Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances

18 June 2022

For all inquiries related to this submission, please contact:

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

Contributors to this report (in alphabetical order):

Siena Anstis (Senior Legal Advisor, The Citizen Lab)
Dr. Ronald J. Deibert, (Professor of Political Science; Director, The Citizen Lab)
Émilie LaFlèche (Research Trainee, The Citizen Lab)
Jon Penney (Citizen Lab Fellow, Associate Professor, Osgoode Hall Law School)

I. Introduction

In September 2014, a group of forty-three students were forcibly disappeared in Iguala, Mexico.[1] The devices of a group of experts subsequently investigating this mass disappearance, including for possible governmental involvement, were targeted for

[1] Forensic Architecture, "The Enforced Disappearances of the Ayotzinapa Students" *Forensic Architecture* <https://forensic-architecture.org/investigation/the-enforced-disappearance-of-the-ayotzinapa-students>.

infection with NSO Group's Pegasus spyware.[2] Evidence suggests that these spyware attacks "were clearly intended to compromise the privacy and integrity of the [...] investigative process."[3] The spyware attacks against the investigators of this mass disappearance is only one illustration of the intimate link between spyware and human rights abuses. These abuses have included enforced disappearances, as spyware has facilitated states' ability to conduct unlawful surveillance, track dissidents and their associates, and interfere in investigations related to disappearances.

Investigations by research groups such as the Citizen Lab and Amnesty International have uncovered that states around the world, ranging from Saudi Arabia to Rwanda, are using new surveillance technologies to monitor human rights defenders, journalists, and political opponents, among others. The global spyware industry which has contributed to the proliferation of these new surveillance technologies has been characterized as "out of control,"[4] "assisting state suppression,"[5] "undermining freedom,"[6] and "a threat to democracy."[7] These new technologies have allowed states to expand their surveillance capabilities to an unprecedented degree, particularly through the ubiquity of cell phones and other devices that can relay information about a target's location, private

[2] John Scott-Railton, Bill Marczak, Bahr Abdul Razaak, Masashi Crete-Nishihata, and Ron Deibert (2017), "Reckless III: Investigation Into Mexican Mass Disapppearance Targeted with NSO Spyware," *The Citizen Lab* <https://citizenlab.ca/2017/07/mexico-disappearances-nso/>.
[3] John Scott-Railton, Bill Marczak, Bahr Abdul Razaak, Masashi Crete-Nishihata, and Ron Deibert (2017), "Reckless III: Investigation Into Mexican Mass Disapppearance Targeted with NSO Spyware," *The Citizen Lab* <https://citizenlab.ca/2017/07/mexico-disappearances-nso/>.
[4] Amnesty International (2021), "Pegasus Project: Apple iPhones Compromised by NSO Spyware," *Amnesty International* (19 July 2021) <https://www.amnesty.org/en/latest/news/2021/07/pegasus-project-apple-iphones-compromised-by-nso-spyware/>.
[5] David Kaye (2019), "The Surveillance Industry is Assisting State Suppression. It Must Be Stopped," *The Guardian* (26 November 2019) <https://www.theguardian.com/commentisfree/2019/nov/26/surveillance-industry-suppression-spyware>.
[6] Joel Simon (2021), "WhatsApp Head Will Cathcart: The Spyware Industry is Undermining Freedom," *Committee to Protect Journalists* (26 July 2021) <https://cpj.org/2021/07/whatsapp-will-cathcart-spyware-undermining-freedom/>.
[7] Noel King (2021), "Former U.N. Adviser Says Global Spyware is a Threat to Democracy," *NPR* (20 July 2021) <https://www.npr.org/2021/07/20/1018226161/global-spyware-is-a-threat-to-democracy-former-u-n-advocate-says>.

communications, and other activities. Technologies touted by activists, human rights defenders, and scholars[8] as essential tools for democratization and the proliferation of human rights have thus been transformed into tools of oppression by this mercenary spyware. Without intervention, the use of spyware will only further proliferate and create an increasingly insecure world for human rights defenders, journalists, and government critics.

The Citizen Lab welcomes the opportunity to submit to the UN Working Group on Enforced and Involuntary Disappearances ("Working Group"). The Citizen Lab is at the forefront of investigating and reporting on abuses of mercenary spyware. Our submission highlights the capabilities of spyware and the nature of the spyware industry; how surveillance technology is used to violate fundamental human rights, and more particularly how it is related to enforced disappearances; and we provide recommendations for states, spyware companies, other businesses, civil society, and the Working Group.[9]

II. What is mercenary spyware?

Spyware is a form of malware that allows an operator to gain access to—or hack—a device and extract, modify, or share its contents. Spyware may also be referred to as "intrusion software," "offensive cyber capabilities," or "access as a service."[10] Devices can be infected with malware through several different vectors. First, infections can occur through socially engineered links, or "exploit links," in which malicious links are designed to trick targets into clicking them. Once clicked, the malware targets software

[8] See e.g. Mohammed M. Arman (2013), "ICT, Social Media, and the Arab Transition to Democracy: From Venting to Acting," 22(2) *Digest of Middle East Studies*; Farid Shirazi (2008), "The Contribution of ICT to Freedom and Democracy: An Empirical Analysis of Archival Data on the Middle East," 35(6) *Electronic Journal of Information Systems in Developing Countries.*
[9] The Citizen Lab, "Targeted Threats," *The Citizen Lab* <https://citizenlab.ca/category/research/targeted-threats/>.
[10] Winnona DeSombre, James Shires, JD Work, Robert Morgus, Patrick Howell O'Neill, Luca Allodi, and Trey Herr (2021), "Countering Cyber Proliferation: Zeroing in on Access-as-a-Service," *Atlantic Council* <https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/>.

