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

February 15, 2019

For all inquiries related to this submission, please contact:

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

Contributors to this report:

Siena Anstis, Senior Legal Advisor, Citizen Lab
Dr. Ronald J. Deibert, Professor of Political Science; Director, Citizen Lab
Jon Penney, Research Fellow, Citizen Lab; Associate Professor and Director, Law & Technology Institute, Schulich School of Law

Acknowledgments:

We would also like to thank Miles Kenyon (Communications Specialist, Citizen Lab) and Adam Senft (Operations Manager, Citizen Lab) for their support in reviewing this submission.

Table of Contents

Executive Summary

Citizen Lab research on the illegal deployment of spyware technology[1] against human rights and civil society actors demonstrates a troubling lack of concern within the private sector regarding the impact of this technology. Despite extensive reporting, documentation, and public exposure on the negative human rights impacts of spyware technology, private companies remain in denial about the use of their products and continue to state that they do not bear responsibility for any abuse of the technology by purchasers or third parties.

This submission summarizes key Citizen Lab research into the abusive deployment of spyware technology manufactured by NSO Group Technologies Ltd. (a Q Cyber Technologies company), Cyberbit Ltd. (a subsidiary of Elbit Systems Ltd.), FinFisher GmbH (formerly part of Gamma Group), and Hacking Team S.r.l. Collectively, this body of research shows that spyware technology manufactured and sold by private companies is not just used by legitimate actors and within the bounds of the law, but is also deployed against unlawful targets, such as journalists, dissidents, and activists.

This type of unlawful targeting has a number of negative impacts on human rights. Human rights actors are critical to a robust civil society and the maintenance of democratic and rights-respecting norms. The deployment of spyware against such actors limits and impairs their capacity to undertake human rights work and undermines fundamental human rights like freedom of expression and opinion and the right to privacy.[2] Further, emerging research suggests that even the threat of being under surveillance has the capacity to silence human rights actors and consequently undermine fundamental rights.[3]

This submission highlights Citizen Lab research tracking the abusive deployment of spyware manufactured and sold by private companies. It also seeks to highlight four important trends in

[1] This submission focuses specifically on the manufacture, transfer, and sale of spyware technology by private companies as a subcategory of surveillance technologies.
[2] Previous Special Rapporteur reports have addressed the link between freedom of opinion and expression and surveillance technology. See, for example, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/23/40 (17 April 2013) at p 7 (as the Special Rapporteur notes, "[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"); Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/29/32 (22 May 2015) (discussing the relationship between privacy and freedom of opinion and expression in the context of the debate over encryption and anonymity).
[3] See, for example, Jon Penney, "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study" 6:2 Internet Policy Review (2017). Also see sources cited in footnote 21.

the spyware industry, which provide a starting point for any discussion regarding what reforms are required to ensure human rights accountability and the path forward. Specifically:

- Private companies in the spyware industry sell their technology to authoritarian and repressive governments with poor human rights records. Existing regulatory and legislative regimes (such as export controls) do not appear to have been effective against such transfers.

- Private companies in the spyware industry justify the sale of their technology to any government—regardless of that government's human rights record—by arguing that they sell exclusively to sovereign States for the sole purpose of clients engaging in lawful activities and that such sales are done in compliance with all applicable laws.

- Private companies in the spyware industry operate in a non-transparent environment, creating enormous obstacles to evaluating and assessing the use of human rights due diligence processes within the industry or other mechanisms for mitigating human rights impacts.

- In addition to the lack of transparency, private companies in the spyware industry operate in violation of a number of other fundamental human rights principles, such as the right to privacy in the *Universal Declaration of Human Rights* (*UDHR)* and the *International Covenant on Civil and Political Rights* (*ICCPR*) and rights and norms articulated in the *UN Guiding Principles on Business and Human Rights* (*UN Guiding Principles*).

In summary, the current landscape is challenging. Yet, it is not hopeless. It is generally accepted that private companies have to conduct their business activities in a manner that respects human rights and that States have an obligation to protect against human rights abuses committed by business enterprises within their territories. Further, there is a rapidly developing understanding of the dangers of the unchecked sale and deployment of spyware technology not only with respect to human rights, but also in relation to considerations of national security and State sovereignty. Building on these developments, Citizen Lab supplements its submission with recommendations to the Special Rapporteur on areas to prioritize in ongoing efforts to ensure human rights compliance and accountability within the industry and deter against future abuses.

Specifically, Citizen Lab recommends that the Special Rapporteur:

- *Support continued research into spyware industry practices of concern, press for the security and safety of researchers in this space, and issue a public report outlining key practices of concern and the main goals of industry reform.*

- *Draft an accountability framework for the spyware industry based on international human rights norms and equivalent domestic norms and rules and develop a road map for ensuring its effective implementation.*

- *Call on States to take concrete measures to prevent domiciled companies from facilitating, causing, or contributing to human rights abuses internationally, with specific recommendations for States to: make government support or procurement contracts contingent on sound human rights due diligence and other practices; clarify or amend export controls to provide for commercial spyware licensing; establish agencies with power to investigate and remedy corporate human rights abuses abroad; and establish, promote, and support "human-rights-by-design" principles and standards for technology industries.*

About the Citizen Lab

Founded in 2001 by Professor Ronald J. Deibert, the Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security. We use a "mixed methods" approach to research combining methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society; documenting Internet filtering and other technologies and practices that impact freedom of expression online; analyzing privacy, security, and information controls of popular applications; and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Citizen Lab Research on the Use of Private Surveillance Technology Against Human Rights Actors

As part of its research on the application of digital threats against human rights and civil society actors, Citizen Lab publishes reports identifying, analyzing, and documenting the deployment of spyware technology manufactured and sold by private companies, among other types of targeted digital threats. This section provides an overview of Citizen Lab's research into spyware, which is a subset of its work on targeted digital threats.[4] It demonstrates that, while private companies manufacturing and selling spyware routinely argue that their technology is sold only to legitimate governments and law enforcement agencies, it continues to be deployed against human rights and civil society actors and used in an abusive and illegal manner.

