Logan Wren (2021), "Recent Additions to Entity List Part of Broader U.S. Effort Targeting Spyware," *Lawfare* <https://www.lawfareblog.com/recent-additions-entity-list-part-broader-us-effort-targeting-spyware>.

[116] Soliman, Tamer A., Rajesh De, David A. Simon, and Anjani D. Nadadur (2021), "BIS Announces New Export Controls on Cybersecurity Items Used for Malicious Cyber Activity," *Mayer Brown* <https://www.mayerbrown.com/en/perspectives-events/publications/2021/10/bis-announces-new-rule-to-limit-exports-of-certain-cybersecurity-products>; Bureau of Industry and Security, *Information Security Controls: Cybersecurity Items*, 87 FR 31948, Final rule, May 26, 2022 <https://www.federalregister.gov/documents/2022/05/26/2022-11282/information-security-controls-cybersecurity-items>.

[117] Office of the Spokesperson (2022), "Joint Statement on Protecting Human Rights Defenders Online," *U.S. Department of State* <https://www.state.gov/joint-statement-on-protecting-human-rights-defenders-online/>.

[118] European Union Agency for Cybersecurity (2021), "ENISA Threat Landscape 2021," *European Union Agency for Cybersecurity* <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021> at 16.

[119] Catalan News (2023), "Catalonia First After US to Restrict Pegasus Spyware Use," *Catalan News* (April 4, 2023) <https://www.catalannews.com/politics/item/catalonia-first-after-us-to-restrict-pegasus-spyware-use>. Note that Costa Rica was the first country to call for a spyware moratorium, see Access Now (2022), "Stop Pegasus: Costa Rica is the First Country to Call for a Moratorium on Spyware Technology," *Access Now* <https://www.accessnow.org/press-release/costa-rica-first-country-moratorium-spyware/>.

governments of Poland, Hungary, Spain, and Greece.[120] It has focused on threats to fundamental human rights, democracy and the rule of law, as well as data security and protection. The PEGA Committee's Draft Report, released in November 2022, made several recommendations, including an immediate moratorium on the sale, acquisition, transfer, and use of spyware, for the EU to agree on a definition of "national security" as it relates to justifying spyware use, the creation of a standard and legal framework for spyware use, and better enforcement mechanisms in existing legislation.[121] In May 2023, the Members of the PEGA Committee adopted the final non-binding report and recommendations, with 30 votes in favour, 3 against, and 4 abstaining for the report, and 30 votes in favour, 5 against, and 2 abstaining, for the recommendations.[122] The PEGA Committee's recommendations will be voted on by all Members of Parliament at their upcoming plenary session in June 2023.[123] Notably, the final recommendations do not contain the Draft Report's call for the immediate moratorium of spyware—instead, it asks that EU states fulfil certain criteria by the end of the year in order to continue using spyware.[124]

Regulatory fragmentation is an ongoing source of concern for the EU. Mercenary spyware companies have been able to circumvent export controls by establishing offices in Member States where export controls are weaker.[125] For example, NSO Group and Intellexa have established subsidiaries in countries including Bulgaria, Cyprus, Greece and Malta to facilitate product sales.[126] This issue of "deliberate lax national implementation," which was identified

[120] European Parliament Press Release (2022), "EP Inquiry Committee for Pegasus and Other Spyware Launched," *European Parliament* <https://www.europarl.europa.eu/news/en/press-room/20220412IPR27112/ep-inquiry-committee-for-pegasus-and-other-spyware-launched>.

[121] Sophie in't Veld (2022), "Draft Report: Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware," *European Parliament Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware (PEGA)* <https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf> at 148–151.

[122] European Parliament Press Release (2023), "Spyware: MEPs Sound Alarm on Threat to Democracy and Demand Reforms," *European Parliament* <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84901/spyware-meps-sound-alarm-on-threat-to-democracy-and-demand-reforms>.

[123] European Parliament Press Release (2023), "Spyware: MEPs Sound Alarm on Threat to Democracy and Demand Reforms," *European Parliament* <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84901/spyware-meps-sound-alarm-on-threat-to-democracy-and-demand-reforms>.