vulnerabilities, allowing the malware to be installed without the target's consent or knowledge.[11] For example, a lawyer who represented former president Carles Puigdement of Catalonia was successfully infected with Pegasus spyware after clicking a link which appeared to be an app update.[12] Second, devices can be infected with zero-click exploits, in which no action has to be taken by the target for the spyware to infect their device. For example, a target's phone may be infected after receiving a phone call that they do not answer.[13] In 2020, the Citizen Lab found that the phones of thirty-six journalists, executives, and others working at *Al Jazeera* were infected with Pegasus from what was likely a zero-click iMessage exploit.[14] Third, spyware can be manually installed on a user's phone. Evidence suggests that UAE officials at a Dubai airport manually installed Pegasus spyware on Jamal Khashoggi's wife's phone in a matter of minutes.[15]

Depending on the sophistication of the spyware, an infection may give the perpetrator full access to a target's device. The Citizen Lab has reported that a Pegasus infection gives state actors access to all of the target phone's content and passwords, as well as the ability to download files, listen to telephone calls, track the target's location, and

[11] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert (2018), "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab* at 7 <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.
[12] Ronan Farrow (2022), "How Democracies Spy on Their Citizens," *The New Yorker* (18 April 2022), <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>.
[13] Bill Marczak, John Scott-Railton, Noura Al-Jiwazi, Siena Anstis, and Ron Deibert (2020), "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit," *The Citizen Lab* at 2 <https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/>.
[14] Bill Marczak, John Scott-Railton, Noura Al-Jiwazi, Siena Anstis, and Ron Deibert (2020), "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit," *The Citizen Lab* at 1 <https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/>. See also Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jiwazi, Siena Anstis, Kristin Berdan, and Ron Deibert (2021), "FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild," *The Citizen Lab* <https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/>.
[15] Dana Priest (2021), "A UAE Agency Put Pegasus Spyware on Phone of Jamal Khashoggi's Wife Months Before his Murder; New Forensics Show," *The Washington Post* (21 December 2021) <https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/>.

remotely turn on the microphone and camera.[16] These infections can even successfully target encrypted calls and messages.[17] Similarly, when Candiru spyware infects a device, it can extract files and messages from encrypted apps, as well as cookies and passwords, and can use the target's Cloud accounts to send and post messages, making it appear as though the target sent them.[18] Hacking Team's (now rebranded as Memento Labs) Remote Control System spyware can also collect data from devices, including files, encrypted communications, and passwords. Their spyware can remotely activate microphones and cameras.[19] Gamma Group's FinFisher spyware can access data from various apps, including contact lists, files, and geolocation, in addition to monitoring communications from encrypted applications.[20] FinFisher can also send targets silent calls (known as "SpyCalls") to listen to the phone's surroundings.[21]

III. Background on the spyware industry

The spyware industry has thrived over the course of the last decade, as states are increasingly buying and using surveillance technology. The industry was valued at an

[16] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert (2018), "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab* at 7 <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.
[17] The Citizen Lab (2022), "Would You Click?" *The Citizen Lab* <https://catalonia.citizenlab.ca/>.
[18] Bill Marczak, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert (2021), "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus," *The Citizen Lab* <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/>.
[19] Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton (2014), "Mapping Hacking Team's 'Untraceable' Spyware," *The Citizen Lab* <https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/>; Joseph Cox (2020), "Memento Labs, the Reborn Hacking Team, Is Struggling," *Motherboard* (31 March 2020) <https://www.vice.com/en/article/xgq3qd/memento-labs-the-reborn-hacking-team-is-struggling>.
[20] Access Now (2018), "Alert: FinFisher Changes Tactics to Hook Critics," *Access Now* at 13 <https://www.accessnow.org/cms/assets/uploads/2018/05/FinFisher-changes-tactics-to-hook-critics-AN.pdf>.
[21] Morgan Marquis-Boire, Bill Marczak, and Claudio Guarnieri (2012), "The SmartPhone Who Loved Me: FinFisher Goes Mobile?" *The Citizen Lab* <https://citizenlab.ca/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/>.

estimated 12 billion dollars in 2018,[22] and NSO Group's spyware alone has been identified in forty-five states.[23] In 2016, there were "over five hundred companies developing, marketing and selling [digital surveillance] products to government purchasers."[24] Every aspect of the industry is cloaked in secrecy, from who buys and sells the products,[25] to the secret trade shows which promote the spyware,[26] to the names of the spyware companies.[27] Companies who sell spyware tend to operate using a complex sales structure including multiple corporate entities operating from a range of countries, making it difficult to monitor and report on their activities, in particular where companies are applying for and receiving export licences.[28]

There is very little regulation of the commercial spyware industry at domestic or international levels, allowing private surveillance corporations like NSO Group to

[22] Ronan Farrow (2022), "How Democracies Spy on Their Citizens," *The New Yorker* (18 April 2022), <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>.
[23] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert (2018), "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab* (18 September 2018) <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.
[24] UN Human Rights Council (2019), "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," 41st Sess, UN Doc A/HRC/41/35 at para 6 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement>.
[25] See e.g. Merlin Delcid (2022), "El Salvador Denies Responsibility for Hacking Journalists After Report Finds Pegasus Spyware on their Phones," *CNN World* (13 January 2022) <https://www.cnn.com/2022/01/13/americas/el-salvador-pegasus-spyware-intl/index.html >.
[26] Ilya Lozovsky (2021), "Where NSO Group Came From – Any Why It's Just the Tip of the Iceberg," *OCCRP* (20 July 2021) <https://www.occrp.org/en/the-pegasus-project/where-nso-group-came-from-and-why-its-just-the-tip-of-the-iceberg>.
[27] For example, the mercenary spyware company "Candiru" has changed its name to "DF Associates Ltd.," "Grindavik Solutions Ltd.," "Taveta Ltd.," and "Saito Tech Ltd." (Bill Marczak, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert (2021), "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus," *The Citizen Lab* <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/>).
[28] See e.g. Bill Marczak, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert (2021), "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus," *The Citizen Lab* <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/> (Candiru "makes efforts to keep its operations, infrastructure, and staff identities opaque to public scrutiny.").