1. NSO Group's Pegasus

Citizen Lab has published a number of reports documenting the deployment of NSO Group's[5] Pegasus spyware against a broad range of human rights and civil society actors and other individuals such as journalists, scientists, and politicians. In Mexico alone, Citizen Lab has uncovered a total of 24 individuals who are known to have been abusively targeted with Pegasus.

In brief, Pegasus spyware is a sophisticated tool for spying on mobile phones and is designed to allow an operator to monitor targeted iPhone or Android devices. Among other functions,

[4] Citizen Lab research also investigates other forms of targeted digital threats, such as non-commercial phishing campaigns. For example, in a 2018 report, Citizen Lab analyzed an extensive phishing operation with targets in the Tibetan community. One of the report's conclusions was that simplistic and inexpensive digital operations can still achieve success. In other words, global concern for the use of digital threats against human rights actors should not necessarily focus solely on commercial spyware or expensive surveillance technology. For more information, see Citizen Lab, "Spying On A Budget: Inside a Phishing Operation With Targets in the Tibetan Community" (2018). Similarly, in 2014, the Citizen Lab published a four-year study on the digital threats faced by civil society actors. This report demonstrated that commercial spyware is not the only form of digital threat faced by civil society and human rights defenders and that less expensive forms of such threats can serve to undermine and impair the human rights mandates of civil society organizations. For more information, see Citizen Lab, "Communities @ Risk: Targeted DIgital Threats Against Civil Society" (2014).

[5] NSO Group was previously majority owned by Francisco Partners. In February 2019, NSO Group announced that the company was acquired by its founders and management with support from Novalpina Capital, a European private equity firm. NSO Group describes itself as a Q Cyber Technologies company that is headquartered in Luxembourg (although it also has offices in Israel). For more information on the company, see a non-exhaustive list of resources on NSO Group and other spyware companies that the Citizen Lab has collected: Citizen Lab, "Litigation and Other Formal Complaints Concerning Targeted Digital Surveillance and the Digital Surveillance Industry" (2018).

Pegasus allows an operator to read text messages (including encrypted messages), examine photos, and track a phone's location. It can also silently enable microphones and cameras, turning the phone into a portable surveillance tool to snoop on conversation's happening in the phone's vicinity.

The case of Ahmed Mansoor in the United Arab Emirates

Citizen Lab first reported on Pegasus in the "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender" report. This report documented how an internationally-renowned Emirati human rights defender, Ahmed Mansoor, was targeted with Pegasus spyware in August 2016. Mansoor was the recipient of SMS text messages on his iPhone which promised "new secrets" about detainees tortured in Emirati jails if he clicked on a link included in the text messages. Citizen Lab's investigation determined that the links led to a chain of zero-day exploits[6] that would have remotely jailbroken Mansoor's iPhone 6 and installed sophisticated spyware. Mansoor's phone—once infected—would have become a digital pocket spy, capable of employing his phone's camera and microphone to survey his activities and those of anyone in his vicinity. This would have included recording his WhatsApp and Viber calls (both marketed as secure services), logging messages sent in mobile chat applications, and tracking his movements. While there was no conclusive evidence as to who deployed Pegasus against Mansoor, a number of indicators—in particular, the high cost of zero-day exploits, the apparent use of NSO Group's government-exclusive Pegasus product, and prior known targeting of Mansoor by the UAE—all pointed to the UAE government as the likely cause of the targeting.

Targeting civil society, journalists, politicians, and others in Mexico

In a series of reports, Citizen Lab examined the widespread deployment of Pegasus spyware in Mexico. The first report in this series considered the use of Pegasus spyware against a Mexican government food scientist and two public health advocates who supported the Mexican "soda tax" on sugary drinks in July and August 2016. The second report explained how ten Mexican journalists and human rights defenders, a minor child, and a U.S. citizen were targeted with NSO Group spyware. The targeted individuals were involved or linked to investigations of high-level official corruption or government involvement in human rights abuses in Mexico and the infection attempts often coincided with work on specific high-profile investigations and sensitive issues. The third report detailed the targeting of Mexican politicians with infection attempts using NSO Group's spyware. Subsequent reports showed that NSO Group's spyware

[6] A "zero-day" exploit is a computer software vulnerability that is unknown to those interested in mitigating it. For example, in the case of Mansoor, Apple clearly had an interest in mitigating this vulnerability for Mansoor and any other iPhone user: soon after it was informed by Citizen Lab of the zero-day exploit, it issued a security update affecting more than one billion Apple users worldwide

was being deployed against an international group of experts investigating the Iguala mass disappearance in Mexico, lawyers representing the families of three slain Mexican women, the director of a prominent anti-corruption organization, and Mexican journalists investigating cartels.

Mapping Pegasus infections and the case of Omar Abdulaziz in Canada

In September 2018, Citizen Lab published a report titled "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries." This report identified 45 countries where Pegasus operators might be conducting surveillance operations. In October 2018, Citizen Lab published a follow-up report showing with high confidence that one of the Pegasus spyware infections located in Canada was the cellphone of Omar Abdulaziz, a well-known Saudi activist and Canadian permanent resident. Soon after the publication of that report, it was revealed that Abdulaziz was in close communication with Jamal Khashoggi, a prominent Saudi journalist who was murdered by the Saudi regime in October 2018.

Additional cases of targeting

In addition to analyzing and reporting on the above-mentioned infections/attempted infections, there have been other confirmed cases of NSO Group's Pegasus being used against human rights actors. In August 2018, Amnesty International reported that one of its staff members had been targeted with NSO Group spyware. The staff member received a malicious WhatsApp message with Saudi Arabia-related bait content that belonged to infrastructure connected with NSO Group and previously documented attacks. Through further analysis, Amnesty International also determined that a Saudi-based activist had also received similar messages.[7] In November 2018, it was confirmed that Ghanem al-Masarir, based in London, U.K., was targeted with NSO Group spyware. Al-Masarir is a Saudi dissident and well-known for his YouTube comic and satirical work.