[124] European Parliament Press Release (2023), "Spyware: MEPs Sound Alarm on Threat to Democracy and Demand Reforms," *European Parliament* <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84901/spyware-meps-sound-alarm-on-threat-to-democracy-and-demand-reforms>. See also Amnesty International News (2023), "EU: 'Greater Steps' Needed to Protect Rights After EU Parliament Suggests Regulating Spyware," *Amnesty International* <https://www.amnesty.org/en/latest/news/2023/05/eu-greater-steps-needed-to-protect-rights-after-eu-parliament-suggests-regulating-spyware/>.

[125] Feldstein, Steven, and Brian (Chun Hey) Kot (2023), "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses," *Carnegie Endowment for International Peace* <https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229> at 14.

[126] Feldstein, Steven, and Brian (Chun Hey) Kot (2023), "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses," *Carnegie Endowment for International Peace* <https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229> at 14.

in the PEGA Committee's Draft Report, will persist until there is more consistency in implementation and enforcement.[127]

The EU has also emphasised the need to protect journalists from spyware targeting. The proposed *European Media Freedom Act* (*EMFA*) aims to strengthen media independence, safeguard media pluralism, and increase transparency around media ownership.[128] The *EMFA* proposes safeguards against the use of spyware on media service providers or journalists, although recent reporting suggests a concerning attempt by certain EU governments to water down these protections.[129]

Another focus of EU spyware regulation has been data protection and cybersecurity. The EDPS released a statement to the effect that current iterations of spyware are incompatible with human rights and data protection rights.[130] The EU recently passed the *NIS 2 Directive*, which replaces the *2016 Network and Information Security (NIS) Directive* and sets out a higher standard for cybersecurity within the EU.[131] There is also the proposed *Cyber Resilience Act*, which sets out cybersecurity requirements for manufacturers of digital products to ensure more secure hardware and software.[132]

The Threat of Mercenary Spyware to Canadian National Security

The risks posed to Canada by the proliferation of mercenary spyware are two-fold. First, the adoption of spyware by the Canadian government in the context of law enforcement risks breaching human rights laws, constitutional protections, and corroding Canadian democracy. Fractures to Canadian democracy can become a seedbed of public distrust or discontent and propagate activities which threaten national security. Second, legislative inaction regarding the growing mercenary spyware industry enables the widespread and surreptitious targeting of Canadian government officials, residents, and businesses by hostile state actors, of which Canada is not immune, and itself represents a serious national security risk should a Canadian agency or official be the target.

---

[127] Sophie in 't Veld (2022), "Draft Report: Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware," *European Parliament Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware (PEGA)* <https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf> at 95.
[128] European Commission (2022), "European Media Freedom Act: Commission Proposes Rules to Protect Media Pluralism and Independence in the EU," *European Commission* <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5504>.
[129] Julie Fuchs (2023), "Is the EU Protecting People from Pegasus Spyware?" *Access Now* <https://www.accessnow.org/eu-pegasus-spyware/>; Harald Schumann and Alexander Fanta (2023), "EU governments plan 'blank cheque' to spy on journalists," *Investigate Europe* <https://www.investigate-europe.eu/en/2023/eu-media-freedom-act-governments-exemption-spy-surveillance-journalists/>.
[130] Dunja Mijatović (2023), "Highly Intrusive Spyware Threatens the Essence of Human Rights," *Commissioner for Human Rights* <https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights>.
[131] Cyber Risk GmbH (2022), "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)" *Cyber Risk GmbH* <https://www.nis-2-directive.com/>.
[132] European Commission (2022), "Cyber Resilience Act," *European Commission* <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>; Martinet, Charles, and Romain Bosc (2022), "Europe Uses Spyware on its Own Citizens," *Center for European Policy Analysis (CEPA)* <https://cepa.org/article/europe-uses-spyware-on-its-own-citizens/>.