operate largely without scrutiny. Export control is currently the primary regulatory mechanism that impacts the commercial spyware industry at a global level. The *Wassenaar Arrangement* is a non-binding, multilateral export regime with forty-two participating states. The regime sets out controls on the export of dual-use technologies, which includes "intrusion software" and "IP network communications surveillance systems."[29] Participating states are to implement these export regulations domestically through legislation. The regime has been criticized as woefully inadequate in addressing human rights concerns associated with the mercenary spyware industry. States may be slow or reluctant to implement controls, and the regime is non-binding.[30] The *Arrangement* is not concerned with exports that will infringe on human rights or have a negative impact on such rights. As summarized by Dr. Ronald Deibert and Sarah McKune:

> "[e]xport regulations do not prohibit the trade in spyware; rather, they establish a licensing framework that relies entirely on informed and unbiased decision-making by national-level export authorities. They are designed to account for security considerations while also facilitating commerce to the extent possible. There is simply no guarantee that licensing parameters and decisions in any given state will properly account for human rights concerns."[31]

Beyond the regulation of dual-use exports, there is no specific regime addressing the international trade of mercenary spyware and few countries have adopted domestic

[29] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (2021), "Public Documents: Volume II, List of Dual-Use Goods and Technologies and Munitions List" (December 2021) <https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-II-2021-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-2021.pdf>.
[30] Brandon L. Van Grack and Charles K. Capito (2021), "BIS Releases Interim Final Rule on Export Controls for Cybersecurity Items," *Morrison & Foerster* (5 November 2021) <https://www.mofo.com/resources/insights/211105-bis-releases-interim-final-rule.html>.
[31] Sarah McKune and Ron Deibert (2017), "Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking," *The Citizen Lab* <https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf>.

legislation that specifically covers the use of Pegasus-like spyware by government bodies such as law enforcement and intelligence agencies.[32]

Spyware companies typically deflect criticism by framing their technology as tools to combat terrorism and crime.[33] Notably, NSO Group has used the fact that they sell their product exclusively to governments as both a justification and a marketing tactic. They further claim that the company "only sells to 'vetted government agencies' for use against terrorists and major criminals."[34] Reports by civil society organizations and journalists paint a different picture. Amnesty International's Secretary General has argued that NSO Group's justifications are not credible when considering the number of activists, journalists, and other members of civil society under unlawful surveillance, noting that "the company can no longer hide behind its claims when its spyware is clearly being used for repression on a global scale."[35] NSO Group is not the only spyware company with significant discrepancies between their affirmation for human rights and business practices, however. Hacking Team also claimed that they would "refuse to provide or cease providing products or services to entities that Hacking Team believes uses its products to violate human rights."[36] Despite such a policy, Citizen Lab

[32] Heejin Kim (2021), "Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue," 70 *International and Comparative Law Quarterly* at 380; Jonathon W. Penney and Bruce Schneier (2021), "Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group," 36 *Berkeley Technology Law Journal* at 137.
[33] The Citizen Lab (2019), "NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases," *The Citizen Lab* <https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/>; Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton (2014), "Mapping Hacking Team's 'Untraceable' Spyware," *The Citizen Lab* <https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/>.
[34] The Associated Press (2021), "Hundreds of Journalists, Activists Among Firm's Spyware Targets, Probe Finds," *CBC News* (19 July 2021) <https://www.cbc.ca/news/world/spyware-journalists-activists-1.6108070>.
[35] Amnesty International (2021), "Pegasus Project: Rwandan Authorities Chose Thousands of Activists, Journalists and Politicians to Target with NSO Spyware," *Amnesty International* <https://www.amnesty.org/en/latest/news/2021/07/rwandan-authorities-chose-thousands-of-activists-journalists-and-politicians-to-target-with-nso-spyware/>.
[36] The Citizen Lab (2014), "Open Letter to Hacking Team," *The Citizen Lab* <https://citizenlab.ca/2014/08/open-letter-hacking-team/>. Note that Hacking Team's original policy is no longer available online.

findings suggest that Hacking Team's products kept being used by Ethiopian authorities to target Ethiopian journalists in Washington, even after widespread reporting on the issue by various news outlets and research groups.[37] After the company's servers were hacked in 2015, data released by WikiLeaks showed that the company was engaged in or considering business with a variety of repressive regimes.[38]

Mercenary spyware has repeatedly been used against civil society, journalists, and political opponents rather than only people committing crimes.[39] States with poor human rights records, such as Hungary and Saudi Arabia, are Pegasus customers.[40] Spyware has also been used to spy on other governments, presenting significant national and international security risks. For example, French President Emmanuel Macron and a device in UK Prime Minister Boris Johnson's office have been targeted by Pegasus spyware.[41] In May 2022, Madrid announced that the devices of Spanish Prime Minister Pedro Sánchez and Defense Minister Margarita Robles had been infected with Pegasus spyware. The infection of Sánchez's device was the first confirmed instance of a

[37] Bill Marczak, John Scott-Railton, and Sarah McKune (2015), "Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware," *The Citizen Lab* <https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/#>.

[38] Alex Hern (2014), "Hacking Team Hack Casts Spotlight on Murky World of State Surveillance," *The Guardian* (11 July 2014) <https://www.theguardian.com/technology/2015/jul/11/hacking-team-hack-state-surveillance-human-rights>.

[39] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert (2018), "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab* at 25 <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>; Amnesty International (2021), "Pegasus Project: Rwandan Authorities Chose Thousands of Activists, Journalists and Politicians to Target with NSO Spyware," *Amnesty International* <https://www.amnesty.org/en/latest/news/2021/07/rwandan-authorities-chose-thousands-of-activists-journalists-and-politicians-to-target-with-nso-spyware/>.

[40] Daniel Estrin (2021), "What to Know about the Spying Scandal Linked to Israeli Tech Firm NSO," *NPR* (25 August 2021) <https://www.npr.org/2021/08/25/1027397544/nso-group-pegasus-spyware-mobile-israel>.