[7] After this discovery, Amnesty International made a request to the Israeli Ministry of Defence asking that NSO Group's defence export license be revoked, which was refused. Amnesty International is currently seeking legal advice in order to revoke the export license. The decision of the Israeli Ministry of Defense not to take any action regarding NSO Group and the documented abuses of its spyware is just one example which calls for greater scrutiny into the effectiveness of export control and other regulatory systems in preventing the sale and transfer of spyware to clients that will engage in illegal uses of the technology. While this submission does not address the state of existing regulations and legislative controls around the manufacture, sale, and transfer of spyware, Citizen Lab has discussed these issues in other papers and forums. See, for example, Ron Deibert and Sarah McKune, "Who's Watching Little Brother?: A Checklist for Accountability in the Industry Behind Government Hacking" (2017). For more information on the state of export control in Canada specifically, see Ron Deibert's 2016 written testimony to the Standing Committee on Human Rights and the Committee's 2018 findings and recommendations.

2. Cyberbit's PC Surveillance System

In 2017, Citizen Lab published a report dealing with the use of commercial spyware against Ethiopian dissidents in the U.S., U.K., and other countries. Citizen Lab's analysis revealed that the dissidents were being targeted with a product called PC Surveillance System (PSS), a commercial spyware product with a novel exploit-free architecture. PSS is sold by Cyberbit, a cyber security company that is a subsidiary of Elbit Systems. Cyberbit marketing materials available at the time explained that PSS could monitor and extract information including "VoIP calls, files, emails, audio recordings, key logs and virtually any information available on the target device."

The initial operations analyzed by Citizen Lab targeted Jawar Mohammed, an activist and Executive Director of the Oromia Media Network. However, additional targets were also discovered after further investigations. These targets included Etana Habte, a PhD candidate and Senior Teaching Fellow at SOAS, University of London, who is a frequent commentator on Ethiopian issues; Dr. Henok Gabisa, a Visiting Academic Fellow teaching in the U.S. and founder of the Association of Oromo Public Defenders in Oromia; Bill Marczak, one of Citizen Lab's staff members who was researching Cyberbit's deployment; and finally a list of 39 additional email addresses were also identified with at least 12 of these being linked to individuals active on Oromo issues or working for Oromo groups. These targets received a link via email to a malicious website impersonating an online video portal. When a target clicked on one of these links, they were invited to download and install an Adobe Flash update containing spyware. In some cases, targets were instead directed to install a fictitious application called "Adobe PdfWriter" in order to view a PDF file.

Based on information revealed in a public log file found on the spyware's command and control server, Citizen Lab further concluded that the spyware's operators appeared to originate from inside Ethiopia and that other victims included various Eritrean companies and government agencies.

3. FinFisher and FinSpy

Citizen Lab has also published multiple reports on FinFisher, a sophisticated computer spyware suite developed by FinFisher GmbH based in Germany (FinFisher was formerly a part of Gamma Group).[8] FinFisher has been marketed as a powerful tool for government IT intrusion and remote monitoring solutions.

[8] As noted, it is our understanding that FinFisher was formerly a part of Gamma Group. FinSpy is one of the spyware products in the FinFisher suite.

While marketed as a tool to fight crime (like NSO Group's Pegasus), the spyware has been implicated in surveillance abuses. Between 2010 and 2012, Bahrain's government used FinFisher to monitor some of the country's top law firms, journalists, activists, and opposition political leaders. In a report entitled "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," Citizen Lab further identified 33 likely government users of FinFisher in 32 countries. The countries identified included some known for human rights abuses such as Saudi Arabia. Citizen Lab was also able to attribute some of the FinFisher Master servers to specific governmental entities by correlating scan results with publicly available data, including emails from FinFisher's competitor Hacking Team. These governmental entities included the Bangladeshi Directorate General of Forces Intelligence, the Belgium Federal Police Service, the Egyptian Technology Research Department, the Indonesian National Encryption Body, the Kenyan National Intelligence Service, the Lebanese General Directorate of General Security, and the Lebanese Internal Security Forces, among others.[9]

4. Hacking Team's Remote Control System

Citizen Lab's investigations have also examined the deployment of Hacking Team's Remote Control System (RCS) against Ethiopian journalists. Hacking Team is an Italy-based company that purports to provide "offensive technology" to worldwide law enforcement and intelligence communities. The spyware manufactured by Hacking Team, RCS, infects a target's computer or mobile phone to intercept data before it is encrypted for transmission and can also intercept data that is never transmitted. This means that it can, for example, copy files from a computer's hard disk and can also record Skype calls, emails, instant messages, and passwords typed into a Web browser. It can also turn on a device's webcam and microphone to spy on the user.

In a 2014 report, Citizen Lab documented how an attacker made three separate attempts to target employees of the Ethiopian Satellite Television Service (ESAT), an independent satellite television radio and online news media outlet run by members of the Ethiopian diaspora. The service had operations in the U.S., as well as other countries, and had been the subject of jamming from within Ethiopia. In a 2015 report, Citizen Lab further detailed how the same attacker again targeted ESAT journalists based in the U.S. with what appeared to be updated versions of the RCS spyware. In this second report, Citizen Lab concluded that the attacker may have been the Ethiopian Information and Network Security Agency (INSA).

[9] In other reports, Citizen Lab also documented the targeted use of FinSpy, which is part of the commercial intrusion kit, FinFisher, against Bahraini activists and a FinSpy campaign in Ethiopia which used pictures of Ginbot 7, an Ethiopian opposition group, as bait.

In addition to reporting on the deployment of RCS against ESAT journalists, Citizen Lab published a report mapping the use of RCS spyware and identified a number of current and/or former government users of the spyware. The report suspected that agencies of the following governments were current or former users of RCS: Azerbaijan, Colombia, Egypt, Ethiopia, Hungary, Italy, Kazakhstan, Korea, Malaysia, Mexico, Morocco, Nigeria, Oman, Panama, Poland, Saudi Arabia, Sudan, Thailand, Turkey, UAE, and Uzbekistan. Through this technical research, Citizen Lab was also able to identify at least 12 cases where U.S.-based *data centres* were part of the RCS infrastructure and were assisting the governments of Azerbaijan, Colombia, Ethiopia, Korea, Mexico, Morocco, Poland, Thailand, Uzbekistan, and the UAE in their use of RCS.