Threats Arising From Government Use of Spyware

Without adequate safeguards, the purchase and use of spyware by Canadian agencies is likely to replicate the human rights violations seen in other states, and to have a deleterious effect on Canadian democracy. Furthermore, the secretive, unregulated, and easily exploitable nature of this invasive technology hinders and distorts the information ecosystems that citizens need to participate in democratic processes and hold governments accountable. Meaningful "accountability exists when there is a relationship where an individual or institution, and the performance of tasks or functions by that individual or institution, are subject to another's oversight, direction or request that the individual or institution provide information or justification for its actions."[133] Accountability in a democratic state can be divided into horizontal and vertical mechanisms, which involve answerability and enforcement tools.[134] The characteristic secrecy of the spyware industry and its use by the government represents a significant barrier to any meaningful accountability in Canada.

For example, in June 2022, the RCMP revealed it has been using ODITs since at least 2012,[135] citing the increasing challenges of gathering digital evidence during criminal investigations due to quickly evolving technologies.[136] The RCMP's decision to use ODITs was not subject to scrutiny by the Privacy Commissioner, and was quietly revealed in the context of the RCMP's answer to a question on the *Order Paper* in the House of Commons.[137] During the 2022 hearings held by the Standing Committee on Access to Information, Privacy and Ethics ("ETHI Standing Committee Hearings"), which were organised in response to the RCMP's revelation, Public Safety Minister Marco Mendicino insisted that the RCMP's use of surveillance technology was reserved for the "most serious offences" and that interceptions of private communications are done in conformity with the judicial authorization requirements described in the *Canadian Criminal Code,* and within the limits of the *Canadian Charter of*

[133] Riccardo Pelizzo and Frederick Stapenhurst (2013), *Government Accountability and Legislative Oversight* (Routledge: 2013) at 2.

[134] Parsons, Christopher and Adam Molnar (2018), "Government Surveillance Accountability: The Failures of Contemporary Canadian Interceptions Reports," *Canadian Journal of Law and Technology* 1(16) at 148–149 (Vertical accountability refers to the formal mechanisms that oblige certain government agents to answer to a forum, like a government body or department, who has the power to sanction the actor if they fail to perform their duties. Horizontal accountability measures involve informal and indirect mechanisms, where the relevant actor voluntarily discloses information which allows stakeholders, external to government, to provide feedback, raise concerns, and complement the vertical accountability processes in place).

[135] Standing Committee on Access to Information, Privacy and Ethics, "031/1/44 - Evidence - Monday, August 8, 2022" *The House of Commons, Canada* <https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/meeting-31/evidence>.

[136] Maura Forrest (2022), "Canada's National Police Force Admits Use of Spyware to Hack Phones," *POLITICO* (June 29 2022) <https://www.politico.com/news/2022/06/29/canada-national-police-spyware-phones-00043092>; Standing Committee on Access to Information, Privacy and Ethics (2022), "Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues," *The House of Commons, Canada* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-e.pdf> at 5; Standing Committee on Access to Information, Privacy and Ethics, "031/1/44 - Evidence - Monday, August 8, 2022" *The House of Commons, Canada* <https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/meeting-31/evidence>.

[137] Standing Committee on Access to Information, Privacy and Ethics (2022), "Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues," *The House of Commons, Canada* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-e.pdf> at 12–13.

Rights and Freedoms.[138] While Minister Mendicino confirmed that the RCMP does not utilise NSO Group's Pegasus spyware, little substantive information has been made public regarding which specific software is used, how often it is used, or what its impact on human rights or on constitutionally protected rights has been.[139] Currently, only a unit internal to the RCMP—the National Technologies Onboarding Program—reportedly oversees that ODITs used by the RCMP meet the requisite legal and ethical standards.[140] The RCMP did not inform nor consult the Office of the Privacy Commissioner of Canada (OPC) on this internal program.[141] There are no other external oversight mechanisms for the RCMP's information to be corroborated, and the RCMP are not currently bound by any other public reporting obligations nor requirements to prepare privacy impact assessments regarding their use of ODITs.[142] It also remains unclear whether other federal agencies such as Canadian Security Intelligence Service (CSIS),[143] the Communications Security Establishment (CSE) or Canada Border Services Agency (CBSA) use similar spyware in the course of their duties.[144]