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

European or NATO leader being successfully hacked.[42] Moreover, spyware technology intended for government use does not always remain in the hands of governments. Reports by *The Guardian* have shown that some Mexican government officials helped Mexican drug cartels procure mercenary spyware, including spyware by NSO Group and Hacking Team.[43]

Both authoritarian and democratic governments have purchased spyware technology—Pegasus customers include Saudi Arabia, Poland, Mexico, Rwanda, and Germany.[44] The United States' Federal Bureau of Investigation (FBI) has admitted to buying Pegasus, though the FBI claims not to have used it.[45] Importantly, human rights abuses linked to mercenary spyware are not limited to authoritarian governments. In April 2022, the Citizen Lab uncovered that spyware had been used to infect the phones of at least 65 Catalan activists and politicians as well as their friends, families, and associates between 2015 and 2020.[46] Evidence suggests that the Spanish government is behind the attacks. It was also revealed in December 2021 that Pegasus spyware had been used to infect the devices of Polish government critics.[47] The Polish

[42] Vincent Manancourt (2022), "Hack of Spanish PM's Phone Deepens Europe's Spyware Crisis," *Politico* (2 May 2022) <https://www.politico.eu/article/pegasus-hacking-spyware-spain-government-prime-minister-pedro-sanchez-margarita-robles-digital-espionage-crisis/>.
[43] Cecile Schilis-Gallego and Nina Lakhani (2020), "'It's a Free-for-All': How Hi-Tech Spyware Ends up in the Hands of Mexico's Cartels," *The Guardian* (7 December 2020) <https://www.theguardian.com/world/2020/dec/07/mexico-cartels-drugs-spying-corruption>.
[44] DW, "German Police Secretly Bought NSO Pegasus Spyware," *DW* (7 September 2021) https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197; Ronan Farrow (2022), "How Democracies Spy on Their Citizens," *The New Yorker* (18 April 2022), <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>.
[45] Ronan Farrow (2022), "How Democracies Spy on Their Citizens," *The New Yorker* (18 April 2022), <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>.
[46] John Scott-Railton, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, and Ron Deibert (2022), "CatalanGate: Extensive Mercenary Spyware Operation Against Catalans Using Pegasus and Candiru," *The Citizen Lab* <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>.
[47] Stephanie Kirchgaessner (2022), "More Polish Opposition Figures Found to Have Been Targeted by Pegasus Spyware," *The Guardian* (17 February 2022)

government admitted to having bought the spyware, but denied using it for "political purposes."[48] Targets included Krzysztof Brejza during the 2019 election in which he headed an opposition party's campaign; Roman Giertych, a lawyer who represented the former prime minister of Poland and current leader of an opposition party; and Ewa Wrosek, a prosecutor who has been fighting against Polish judicial reforms that threaten the separation of powers.[49]

IV. Dangers and risks posed by mercenary spyware for human rights defenders

Mercenary spyware poses grave risks to human rights defenders both domestically and transnationally and has met widespread criticism regarding the heightened risk of human rights violations. The European Data Protection Supervisor (EDPS) recently stated that spyware "has the potential to cause unprecedented risks and damages not only to the fundamental freedoms but also to democracy and the rule of law."[50] Notably, the use of spyware can lead to violations of the rights to privacy, freedom of speech and assembly, and life, liberty and security.

Spyware has been shown to significantly curtail the rights to freedom of expression and assembly, which are guaranteed under Articles 19(2) and 21 of the *International*

<https://www.theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware>.

[48] DW, "Poland: Top Leader Admits Government Bought Pegasus Spyware," *DW* (7 January 2022) <https://www.dw.com/en/poland-top-leader-admits-government-bought-pegasus-spyware/a-60361211>.

[49] Frank Bajak and Vanessa Gera, "Exclusive: Polish Opposition Duo Hacked with NSO Spyware," *AP News* (21 December 2021) <https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e>; Jo Harper (2021)," 'Poland Has Crossed the Rubicon.' Tusk's Lawyer Slams Government Over Alleged Spyware Use," *Politico* (30 December 2021) <https://www.politico.eu/article/roman-giertych-donald-tusk-poland-spy-journalists-lawyers-opposition-citizen-lab-rzeczpospolita/>.

[50] Daniel Boffey (2022), "EU Data Watchdog Calls for Pegasus Spyware Ban," *The Guardian* (15 February 2022) <https://www.theguardian.com/world/2022/feb/15/eu-data-watchdog-calls-for-pegasus-spyware-ban>.

Covenant on Civil and Political Rights ("ICCPR").[51] The use of spyware creates a chilling effect in civil society, as it leads to self-censorship and other types of behavioural modifications.[52] Importantly, human rights defenders may self-censor because of the *threat* of surveillance, and not only when they are actually being surveilled.[53] Cognisant of the spectre of surveillance, human rights defenders may choose to self-censor to avoid jeopardizing their safety and the safety of their loved ones.[54] They may also self-censor for fear of having confidential communications heard.[55] The contents of a target's phone can also be used to blackmail or intimidate activists, further compounding the risk of self-censorship. Both the threat and the actual use of mercenary spyware technology therefore impedes democratization efforts, the advancement of human rights, and "helps preserve [the] status quo" by censoring actors trying to hold governments to account.[56] For example, spyware has become an