Common Trends among Private Companies in the Surveillance Industry

There is an overwhelming lack of transparency in the corporate practices, policies, and standards used by private companies manufacturing and selling digital surveillance technology. These companies, which appear to work in a business-to-government framework and enter into confidentiality agreements, have demonstrated a general reluctance to discuss their operations. In this section, we highlight some key findings regarding what is known or stated of private company practices of concern in the surveillance industry.

1. Sales to states with poor human rights records

Private companies manufacturing and selling digital surveillance technology sell to a variety of governmental authorities. Some of these authorities are States with poor human rights records. The majority of spyware industry actors do not appear to consider clients engaging in human rights abuses as a deterrent to doing business with them and continue to solicit and engage in such transactions. This has been true for some of the leading companies in the industry, including NSO Group,[10] FinFisher,[11] Cyberbit,[12] and Hacking Team.[13]

[10] NSO Group has admitted to selling its technology to Mexico, which is also reflected in Citizen Lab's multiple reports on the deployment of Pegasus in that country. NSO Group has also sold its technology to the UAE and allegedly to Panama (although NSO Group CEO Shalev Hulio has taken issue with reporting on the identity of NSO Group clients). These clients have troubling human rights records. In late 2018, the UAE upheld a ten-year prison sentence for Ahmed Mansoor. Human Rights Watch's *World Report 2018* describes UAE authorities as having "launched a sustained assault on freedom of expression and association since 2011," among other human rights abuses. It is also well-known that Mexico has a poor human rights record, particularly with regards to the harassment and killing of journalists in the country. NSO Group has also refused to confirm or deny a sale to Saudi Arabia.

[11] In 2014, WikiLeaks released FinFisher company documents. According to the leaked documents, FinFisher customers included law enforcement and government agencies in countries like Bahrain, Nigeria, and Pakistan. In 2013, Citizen Lab had published the results of a global Internet scan for FinFisher command and control servers that appeared in 25 countries, including in Bahrain, Ethiopia, the UAE, Canada, and the United States, among others. In

2. Denial of liability for abuses of spyware

Private companies selling surveillance products have largely adopted a two-part defense to accusations regarding the abuse of their spyware products. First, companies state that their spyware products are sold to legitimate governmental authorities and law enforcement agencies only. Second, that these same products are sold in compliance with all applicable laws and

2018, a number of Bahraini nationals announced that they were suing FinFisher and Gamma Group and alleged that they were targeted with FinSpy malware purchased by the Government of Bahrain. Bahrain is well-known for its poor human rights record–Amnesty International's *Bahrain 2017/2018* report describes the government as engaging in a "large-scale campaign to clamp down on all forms of dissent by repressing the rights to freedom of expression and association of human rights defenders and government critics."

[12] As with NSO Group, there is limited information on Cyberbit's client list. Elbit Systems (Cyberbit is a subsidiary of Elbit Systems) is reported to have engaged in business with clients like Azerbaijan–another country with a troubling human rights record. A recent investigation by *Haaretz* into the Israeli cyber-spy industry reported that Elbit Systems had also supplied Nigeria. Further, Citizen Lab's reporting on Cyberbit revealed that public log files on servers that appeared to be operated by Cyberbit tracked Cyberbit employees as they travelled around the world with infected laptops, apparently providing demonstrations of PSS to the Royal Thai Army, Uzbekistan's National Security Service, Zambia's Financial Intelligence Centre, the Philippines President's Malacanang Palace, ISS World Europe 2017 in Prague, and Milipol 2017 in Paris. Employees also appeared to have provided other demonstrations to France, Vietnam, Kazakhstan, Rwanda, Serbia, and Nigeria. Further, Cyberbit took shape after Elbit Systems acquired Nice Systems. Based on the documents leaked from Hacking Team in 2015, Nice Systems was reported to have assisted with Hacking Team sales to Azerbaijan. It was also reported to have pitched sales to Brazil, Colombia, Guatemala, Honduras, Israel, Kuwait, Finland, Georgia, Greece, India, Turkmenistan, Uzbekistan, and Kyrgyzstan.

[13] As noted, in 2015, Hacking Team was the victim of a hack leading to the disclosure of a significant trove of what appeared to be company documents shedding light on the company's corporate practices and policies. Reporting on these documents revealed that Hacking Team sold to government agencies in countries like Bahrain, Ethiopia, Egypt, Kazakhstan, Morocco, Russia, Saudi Arabia, Sudan, Azerbaijan, and Turkey. In 2014, Citizen Lab published a report mapping the use of Hacking Team's RCS technology and identified a number of current or former government users of the spyware, which included similarly troubling customers. More specifically, Citizen Lab suspected that government agencies of Colombia, Egypt, Ethiopia, the UAE, and Saudi Arabia, among others, were using RCS.

regulations. This has been the position of NSO Group,[14] Hacking Team,[15] and Gamma Group.[16] Cyberbit has also stated that it is not responsible for the unlawful use of its products by clients.[17]

3. Doing business in violation of fundamental human rights

Arbitrary and illegal interference with privacy is in violation of both the *UDHR* and the *ICCPR* and other international treaties.[18] Spyware technology facilitates the violation of these rights when provided to States and other entities that engage in illegal surveillance and cyber