---

[138] Standing Committee on Access to Information, Privacy and Ethics, "031/1/44 - Evidence - Monday, August 8, 2022" *The House of Commons, Canada* <https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/meeting-31/evidence>; *Criminal Code,* RSC 1985, c. C-46, <https://laws-lois.justice.gc.ca/eng/acts/c-46/page-26.html#h-118925> at Part VI, Interception of Communications; *Canadian Charter of Rights and Freedoms,* Part I of the *Constitution Act*, *1982,* being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 <https://laws-lois.justice.gc.ca/eng/const/page-12.html>.

[139] Standing Committee on Access to Information, Privacy and Ethics (2022), "Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues," *The House of Commons, Canada* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-e.pdf> at 9–10.

[140] Royal Canadian Mounted Police (2021), "Response to the Report by the Office of the Privacy Commissioner into the RCMP's use of Clearview AI," *Royal Canadian Mounted Police, Government of Canada* <https://www.rcmp-grc.gc.ca/en/news/2021/response-the-report-the-office-the-privacy-commissioner-the-rcmps-use-clearview-ai> ("In March 2021, we created the National Technologies Onboarding Program (NTOP), to centralize and bring more transparency to the processes that govern how the RCMP identifies, evaluates, tracks and approves the use of new and emerging technologies and investigative tools that involve the collection and use of personal information"); See also Standing Committee on Access to Information, Privacy and Ethics, "031/1/44 - Evidence - Monday, August 8, 2022" *The House of Commons, Canada* <https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/meeting-31/evidence> (comments by Minister Mendicino: "[NTOP] will also ensure that a thorough evaluation of the technology is completed, making sure that the technology meets all privacy, legal and ethical standards.").

[141] Office of the Privacy Commissioner of Canada (2022), "Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Study of Device Investigation Tools Used by the RCMP: Opening Statement by Philippe Dufresne Privacy Commissioner of Canada," *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/parl_20220808/>.

[142] Brenda McPhail (2022), "Oral Submission to the Standing Committee on Access to Information, Privacy and Ethics (ETHI) for the Study of Device Investigation Tools Used by the Royal Canadian Mounted Police," *Canadian Civil Liberties Association* <https://ccla.org/wp-content/uploads/2022/08/9-Aug-2022-ETHI-Committee-Submission-on-RCMP-ODIT-Copy.pdf>; Standing Committee on Access to Information, Privacy and Ethics (2022), "Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues," *The House of Commons, Canada* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-e.pdf> at 12–13, 24–25 (M. Dufresne stated that "[i]n its response to the question on the Order Paper, the RCMP indicated that it began drafting a [Privacy Impact Assessment] in relation to these tools in 2021, but [OPC officials] have not yet seen it.")

[143] Standing Committee on Access to Information, Privacy and Ethics, "033/1/44 - Evidence - Tuesday, August 9, 2022," *The House of Commons, Canada* <https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/meeting-33/evidence#Int-11796766> (Former intelligence officer, Mr. Juneau-Katsuya, testified that it is likely that other agencies are using Pegasus-like technology and further admitted that CSIS has surveilled parliamentarians in the past for concern that they are being recruited or paid by foreign agencies).

[144] Standing Committee on Access to Information, Privacy and Ethics (2022), "Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues," *The House of Commons, Canada* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-e.pdf> at 10.

During the ETHI Standing Committee Hearings, government actors consistently cited the need to protect operational secrecy for national security purposes or for the integrity of investigations in their refusal to directly answer questions from the committee.[145] While a level of operational secrecy may be warranted in the context of sensitive investigations, these powerful surveillance technologies have proven ripe for misuse in the absence of strict independent oversight or rigid accountability measures.[146] The contemporary discourse which justifies lack of transparency in the name of operational integrity to address terrorism and serious crime is the same line of reasoning given by other democratic or quasi-democratic governments, who have later abused these technologies against illegal targets for political gain, such as civil activists, dissidents, and journalists. As the Special Rapporteur on human rights and counter terrorism recently noted, counter-terrorism and security rationales "rarely hold" as a justification for the adoption of "high-risk and highly intrusive technologies" and "the claim of exceptional use to respond to security crises is a chimera, when the reality is broad and wholesale use which lacks adequate human rights or rule of law restraints."[147]