[51] *International Covenant on Civil and Political Rights*, 19 December 1966, 999 UNTS 171, arts 19(2), 21 (entered into force 23 March 1976).
[52] Jonathon W. Penney (2021), "Understanding Chilling Effects," 106 *Minnesota Law Review* at 105–106. See also, for example, Lee Rainie and Mary Madden (2015), "Americans' Privacy Strategies Post-Snowden," *Pew Research Center* at 4 <https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf>.
[53] Noura Al-Jizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert (2022), "Psychological and Emotional War: Digital Transnational Repression in Canada," *The Citizen Lab* at 10 <https://citizenlab.ca/2022/03/psychological-emotional-war-digital-transnational-repression-canada/>; Dana M. Moss (2016), "The Ties that Bind: Internet Communication Technologies, Networked Authoritarianism, and 'Voice' in the Syrian Diaspora," *Globalizations* 15(2) at 273; Jonathon W. Penney (2021), "Understanding Chilling Effects," 106 *Minnesota Law Review* at 142–143, 163–164.
[54] Dana M. Moss (2016), "The Ties that Bind: Internet Communication Technologies, Networked Authoritarianism, and 'Voice' in the Syrian Diaspora," *Globalizations* 15(2) at 276–277; Sagi Elbaz, Tamir Magal, Rafi Nets-Zehngut, and Guy Abutbul (2017), "Self-Censorship of Narratives of Political Violence in the Media," in *Self-Censorship in the Contexts of Conflict: Theory and Research*, Ed. Daniel Bar-Tal, Rafi Nets-Zehngut and Keren Sharvit (2017: Springer International Publishing) at 129.
[55] Human Rights Watch (2021), "Unchecked Spyware Industry Enables Abuses," *Human Rights Watch* <https://www.hrw.org/news/2021/07/30/unchecked-spyware-industry-enables-abuses>; Sarah Myers West (2017), "Ambivalence in the (Private) Public Sphere: How Global Digital Activists Navigate Risk," *FOCI '17* at 2, 6 <https://www.usenix.org/conference/foci17/workshop-program/presentation/west>.
[56] Stephanie Kirchgaessner (2022), "'Most Harmful Thing' – How Spyware is Stifling Human Rights in Bahrain," *The Guardian* (18 February 2022) <https://www.theguardian.com/news/2022/feb/18/how-spyware-erodes-human-rights-in-bahrain-nso-group-pegasus-project>.

important weapon in the arsenal of Bahrain, which since the Arab Spring, has sought to quell any unrest and activism that threatens the regime.[57]

The use of spyware also has negative impacts on press freedom. Journalists, whose work is essential to keeping governments accountable, have proven to be vulnerable to spyware. In 2021, the Pegasus Project revealed that at least 180 journalists have been targets of Pegasus spyware.[58] In Mexico, there are numerous examples of egregious attempts to silence journalists that involve the use of spyware. In 2017, the Citizen Lab confirmed that between January 2015 and August 2016, Pegasus spyware targeted eleven people, including journalists. Most of these targets were "involved in investigating or working on reports of high-level official corruption, or government involvement in human rights abuses."[59] In 2017, after Mexican journalist Javier Valdez was killed, two of his colleagues were targeted with Pegasus spyware. The next week, Valdez's wife, Griselda Triana, was targeted multiple times with the same spyware.[60] These examples are part of a broader pattern of spyware abuse against journalists in Mexico,[61] and an even broader pattern globally. Hungarian journalist Syabolcs Panyi claims that spyware leads to journalists being "treated as criminals" rather than as

[57] Stephanie Kirchgaessner (2022), "'Most Harmful Thing' – How Spyware is Stifling Human Rights in Bahrain," *The Guardian* (18 February 2022) <https://www.theguardian.com/news/2022/feb/18/how-spyware-erodes-human-rights-in-bahrain-nso-group-pegasus-project>.
[58] Phineas Rueckert (2021), "Pegasus: The New Global Weapon For Silencing Journalists," *Forbidden Stories* <https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/>.
[59] John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert (2017), "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," *The Citizen Lab* <https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/>.
[60] John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert (2019), "Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware," *The Citizen Lab* <https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/>.
[61] The Citizen Lab has reported on other instances of abuse against Mexican journalists as well: see e.g. John Scott-Railton, Bill Marczak, Claudio Guarnieri, and Masashi Crete-Nishihata (2017), "Bitter Sweet: Supporter of Mexico's Soda Tax Targeted With NSO Exploit Links," *The Citizen Lab* <https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/>.

essential components of a properly functioning state.[62] This dynamic contributes to the erosion of press freedom and by extension to the weakening of democracy.

The arbitrary use of surveillance technology also violates the right to privacy, which is protected under Article 17(1) of the ICCPR.[63] Civil society organizations have explained that mercenary spyware "impacts the right to privacy by design: it is surreptitious, deployed without the knowledge of the rights holder, and has the capacity to collect and deliver an unlimited selection of personal, private data."[64] These types of privacy violations are harmful to the dignity of the targets.[65] Spyware also renders it practically impossible for human rights defenders to undertake the sensitive work they do in safety and privacy. The violation of the right to privacy is therefore intimately linked to the right of free expression and association because of the chilling effects which arise from surveillance.[66]

Victims of this type of surveillance can experience significant psychological harms.[67] Mohammed al-Tajer, a lawyer from Bahrain who experienced government surveillance, explained that "the worst and most harmful thing is you feel you are not secure. That instead of your phone being your friend, it is now your enemy. You don't know what

---

[62] OHCHR (2022), "Digital Surveillance Treats 'Journalists as Criminal'," *OHCHR* (3 May 2022) <https://www.ohchr.org/en/stories/2022/05/digital-surveillance-treats-journalists-criminals>.
[63] *International Covenant on Civil and Political Rights*, 19 December 1966, 999 UNTS 171, arts 17(1) (entered into force 23 March 1976).
[64] Amnesty International et al. (2021), "Joint Open Letter by Civil Society Organizations and Independent Experts Calling on States to Implement an Immediate Moratorium on the Sale and Transfer and Use of Surveillance Technology," *Amnesty International* <https://www.amnesty.org/en/documents/doc10/4516/2021/en/>.
[65] EEF (2014), "Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance," *EFF* at 2 <https://necessaryandproportionate.org/principles/>.
[66] EEF (2014), "Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance," *EFF* at 2 <https://necessaryandproportionate.org/principles/>.
[67] Noura Al-Jizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert (2022), "Psychological and Emotional War: Digital Transnational Repression in Canada," *The Citizen Lab* <https://citizenlab.ca/2022/03/psychological-emotional-war-digital-transnational-repression-canada/>.

information is private, and what is already exposed to the state, this is painful."[68] The psychological impacts on women are particularly severe. Access Now explains that personal information obtained through surveillance is used against women human rights defenders in ways that are exacerbated by "political, societal, and gender power asymmetries."[69]