[14] In response to a letter from Citizen Lab regarding the abusive deployment of NSO Group's Pegasus spyware against human rights actors, NSO Group stated that it "develops products that are licensed only to legitimate government agencies for the sole purpose of investigating and preventing crime and terror" and that it "works in full compliance with all applicable laws, including export control laws." The company has also stated that it "operates … under the guidelines and close oversight of all elements of the defense establishment, including all matters relating to export policies and licenses." Similarly, NSO Group's CEO Shalev Hulio explained that NSO Group sales are done with the approval of the Israeli Defense Export Control Agency and only to "sovereign countries and their police and law enforcement organizations and not to private individuals or bodies." Further, NSO Group claims that sales of its spyware are "carried out with a commitment from the buyers that the system will only be used to fight terrorism and crime." After an Amnesty International staff member was targeted with Pegasus spyware, NSO Group stated to the organization that its products were "intended to be used exclusively for the investigation and prevention of crime and terrorism." Interestingly, NSO Group has admitted that it has the capacity to "immediately disconnect" a spyware system. The company's CEO explained that if "a state or an organization wiretaps journalists or human rights activists simply because of their position, it would be considered an inappropriate use of the system, and if we learned about it, the system we sold them would be disconnected immediately. We can do that both technologically and contractually." NSO Group claimed to have shut off the spyware permanently in three cases. In a previous statement to *Haaretz*, however, NSO Group took the position that it was "not involved in the operation of the systems by customers."

[15] After the publication of Hacking Team's internal documents in 2015, the company disputed reports that the company sold its surveillance and intrusion software to repressive regimes in countries that were under sanction. The company stated that it sold its products "strictly within the law and regulation as it applied at the time any sale was made" (the company's website also provides more detail on its current sales policy). The company claimed that this was "true of reported sales to Ethiopia, Sudan, Russia, South Korea and all other countries." Hacking Team has also stated that should the company "discover abuse or misuse" of its products it could "suspend support, which renders the software liable for detection and therefore makes it useless."

[16] In the face of evidence of sales of its products to the Egyptian Security Services, Gamma International maintained that it acted lawfully. In a statement to *The Guardian* in 2011, Gamma International stated that "Gamma International UK Limited manufacturers equipment for dealing with security related threats and it supplies only to governments." It continued to state that it "complies, in all its dealings, with all relevant UK legislation and regulation."

[17] For example, when confronted by Human Rights Watch with Citizen Lab reporting on surveillance abuses in Ethiopia using Cyberbit technology, the company responded that it "operates under strict regulations of the Israeli competent authorities and under a strict export control regime." It noted that "any transaction made by it was approved by the competent authorities"; that all sales are subject to export control; and that their products are only sold "after obtaining all relevant authorizations." The company continued that it "offers its products only to sovereign governmental authorities and law enforcement agencies" and that these authorities and agencies "are responsible to ensure that they are legally authorized to use the products in their jurisdictions." The same responses were included in a letter addressed to Citizen Lab.

[18] See Articles 12 and 19 of the *UDHR* and Articles 17 and 19 of the *ICCPR*. For a review of the applicable international human rights law framework, see Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/23/40 (17 April 2013) at pp. 6-7; Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014) at p. 5; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/32/38 (11 May 2016) at pp. 4-5.

espionage activities. While the issue as to whether these companies may be legally liable for their business activities under national laws and jurisprudence is still evolving, spyware companies do facilitate, encourage, and/or commit such privacy violations through the sale of their technology and by providing continuous technical support to clients who deploy purchased spyware in an illegal manner.[19]

Surveillance also undermines fundamental rights to freedom of expression and to seek, receive, and impart information and ideas codified in both the *UDHR* and *ICCPR*.[20] The threat of surveillance, particularly targeted or personalized forms, can have chilling effects on people's online activities, causing them to self-censor or avoid seeking or imparting certain information online.[21] Given that surveillance disproportionately impacts vulnerable groups, including racial, religious, ethnic, gender, and sexual minorities, these surveillance practices arguably also violate international human rights prohibitions on discrimination and protections for minority rights.[22]

In addition to violations of the *UDHR* and the *ICCPR*, private companies in the spyware industry operate in transgression of numerous principles set out in the *UN Guiding Principles*,[23] such as

[19] For example, in a suit against Gamma Group and FinFisher, Bahraini plaintiffs argue "that the defendants are liable as accessories to the breach of tort of misuse of private information by the Government of Bahrain" and that "the companies sold the spyware to the Bahraini Government during a time when it was well documented that the government was committing human rights violations and that *they continued to provide technical support to the government despite being aware that the spyware was being used to target the claimants while they were in the UK*." (emphasis added).

[20] See Article 19 of both the *UDHR* and *ICCPR*. See also Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/23/40 (17 April 2013) at pp. 7-8, 13-14; Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014) at p. 7; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/32/38 (11 May 2016) at pp. 15.

[21] For empirical and theoretical work on chilling effects and self-censorship, see Jonathon W. Penney, "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study" 6:2 Internet Policy Review (2017); Jonathon W. Penney, "Chilling Effects: Online Surveillance and Wikipedia Use" 31:1 Berkeley Technology Law Journal 117 (2016); Jonathon W. Penney, "Privacy, Chilling Effects, and Personalized Legal Automation: The Case of the DMCA" 22 Stanford Technology Law Review (forthcoming 2019); Frederick Schauer, "Fear, Risk, and the First Amendment: Unraveling the 'Chilling Effect'" 58 Boston University Law Review (1978); Neil Richards, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (Oxford University Press, 2015).

[22] See Article 7 of the UDHR and Articles 26 and 27 of the ICCPR. See also Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/32/38 (11 May 2016) at pp. 15.

[23] The relationship between human rights, private sector obligations, and the *UN Guiding Principles* has been addressed in previous UN documents and reports. See, for example, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/23/40 (17 April 2013) (noting that the corporate sector has "generated a global industry focused on the exchange of surveillance technologies" and that these "technologies are often sold to countries in which there is a serious risk that they will be used to violate human rights, particularly those of human rights defenders, journalists or other vulnerable groups); Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014) (outlining some of the obligations incumbent on companies in the information and communications sector under the *UN Guiding Principles*); Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/32/38 (11 May 2016)

the duties to "respect human rights" (*Guiding Principle 11*[24]); "[a]void causing or contributing to adverse human rights impacts" and "[s]eek to prevent or mitigate" any such impacts "directly linked to their operations" (*Guiding Principle 13*[25]); establishing and carrying out human rights "policies and processes", including a human rights due diligence process and processes "to enable the remediation of any adverse human rights impacts they cause or to which they contribute", and provide for transparency about these policies and processes (*Guiding Principle 15*[26]; *Guiding Principle 17*[27]; *Guiding Principle 21*[28]); and facilitate human rights remediation (*Guiding Principle 22*[29]).