The ETHI Standing Committee Hearings demonstrate the gaps within the vertical accountability methods at play in Canada: the government forum lacks the information it needs to bring the actor to account, and there is no real consequence following the lack of transparency or the possibility that legal standards are not being adhered to properly. This lack of information has a domino effect on horizontal accountability actors (civil actors or stakeholders external to government) who are consequently similarly precluded from a meaningful opportunity to provide feedback, voice concerns or disapproval of the policies in place.[148]

---

[145] Standing Committee on Access to Information, Privacy and Ethics, "031/1/44 - Evidence - Monday, August 8, 2022," *The House of Commons, Canada* <https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/meeting-31/evidence > (For e.g., see Minister Mendicino responding to Member of Parliament James Bezan's question regarding which technology is being used: "as I said towards the end of my remarks… the investigative techniques are kept confidential to preserve operational integrity and ensure that we can bring people to justice when necessary").

[146] Brenda McPhail (2022), "Oral Submission to the Standing Committee on Access to Information, Privacy and Ethics (ETHI) for the Study of Device Investigation Tools Used by the Royal Canadian Mounted Police," *Canadian Civil Liberties Association* <https://ccla.org/wp-content/uploads/2022/08/9-Aug-2022-ETHI-Committee-Submission-on-RCMP-ODIT-Copy.pdf>.

[147] UN Human Rights Council (2023) "Human Rights Implications of the Development, Use and Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism," 52nd Sess, UN Doc A/HRC/52/39 <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/reports/A-HRC-52-39-AdvanceEditedVersion.docx> at 1; see also United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism (2023), "Position paper on Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach," *United Nations Special Procedures of the Human Rights Council* <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf> at 18 (on how counter-terrorism justifications, and vague defitnions of "terrorism" have granted governments "largely unchecked" powers to surveil citizens "so long as doing so linked, in some way, to broad and self-defined counter-terrosim objectives").

[148] Standing Committee on Access to Information, Privacy and Ethics, "031/1/44 - Evidence - Monday, August 8, 2022" *The House of Commons, Canada* <https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/meeting-31/evidence> (For e.g Member of Parliament Damien Kurek's comments: "Minister, you are the elected official, the cabinet minister, who provides that oversight that Canadians expect. The fact that there have been less than direct answers I think is very, very telling of that culture of secrecy that seems to be involving… Certainly, I hear often from constituents who are frustrated with the actions of this government when it comes to its unwillingness to be forthcoming with what I think are very, very simple questions").

These accountability gaps are alarming not simply because they create a vacuum where law enforcement agencies may be permitted to operate outside the scope allowed by law. They also threaten national security and democracy more broadly by undermining the public's confidence in governmental institutions and destabilising the integrity of democratic governance.[149] In particular, the breakdown of accountability mechanisms understandably feeds public scepticism regarding legislators' competency in ensuring that the rule of law is being respected, or even of their intentions to take this responsibility seriously.[150] The insistence on secrecy and reticence to disclose information surrounding government use of spyware therefore weakens "the faith that lawful activities are undertaken with the approval, or democratic consent, of the citizenry."[151] This diminishes the public confidence in the institutions charged with protecting them.[152] Recent surveillance scandals in the US and Spain demonstrate that even functioning democracies can "degenerate into severely defective democracies in the future" and destabilise the security of a nation.[153] The adoption of mercenary spyware in the absence of effective systems of oversight that ensure its use is compliant with domestic law by Canadian government bodies risks violating human rights and contributes to the "democratic regression" witnessed around the world in recent years.[154]

Threats Arising From Proliferation of Mercenary Spyware

The use of spyware against government officials, discussed above, makes the proliferation of this technology a pressing national security threat. The Canadian government is not immune to risks posed by the proliferation of the spyware market. The prevalence of spyware use makes Canadian institutions and officials increasingly vulnerable to such acts of cyber espionage, which will undermine the mission of Canadian government institutions and our national security interests.