Mercenary spyware also threatens the physical safety of human rights defenders, which is a violation of the guarantee of life under Article 6(1) of the ICCPR, and to the right to liberty and security of the person under Article 9(1) of the ICCPR.[70] Spyware can allow states to access a target's physical location and their private communications. This technology therefore poses a direct risk to the individual target, and an indirect risk to the target's contacts, such as other activists, family, and friends, through access to contact lists and other information on a device. Forensic Architecture has "linked Pegasus to three hundred acts of physical violence."[71] Several UN experts have raised the alarm about the "life threatening" use of spyware.[72] UN Special Rapporteur David Kaye has also noted that surveillance of human rights defenders and targets by states "has been shown to lead to arbitrary detention, sometimes to torture and possibly to extrajudicial killings."[73] This has been echoed by Michelle Bachelet, UN High

[68] Stephanie Kirchgaessner (2022), "'Most Harmful Thing' – How Spyware is Stifling Human Rights in Bahrain," *The Guardian* (18 February 2022) <https://www.theguardian.com/news/2022/feb/18/how-spyware-erodes-human-rights-in-bahrain-nso-group-pegasus-project>.
[69] Marwa Fatafta (2022), "Unsafe Anywhere: Women Human Rights Defenders Speak Out about Pegasus Attacks," *Access Now* <https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/>.
[70] *International Covenant on Civil and Political Rights*, 19 December 1966, 999 UNTS 171, arts 6(1), 9(1) (entered into force 23 March 1976).
[71] Ronan Farrow (2022), "How Democracies Spy on Their Citizens," *The New Yorker* (18 April 2022), <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>.
[72] OHCHR (2021), "Spyware Scandal: UN Experts Call for Moratorium on Sale of 'Life Threatening' Surveillance Tech," *OHCHR* (12 April 2021) <https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening?LangID=E&NewsID=27379>.
[73] UN Human Rights Council (2019), "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," 41st Sess, UN Doc A/HRC/41/35 at para 1 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement>.

Commissioner for Human Rights, and Agnès Callamard, the UN Special Rapporteur who investigated Khashoggi's murder.[74]

Through access to the contents of a target's device, state actors can collect evidence to be used against the target in criminal proceedings. Evidence obtained through spyware can also be used against a target in torture and interrogations. This happened to Loujain Alhathloul, who had her phone infected with spyware. Contents from her private communications were mentioned in both her charging documents and during her torture and interrogation by Saudi authorities.[75] Similarly, Moroccan journalist Hajar Raissouni and her husband, Rifaat Al-Amin, both had their phones targeted with Pegasus spyware. In 2019, they were arrested and repeatedly interrogated about things which could only have been learned through surveillance on their private devices.[76] Moreover, because state actors may have the ability to remotely control a target's device, they could plant incriminating evidence on the device and subsequently use that evidence against them.[77]

---

[74] Michelle Bachelet stated that the "[u]se of surveillance software has been linked to arrest, intimidation and even killings of journalists and human rights defenders" (OHCHR, "Use of Spyware to Surveil Journalists and Human Rights Defenders: Statement by High Commissioner for Human Rights Michelle Bachelet," *OHCHR* (19 July 2021) <https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high-commissioner?LangID=E&NewsID=27326)>); Agnes Callamard stated that "[t]he States of the countries where journalists, human rights defenders or dissidents have found residence or exile are under an obligation to respect their human rights, and to protect them against violence by the States of the countries from which they have escaped. Obligations to protect the rights of that community, including their right to life, should figure highly among the priorities of a State" (UN Human Rights Council (2019), "Investigation of, accountability for and prevention of intentional State killings of human rights defenders, journalists and prominent dissidents: Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions," 41st Sess, UN Doc A/HRC/41/36 at para 70 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/296/91/PDF/G1929691.pdf?OpenElement>).
[75] EFF (2021), "AlHathloul v. DarkMatter Group – Complaint," *EFF* at 30 <https://www.eff.org/document/alhathloul-v-darkmatter-group-complaint>.
[76] Hajar Raissouni (2021), "The Day Morocco Bugged Us; Hajar Raissouni's Story," *Daraj* (6 August 2021) <https://daraj.com/en/77594/>.
[77] Bill Marczak, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert (2021), "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus," *The Citizen Lab* <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/>.

Spyware also has important transnational implications, as surveillance technology makes it easier for states to extend their reach across borders. State repression of activists abroad using the digital sphere has been dubbed "digital transnational repression."[78] States have increasingly turned to digital technologies, including spyware, to "harass, intimidate, silence, persecute, or otherwise pursue activists and dissidents living outside the country."[79] This type of repression is increasingly common, as the use of spyware to infect devices has made it more difficult for dissidents to fully escape their states' influence; human rights defenders can no longer evade state surveillance by settling abroad. Indeed, the Citizen Lab has found that it is "a relatively common practice" for states to use spyware against targets beyond their borders.[80] Surveillance technology also facilitates transnational surveillance of perceived threats to their regime given spyware's relatively low cost and effectiveness.[81] Mercenary spyware thus facilitates digital transnational repression and increases governments' ability to threaten targets psychologically and physically.

It is highly unlikely that targeted surveillance of human rights defenders with spyware could meet requirements under international human rights law for restrictions on the rights to privacy and freedom of expression, among others. Such restrictions must be provided by law and be legitimate, necessary, and proportionate. The UN Human Rights Committee has concluded that "restrictions [on the right to freedom of expression] may never be invoked as a justification for the muzzling of any advocacy of multiparty

[78] Noura Al-Jiwazi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert (2022), "Psychological and Emotional War: Digital Transnational Repression in Canada," *The Citizen Lab* at 1 <https://citizenlab.ca/wp-content/uploads/2022/03/Report151-dtr_022822.pdf>.
[79] Siena Anstis and Sophie Barnett (2022), "Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses," *Journal of Human Rights Practice* at 4.
[80] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert (2018), "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab* at 25 <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> (they note that "[t]en Pegasus operators appear to be conducting surveillance in multiple countries. While we have observed prior cases of cross-border targeting, this investigation suggests that cross-border targeting and/or monitoring is a relatively common practice.")
[81] Siena Anstis and Sophie Barnett (2022), "Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses," *Journal of Human Rights Practice* at 7–8.