(discussing the role of the private sector in promoting and protecting freedom of expression and outlining the existing framework for private sector responsibilities and what steps are required such as implementing human rights assessment procedures and developing policies that take into account potential impact on human rights); Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, UN Doc CCPR/C/ITA/CO/6 (28 March 2017) (noting a concern about allegations that companies in Italy have been providing online surveillance equipment to governments with a record of serious human rights violations and about the absence of legal safeguards or oversight mechanisms regarding the export of such equipment).

[24] *Guiding Principle 11* provides that businesses "should respect human rights," which means that "they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved." Current practices within the industry suggest that human rights impacts and the infringement of human rights are largely not a concern in conducting business.

[25] *Guiding Principle 13* provides that the responsibility to respect human rights "requires" that businesses "[a]void causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur." It also requires that businesses "[s]eek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts." Businesses in the spyware industry have largely take the position—contrary to the *UN Guiding Principles*—that they do not bear responsibility for the human rights impacts associated with clients' or third parties' use of spyware.

[26] *Guiding Principle 15* provides that businesses "should have in place policies and processes appropriate to their size and circumstance" including a "policy commitment to meet their responsibility to respect human rights," a "human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights," and "[p]rocesses to enable the remediation of any adverse human rights impacts they cause or to which they contribute." The company websites for Cyberbit, Gamma Group, and FinFisher do not publish such policy commitments. Hacking Team has articulated its position on the abuse of surveillance technology on its website. NSO Group's website includes a page on "governance." However, the website does not provide any more information than NSO Group has already stated in response to investigations into the company.

[27] *Guiding Principle 17* states that business enterprises "should carry out human rights due diligence" which should cover, among other issues, the "adverse human rights impacts that the business enterprise may cause or contribute to through its own activities, or which may be directly linked to its operations, products or services by its business relationships." There remains no industry standard on what kind of due diligence is required and companies have provided very limited information regarding what efforts have been undertaken. In 2011, the European Commission commissioned a guide on the implementation of the *UN Guiding Principles* within the ICT sector, which could provide some useful guidance specific to the surveillance industry. See European Commission, "ICT sector guide on implementing the UN Guiding Principles on Business and Human Rights."

[28] For example, commentary to *Guiding Principle 21* notes that showing respect for human rights includes "providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders, including investors." The effectiveness criteria outlined in *Guiding Principle 31* for non-judicial grievance mechanisms also provides that such mechanisms should be "transparent."

[29] *Guiding Principle 22* states that business enterprises "should provide for or cooperate" in the remediation of adverse impacts through "legitimate processes." Spyware companies have largely failed to articulate a policy or process with regards to their responsibility to respect human rights. Nor have spyware companies articulated a comprehensive due diligence process that demonstrates a concern for the human rights impacts of their technology and a mechanism through which to mitigate such negative impacts.

5. Limited national or international measures to hold businesses accountable

Despite such human rights violations, there are limited national and international measures to hold these businesses accountable. States have an international legal obligation to protect against human rights abuses committed by business enterprises within their territories (*Guiding Principle 1*[30]). This includes enacting and enforcing laws and regulations requiring businesses to respect human rights (*Guiding Principle 3*[31]). States should also encourage or require businesses that receive government support or services to carry out human rights due diligence (*Guiding Principle 4*[32]). Yet, no national laws, regulations, or requirements, or their enforcement, prevented these spyware companies from facilitating or contributing to these human rights abuses. Nor have these companies apparently suffered any serious legal or regulatory consequences for doing so.

A central challenge is the business activities contributing to these corporate human rights abuses occur in transnational and international contexts. State obligations to regulate businesses operating extraterritorially for human rights purposes is less clear under international law. Commentaries to the *UN Guiding Principles*, for instance, state that there is no such general obligation under international human rights law.[33] But this position has been criticized as a "weak" and "cautious" formulation by former UN Special Rapporteur Olivier De Schutter, and has likely encouraged States to be more reluctant in taking on these responsibilities.[34] The result is little accountability nationally or internationally for businesses abusing human rights abroad.

4. Non-transparent working environment

While the human rights norms and obligations underlying the *UN Guiding Principles* are all fundamentally important to ensuring human rights compliance, there is one norm in particular

[30] See *Guiding Principle 1,* which provides "States must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises. This requires taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication."
[31] See *Guiding Principle 3,* which provides "In meeting their duty to protect, States should: (a) Enforce laws that are aimed at, or have the effect of, requiring business enterprises to respect human rights, and periodically to assess the adequacy of such laws and address any gaps."
[32] See *Guiding Principle 4,* which provides "States should take additional steps to protect against human rights abuses by business enterprises that are owned or controlled by the State, or that receive substantial support and services from State agencies such as export credit agencies and official investment insurance or guarantee agencies, including, where appropriate, by requiring human rights due diligence."
[33] See Commentary to *Guiding Principle 1*, pp. 3-4.
[34] Olivier De Schutter, "Towards a New Treaty on Business and Human Rights" 1:1 Business and Human Rights *Journal* 41 (2015) at pp. 45-46.

that should receive special consideration in the context of the spyware industry: the need for transparency.[35]

A common theme identified across all private companies in the surveillance industry is a marked lack of transparency–a fact that has been previously noted in research in this area.[36] In addition to refusing to disclose clients, these companies provide little substantive information regarding how they manage the human rights impacts of their spyware, whether they have an effective due diligence system in place that provides tangible and verifiable results, or whether they have implemented accessible and effective grievance systems.[37]

---

[35] See footnote 24.