By positioning itself as another willing customer (assuming it is buying from the private market), the Canadian government contributes to the global spread of the spyware market and its associated dangers.[155] Canada's stagnant legislative action on this issue similarly

[149] See e.g., Clark Campbell (2022), "A Government that Misses Step One in Transparency Sparks a Tizzy about 'Surveillance'," *The Globe and Mail* (January 11 2022) <https://www.theglobeandmail.com/politics/article-a-government-that-misses-step-one-in-transparency-sparks-a-tizzy> (discussing how lack of clear disclosure ahead of time regarding data collection by Public Heath Agency of Canada to deal with COVID-19 contributed to public concerns regarding mass surveillance and diminished confidence in government).
[150] Parsons, Christopher, and Adam Molnar (2018), "Government Surveillance Accountability: The Failures of Contemporary Canadian Interceptions Reports," *Canadian Journal of Law and Technology* 1(16) at 150.
[151] Parsons, Christopher, and Adam Molnar (2018), "Government Surveillance Accountability: The Failures of Contemporary Canadian Interceptions Reports," *Canadian Journal of Law and Technology* 1(16) at 150.
[152] See e.g., Standing Committee on Access to Information, privacy and Ethics (2022), "Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues," *The House of Commons, Canada* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-e.pdf> at 13.
[153] Peter Königs (2022), "Government Surveillance, Privacy and Legitimacy," *Philosophy and Technology* 8(35) at 13.
[154] Ronald J. Deibert (2022), "Subversion Inc: The Age of Private Espionage," *Journal of Democracy* 2(33) at 39.
[155] United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism (2023), "Position paper on Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach," *United Nations Special Procedures of the Human Rights Council* <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulat

enables the market to prosper. As the Special Rapporteur on human rights and counter terrorism noted:

> Responsibility for these grave problems lies not only with the private entities that develop and either knowingly provide such technologies directly to rights-violating regimes or fail to exercise due diligence about the end use of their product, but also with State agencies that misuse these technologies in violation of international and domestic law and with States and international organizations that either actively facilitate or, through lack of robust regulation, have failed to prevent the trade of such technologies into the wrong hands.[156]

Canada lags behind the US and EU in its response to the threats raised by mercenary spyware. The only concrete regulatory tool in Canada that affects the spyware market is the requirement for Canadian companies to apply for licences to export dual-use technology.[157] However, research shows that export controls alone have not been able to address the human right concerns associated with spyware.[158] In particular, such controls only address the export of surveillance technology that falls within the specific scope of the items listed in the dual-use provisions in the *Export and Import Permits Act*, R.S.C., 1985, c. E-19. It does not regulate the purchase or use of such technology by the Canadian government.

The 2022 ETHI Standing Committee Hearings were the first public discussion in Canada on this global issue.[159] The Standing Committee subsequently published a report with nine

---

ion-ct-spyware-technology-trade.pdf> at 22 ("States must be mindful of the risk that the development of such technologies in the private sector, and their promulgation through trade and partnerships between States, raises risks of the transfer and dispersal of this technology to repressive environments, and into the hands of criminals as well as UN designated terrorist organizations").

[156] UN Human Rights Council (2023), "Human Rights Implications of the Development, Use and Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism," 52nd Sess, UN Doc A/HRC/52/39 <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/reports/A-HRC-52-39-AdvanceEditedVersion.docx> at para 46.

[157] Anstis, Siena, Ronald J. Deibert, and Angela Yang (2022), "Submission to the Standing Committee on Access to Information, Privacy and Ethics," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2022/08/Brief-to-the-House-of-Commons-Standing-Committee-on-Access-to-Information-Privacy-and-Ethics.pdf> at 6.