democracy, democratic tenets and human rights."[82] The EDPS has concluded that the use of technology like NSO Group's Pegasus spyware by European states was "highly unlikely" to meet the requirements of proportionality that are part of the *EU Charter of Fundamental Rights*. It observed that: "The level of interference with the right to privacy is so severe that the individual is in fact deprived of it." Because the use of this technology affects the "essence" of the right to privacy, the EDPS concluded that its use "cannot be considered proportionate – irrespective of whether the measure can be deemed necessary to achieve the legitimate objectives of a democratic state."[83]

V. Relationship between mercenary spyware and enforced disappearances

Mercenary spyware has been linked to instances of enforced disappearances. The inherent secrecy surrounding both the use of mercenary spyware and enforced disappearances makes the study of their relationship challenging. More information about the use of spyware is coming to light, however. The following case studies highlight that mercenary spyware facilitates enforced disappearances: spyware allows states to surveil and locate targets, find incriminating evidence, and spy on the associates of the forcibly disappeared person, making it more difficult to conduct investigations and to prepare for legal proceedings in relation to the enforced disappearance.

Spyware has been linked to the enforced disappearance of Loujain Alhathloul, a human rights defender and prominent women's rights activist from Saudi Arabia. In 2018, DarkMatter spyware was used to infiltrate Alhathloul's phone, "surveil her movements, and exfiltrate her confidential communications for use against her."[84] On May 13, 2018,

[82] 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>.
[83] European Data Protection Supervisor (2022), "Preliminary Remarks on Modern Spyware," *EDPS* <https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf>.
[84] EFF (2021), "AlHathloul v. DarkMatter Group – Complaint," *EFF* at 2 <https://www.eff.org/document/alhathloul-v-darkmatter-group-complaint>.

Alhathloul was arbitrarily detained in the United Arab Emirates and forcibly rendered to Saudi Arabia, where she was placed under a travel ban.[85] On May 15, she was arrested by Saudi officers and imprisoned, where she was interrogated, tortured, and threatened with rape and murder.[86] While Alhathloul was being interrogated and tortured, "her interrogators mentioned details regarding Ms. Alhathloul's communications that were available through unlawful access to [her] device."[87] Her private communications were also featured in her charging documents.[88] Alhathloul is no longer in prison, but is still under a travel ban in Saudi Arabia. Under her suspended sentence, she can be returned to prison if she continues to engage in activism.[89] In 2021, Alhathloul filed a civil action against the Emirati cyber-surveillance company DarkMatter Group and American citizens who held senior positions at the company for their role in her arrest and imprisonment.[90]

Another example is the high-profile case of Khashoggi, a journalist and critic of the Saudi government who was assassinated by Saudi authorities in Turkey on October 2, 2018. People close to Khashoggi had been targets of Pegasus spyware before and after his murder. Khashoggi's wife, Hanan Elatr, had her phone infected with Pegasus spyware before the murder, between November 2017 and April 2018. She believes that surveillance through her phone may have made it easier for Saudi officials to track Khashoggi.[91] Khashoggi's fiancée, Hatice Cengiz, was targeted with Pegasus spyware

[85] EFF (2021), "AlHathloul v. DarkMatter Group – Complaint," *EFF* at 9 <https://www.eff.org/document/alhathloul-v-darkmatter-group-complaint>.
[86] EFF (2021), "AlHathloul v. DarkMatter Group – Complaint," *EFF* at 27 <https://www.eff.org/document/alhathloul-v-darkmatter-group-complaint>.
[87] EFF (2021), "AlHathloul v. DarkMatter Group – Complaint," *EFF* at 30 <https://www.eff.org/document/alhathloul-v-darkmatter-group-complaint>.
[88] EFF (2021), "AlHathloul v. DarkMatter Group – Complaint," *EFF* at 30 <https://www.eff.org/document/alhathloul-v-darkmatter-group-complaint>.
[89] Arwa Youssef (2021), "Saudi Women's Rights Defenders Released, But Not Free," *Human Rights Watch* <https://www.hrw.org/news/2021/02/12/saudi-womens-rights-defenders-released-not-free>.
[90] "EFF (2021), "Saudi Human Rights Activist, Represented by EFF, Sues Spyware Maker DarkMatter for Violating U.S. Anti-Hacking and International Human Rights Law," *EFF* <https://www.eff.org/press/releases/saudi-human-rights-activist-represented-eff-sues-spyware-maker-dark matter-violating>.
[91] Philip Bennett (2021), "Pegasus Spyware Placed on Phone of Jamal Khashoggi's Wife Before his Murder, Washington Post Reports," *PBS Frontline* (21 December 2021)

four days after his murder.[92] Omar Abdulaziz, who was a close associate of Khashoggi, also had his phone infected with Pegasus spyware prior to Khashoggi's assassination in 2018.[93] The surveillance may have informed Saudi officials of "sensitive plans he had been developing with Khashoggi" in their activism against the Saudi government.[94] Khashoggi's murder is part of a broader campaign by Saudi officials to use digital transnational repression in their pursuit of repressing dissent abroad.[95] The use of spyware facilitates that campaign and makes life more dangerous for dissidents.

Spyware is also linked to the case of Paul Rusesabagina, who has long been an outspoken critic of Kagame's government in Rwanda.[96] In August 2020, Rusesabagina was forcibly disappeared on a layover in Dubai on his way to Burundi.[97] A few days later, he was imprisoned in Rwanda for purportedly "financing terrorist activities."[98] His

---

<https://www.pbs.org/wgbh/frontline/article/pegasus-spyware-jamal-khashoggi-wife-phone-washington-post/>.

[92] Dana Priest, Souad Mekhennet, and Arthur Bouvart (2018), "Jamal Khashoggi's Wife Targeted with Spyware Before his Death," *The Washington Post* (18 July 2018) <https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/>.

[93] Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ron Deibert (2018), "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil," *The Citizen Lab* <https://tspace.library.utoronto.ca/bitstream/1807/95329/1/Report%23115--Kingdom%20Came.pdf>.