[36] Lack of transparency has long been a key concern regarding the surveillance industry. In 2012, for example, Electronic Frontier Foundation published a white paper calling for corporations selling surveillance and filtering/block technology to implement robust *Know Your Customer* programs and noted that the first step to mitigating human rights abuses in this sector was transparency. See Cindy Cohn, Trevor Timm and Jillian C. York, "Human Rights and Technology Sales: How Corporations Can Avoid Assisting Repressive Regimes" (2012). In a 2015 policy paper on surveillance and censorship and the impact of technologies on human rights, the European Parliament noted that one of the next steps in this sector was improved transparency by both private companies and government. See Directorate-General for External Policies, Policy Department, European Parliament, "Surveillance and Censorship: The Impact of Technologies on Human Rights" (2015) at p. 29.

[37] Even when information is made available regarding the existence of due diligence practices or a concern for human rights, such information is provided with limited context and without an evidentiary basis. For example, in response to Citizen Lab reporting on the abuse of Pegasus, NSO Group stated that the company has a "Business Ethics Committee, which includes outside experts from various disciplines, including law and foreign relations, reviews and approves each transaction and is authorized to reject agreements or cancel existing agreements where there is a case of improper use." Additional details on the ethics committee that were provided to the *New York Times* on an anonymous basis provide that the company has a "strict internal vetting process to determine who it will sell to," that the "ethics committee" is "made up of employees and external counsel," and that this committee "vets potential customers based on human rights rankings set by the World Bank and other global bodies." It is also allegedly a contractual requirement that the spyware be used only to "investigate and prevent crime or acts of terror." The company has stated that it is their "policy to investigate any allegations of misuse" and claims to have shut down three systems previously due to abuse. In a statement to *Haaretz*, NSO Group further stated that the company did not "sell its products or allow their use in many countries" and that the "company greatly limits the extent to which its customers use its products and is not involved in the operation of the systems by customers." NSO Group has not provided any objective evidence or external auditing to substantiate its claims regarding internal due diligence processes. Hacking Team also once claimed to have an "outside panel of technical experts and legal advisors." In 2014, before internal company documents were made publicly available, the company claimed that it relied on its "own due diligence, published reports, international black lists and conversations with potential clients to assure ourselves to the extent possible that our software will be used legally and responsibly." It further stated that its "panel" reviewed "any potential sale." When pressed for more details on this purported due diligence process, the company declined to identify members of the panel and stated that it could not "specifically describe in detail its work." The company's spokesperson at the time, Eric Rabe, explained that in pre-sale negotiations, the company looked for "red flags that might indicate a risk that our product might be used improperly either in activities that could violate the law or simply due to sloppy deployment that might expose our software." He further noted that, after a sale, if the company discovered "abuse or misuse of our products" it "can suspend support, which renders the software liable for detection and therefore makes it useless." The company refused to disclose whether it had suspended a client (as these were "internal business decisions"), stating only that it had "both suspended support, and refused to do business in the first place with clients or potential clients we believed had or might abuse the software." Internal emails later revealed that this panel was only the law firm Bird & Bird, which apparently did not review every sale. Emails reported on by *The Intercept* indicated that Hacking Team did not necessarily follow its guidelines.

There are numerous reasons for this lack of transparency. For example, the close link between these private companies and State national security, military, and defense bodies suggests that there is a perceived mutual benefit to a lack of transparency in this space.[38] Confidentiality agreements are also routine in the security industry.[39] Further, because the surveillance industry reviewed here sells to governments, there is little external pressure requiring transparency in the context of doing business. Silence is mutually beneficial.

While there may be an argument that some secrecy is necessary in the spyware industry–in light of the fact that spyware is used in sensitive law enforcement activities–this cannot justify the broad, blanket type of secrecy that spyware companies believe they are entitled to regardless of context or the nature of the disclosure. Meeting the obligations set out in the *UN Guiding Principles* does not require spyware companies to reveal sensitive operational details; the fact that law enforcement agencies use spyware cannot justify a *carte blanche* approach to human rights and business practices within the industry itself.

Recommendations

Citizen Lab has prepared a list of recommendations for the Special Rapporteur to be taken into consideration in the process of studying the obligations and responsibilities of States and businesses to ensure compliance with human rights standards in the procurement, transfer, and use of surveillance technologies. These recommendations are primarily drawn from previously-published Citizen Lab reports and papers, including "Planet Netsweeper" by Jakub Dalek et. al.;[40] "Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking" by Ron Deibert and Sarah McKune; and "Advancing Human Rights By Design in the Dual-Use Technology Industry" published in the *Columbia Journal of International Affairs* and co-authored by Citizen Lab's Jon Penney, Sarah McKune, Lex Gill, and Ron Deibert.

[38] The close relationship between the private companies manufacturing surveillance technology and State military and defense in Israel was discussed in this 2018 investigation by *Haaretz* on the spyware industry in Israel.
[39] Ron Deibert and Sarah McKune, "Who's Watching Little Brother."
[40] We also made this recommendation in our Planet Netsweeper Report: Jakub Dalek, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft, and Ron Deibert, "Planet Netsweeper" (2018) at ss. 3.6.1.

1. Describe practices of concern in the spyware industry and the aim of industry reform

The first step in ensuring successful industry reform is determining what industry practices are of pressing concern. While there is limited public information on how the spyware industry functions at least three highly problematic overarching practices of concern can be identified: limited international and national measures to hold businesses accountable, a lack of transparency regarding human rights due diligence policies or processes, and a belief that responsibility for lawful product use lies with the spyware purchaser only. In order to develop a successful and impactful accountability framework, more research is necessary to continue to document and expose these and other practices of concern by the spyware industry. Further, in addition to identifying industry practices of concern, it is also necessary to articulate the aim of industry reform. An initial list of industry reform goals might include addressing some of the clear negative trends within the industry, such as securing transparency regarding due diligence processes, preventing the sale and transfer of spyware technology to certain types of clients through more robust regulation and law, ensuring access to effective remedies for those unlawfully targeted with spyware, and re-allocating negative externalities associated with the spyware industry.