[158] McKune, Sarah, and Ronald J. Deibert (2017), "Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking," *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf> at 7; Heejin Kim (2021), "Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue," *The International & Comparative Law Quarterly* 2(70) <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/global-export-controls-of-cyber-surveillance-technology-and-the-disrupted-triangular-dialogue/3C755DA93E2E1F1F90D38179173334CA> at 380; Anstis, Siena, and RJ Reid (2023), "The Adverse Human Rights Impacts of Canadian Technology Companies: Reforming Export Control with the Introduction of Mandatory Human Rights Due Diligence," *Canadian Journal of Law and Technology* 1(19) <https://digitalcommons.schulichlaw.dal.ca/cjlt/vol19/iss1/3/>.

[159] Ronald J. Deibert, the Director of the Citizen Lab, testified at the Standing Committee with regard to the unique technological capabilities of spyware, human rights, public, and national security risks associated with spyware and the unregulated nature of the mercenary spyware industry, and the need for public debate and the development of a specific legal framework for the use of spyware by government agencies.

recommendations pertaining to the RCMP's use of ODITs.[160] Among other points, the report outlined how lack of a meaningful policy response by the Canadian government undermines human rights protections, democracy, and the rule of law, and threatens national security. It is unclear how the Canadian government has implemented any of the recommendations, or whether there is any political will or interest in doing so.

Conclusion and Recommendations

Inaction in the face of Canadian government agencies using spyware without sufficient oversight and accountability entails serious risks to Canadian constitutional protections and human rights. It also threatens national security as the proliferation of this technology renders Canadian government bodies more vulnerable to surveillance by hostile actors. Inaction in the face of authoritarian and quasi-democratic states illegally employing mercenary spyware diminishes Canada's international reputation as a country committed to upholding and defending international human rights law.[161] Further, Canada fails to protect vulnerable communities in Canada targeted with this technology, such as human rights defenders, journalists, and dissidents who have fled or immigrated to Canada.

Concrete action is needed to aid in the prevention of spyware abuse domestically, as well as to counter the international proliferation of the mercenary spyware industry.[162] With this background in mind, we urge NSICOP to recommend that the Government of Canada take the following preliminary steps regarding mercenary spyware:

1. Impose a moratorium on the sale, export, transfer, and use of spyware until a human-rights compliant safeguards regime is in place;
2. Establish an independent oversight body over the use of spyware by Canadian government bodies;
3. Develop legislation that injects greater transparency into the spyware market both domestic and international (for example, requiring regular reporting by the intelligence community to Parliament on domestic and international spyware companies and threats to Canada);
4. Legally prescribe specific conditions for government hacking and surveillance with spyware that are compliant with the *Charter* and international human rights law (in particular, through potential *Criminal Code* reforms);

[160] Standing Committee on Access to Information, privacy and Ethics (2022), "Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues," *The House of Commons, Canada* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-e.pdf> at 3–4.
[161] Branda McPhail (2022), "Oral Submission to the Standing Committee on Access to Information, Privacy and Ethics (ETHI) for the Study of Device Investigation Tools Used by the Royal Canadian Mounted Police," *Canadian Civil Liberties Association* <https://ccla.org/wp-content/uploads/2022/08/9-Aug-2022-ETHI-Committee-Submission-on-RCMP-ODIT-Copy.pdf>.
[162] UN Human Rights Council (2023), "Human Rights Implications of the Development, Use and Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism," 52nd Sess, UN Doc A/HRC/52/39 <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/reports/A-HRC-52-39-AdvanceEditedVersion.docx> at para 46.

5. Establish effective remedies for victims of spyware targeting and infections by reforming or strengthening laws to facilitate holding governments and companies accountable for the abuse of spyware;
6. Establish a national vulnerability assessment and management process;
7. Make corporate human rights due diligence a legal obligation for spyware companies, with appropriate sanctions for non-compliance;
8. Impose sanctions on spyware companies and individuals contributing to human rights abuses, including developing a 'no buy' list to identify companies from which Canadian government agencies cannot purchase technology and harmonise sanctions with the US and EU; and,
9. End the provision of foreign security and/or surveillance aid, equipment, and training which is likely to be used by recipient foreign governments for human rights abuses.