Among the specific activities that the Special Rapporteur could facilitate, we recommend:

1.1 Supporting continued research and investigation into documenting and disclosing corporate practices of concern by civil society, research groups, and other institutions with a human rights-focused mandate and facilitating a public debate and review of such unlawful or unethical corporate practices by spyware industry actors.

1.2 Condemning any activities taken by States or corporate actors to suppress, impair, limit, or otherwise interfere with research being conducted by such bodies into investigating and revealing corporate practices of concern and call on States to take concrete action to prevent such behavior.

1.3 Engaging in a public dialogue on spyware industry reform with all relevant stakeholders and issuing a public report outlining high priority areas of concern and the key aims of spyware industry reform.

Citizen Lab recommends that the UN Special Rapporteur support continued research into spyware industry practices of concern, press for the security and safety of researchers in this

space, and issue a public report outlining key practices of concern and the main goals of industry reform.

2. Develop an accountability framework for the spyware industry and take steps to ensure its implementation and enforcement

A robust accountability framework is required in order to prevent the continued sale of surveillance technology to repressive and authoritarian governments that deploy them in abusive and illegal manners. While it is commonly understood that there is a need for accountability, it is clear from the continued sale of surveillance technology that sufficient progress has not been made in ensuring tangible outcomes. An effective accountability framework needs to respond to the practices of concern within the industry and identified reform priorities, as noted above. Such a framework may be multi-faceted, considering not only international agreements, but also, for example, litigation, regulatory schemes, and export control.

Among the specific activities that the Special Rapporteur could facilitate, we recommend:

2.1 Conducting a comprehensive review of existing accountability mechanisms (such as international frameworks, litigation, regulatory measures, and export control) and issue a public report identifying key gaps and concerns regarding the effectiveness of these mechanisms.

2.2 Based on a review of prior accountability mechanisms and consultation with relevant stakeholders, issuing a public report outlining an accountability framework for the spyware industry, identifying key areas where further action is required by States, and providing a roadmap for action and implementation.

Citizen Lab recommends that the Special Rapporteur draft an accountability framework for the spyware industry based on international human rights norms and equivalent domestic norms and rules and develop a plan for ensuring its implementation and effectiveness.

3. Call on States to take concrete steps to prevent corporate human rights abuses abroad

UN treaty bodies have consistently taken the view that States "should take steps" to prevent human rights abuses internationally by companies incorporated under their laws.[41] And most

[41] De Schutter, "Towards" at p. 45.

international law scholars that have examined this issue, including former UN Special Rapporteur Olivier de Schutter, believe such a State duty to regulate corporate activities human rights abuses abroad already exists under international human rights law.[42] The competence of States to take measures impacting the extraterritorial activities of businesses domiciled in their territories is well established under international law,[43] and as a matter of policy, such measures would also provide guidance and certainty for businesses, while protecting the State's reputation.[44]

Consistent with this duty, the Special Rapporteur should call on States to take concrete steps to prevent corporate human rights abuses internationally. There are many such measures that States could take pursuant to this duty. Among those we recommend:

3.1 Where States provide direct or indirect support to businesses operating abroad, financial or otherwise, that support should be tied to clear prohibitions against unlawful and unethical activities, and effective and ongoing due diligence, public transparency reporting, and other accountability measures to ensure compliance with these prohibitions. Such requirements could be backed by effective penalties for non-compliance, including mechanisms to freeze and, where appropriate, revoke financial support and services.[45]

3.2 States should establish human rights-oriented government procurement standards for "dual-use" technology companies like spyware businesses. These could restrict the awarding of government contracts to those businesses that have human rights policies and due diligence processes in place, and strong records of respect for human rights overseas.[46]

3.3 States should follow Europe's lead and clarify or amend export controls to require licensing for spyware and surveillance technologies that is provided to designated end users and/or for designated end uses that present significant human rights risks.[47]

[42] O'Brien, "The Home State Duty" at pp. 49-51; De Schutter, "Towards" at pp. 43-45.
[43] De Schutter, "Towards" at pp. 46.
[44] See Commentary to *Guiding Principle 1* at pp. 3-4.
[45] Citizen Lab also made this recommendation in the Planet Netsweeper Report: Jakub Dalek, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft, and Ron Deibert, "Planet Netsweeper" at ss. 3.6.1.
[46] See Jakub Dalek et al., "Planet Netsweeper" at ss. 3.6.1.
[47] See Jakub Dalek et al., "Planet Netsweeper" at ss. 3.6.1.

3.4 States should establish agencies with powers to investigate and remedy human rights abuses committed internationally by domiciled companies.[48]

3.5 States should support "human-rights-by-design" principles whereby business commit to designing tools, technologies, and services to respect human rights by default, rather than permit abuse or exploitation as part of their business model. A human-rights-by-design paradigm, for example, could prevent spyware companies from designing surveillance tools and technologies easily repurposed for human rights abusing activities.[49]

Citizen Lab recommends that the Special Rapporteur call on States to take concrete measures to prevent domiciled companies from facilitating, causing, or contributing to human rights abuses internationally, with specific recommendations for States to: make government support or procurement contracts contingent on sound human rights due diligence and other practices; clarify or amend export controls to provide for commercial spyware licensing; establish agencies with power to investigate and remedy corporate human rights abuses abroad; and establish, promote, and support "human-rights-by-design" principles and standards for technology industries.

[48] For example, in 2018, the Government of Canada established the Canadian Ombudsperson for Responsible Enterprise (CORE) with a mandate to "investigate allegations of human rights abuses linked to Canadian corporate activity abroad" and "empowered to independently investigate, report, recommend remedy and monitor its implementation" (although note that the position of Ombudsperson has yet to be filled). See Jakub Dalek et al., "Planet Netsweeper" at ss 3.6.2.

[49] See Jon Penney, Sarah McKune, Lex Gill, and Ron Deibert, "Advancing Human Rights By Design in the Dual-Use Technology Industry" 71:2 Columbia Journal of International Affairs (2018).