[94] Ayman M. Mohyeldin (2019), "No One is Safe: How Saudi Arabia Makes Dissidents Disappear," *Vanity Fair* (September 2019) <https://www.vanityfair.com/news/2019/07/how-saudi-arabia-makes-dissidents-disappear>.

[95] Ayman M. Mohyeldin (2019), "No One is Safe: How Saudi Arabia Makes Dissidents Disappear," *Vanity Fair* (September 2019) <https://www.vanityfair.com/news/2019/07/how-saudi-arabia-makes-dissidents-disappear>.

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

[97] OCCRP (2021), "Israeli Spy Tech Used Against Daughter of Man Who Inspired 'Hotel Rwanda,'" *OCCRP* (19 July 2021) <https://www.occrp.org/en/the-pegasus-project/israeli-spy-tech-used-against-daughter-of-man-who-inspired-hotel-rwanda>.

[98] OCCRP (2021), "Israeli Spy Tech Used Against Daughter of Man Who Inspired 'Hotel Rwanda,'" *OCCRP* (19 July 2021) <https://www.occrp.org/en/the-pegasus-project/israeli-spy-tech-used-against-daughter-of-man-who-inspired-hotel-rwanda>.

daughter Carine Kanimba, who is a dual Belgian and American citizen who resides in Belgium, claimed that the charges against her father were fraudulent and politically motivated, and had been advocating for his release.[99] Amnesty International discovered that Kanimba's phone had likely been infected with Pegasus spyware since January 2021.[100] The Rwandan government had been listening to her phone calls with lawyers, members of the Belgian, British, and European Parliaments, and US officials.[101] Rwandan officials also revealed that they knew about legal plans discussed privately between Rusesabagina's family and their lawyers.[102] Surveillance therefore made it difficult for lawyers to work confidentially. In addition to undermining efforts to free Rusesabagina, Kanimba also argues that the spyware is being used as "an intimidation tool."[103] Indeed, states often use surveillance and other intimidation tactics against

[99] Stephanie Kirchgaessner (2021), "Hotel Rwanda Activist's Daughter Placed Under Pegasus Surveillance," *The Guardian* (19 July 2021) <https://www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance>; Al Jazeera, "World Reaction to 'Hotel Rwanda' Hero's Prison Sentence," *Al Jazeera* (20 September 2021) <https://www.aljazeera.com/news/2021/9/20/world-reaction-hotel-rwanda-star-jailed>.
[100] Stephanie Kirchgaessner (2021), "Hotel Rwanda Activist's Daughter Placed Under Pegasus Surveillance," *The Guardian* (19 July 2021) <www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance>.
[101] Stephanie Kirchgaessner (2021), "Hotel Rwanda Activist's Daughter Placed Under Pegasus Surveillance," *The Guardian* (19 July 2021) <www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance>; OCCRP (2021), "Israeli Spy Tech Used Against Daughter of Man Who Inspired 'Hotel Rwanda'," *OCCRP* (19 July 2021) <https://www.occrp.org/en/the-pegasus-project/israeli-spy-tech-used-against-daughter-of-man-who-inspired-hotel-rwanda>.
[102] OCCRP (2021), "Israeli Spy Tech Used Against Daughter of Man Who Inspired 'Hotel Rwanda'," *OCCRP* (19 July 2021) <https://www.occrp.org/en/the-pegasus-project/israeli-spy-tech-used-against-daughter-of-man-who-inspired-hotel-rwanda>.
[103] OCCRP (2021), "Israeli Spy Tech Used Against Daughter of Man Who Inspired 'Hotel Rwanda'," *OCCRP* (19 July 2021) <https://www.occrp.org/en/the-pegasus-project/israeli-spy-tech-used-against-daughter-of-man-who-inspired-hotel-rwanda>.

family members "because of their ease for the origin state and degree to which they can affect the target."[104]

In 2017, the International Federation for Human Rights and the French Human Rights League filed a complaint with French authorities against a French spyware firm formerly known as "Amesys" and now known as "Nexa Technologies."[105] They claimed that "the company's sale of surveillance software to authoritarian regimes in Libya and Egypt that resulted in torture and disappearance of dissidents" made the company's executives complicit.[106] In June 2021, four senior executives were indicted by investigating judges of the Paris Judicial Court.[107] The surveillance technology was supplied to Egypt's regime under Abdel Fattah al-Sisi in 2014.[108] The spyware they supplied made it possible to surveil and track, and in some cases, to forcibly disappear activists.[109] This

[104] Nate Schenkkan and Isabel Linzer (2021), "Out of Sight, Not Out of Reach," *Freedom House* <(https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf>.
[105] FIDH, "The Surveillance Industry and Human Rights: FIDH Submission," *OHCHR* at Part 1(iii) <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/FIDH.pdf>.
[106] Patrick Howell O'Neill (2021), "French Spyware Bosses Indicted for their Role in the Torture of Dissidents," *MIT Technology Review* (22 June 2021) <https://www.technologyreview.com/2021/06/22/1026777/france-spyware-amesys-nexa-crimes-against-humanity-libya-egypt/>; Radhamely De Leon (2021), "4 Surveillance Company Executives Indicted for Allegedly Aiding Torture," *Motherboard* (23 June 2021) <https://www.vice.com/en/article/m7e3zv/4-surveillance-company-executives-indicted-for-allegedly-aiding-torture>.
[107] Patrick Howell O'Neill (2021), "French Spyware Bosses Indicted for their Role in the Torture of Dissidents," *MIT Technology Review* (22 June 2021) https://www.technologyreview.com/2021/06/22/1026777/france-spyware-amesys-nexa-crimes-against-humanity-libya-egypt/; Radhamely De Leon (2021), "4 Surveillance Company Executives Indicted for Allegedly Aiding Torture," *Motherboard* (23 June 2021) <https://www.vice.com/en/article/m7e3zv/4-surveillance-company-executives-indicted-for-allegedly-aiding-torture>.
[108] Sidney Fussell (2021), "French Spyware Executives Are Indicted for Aiding Torture," *Wired* (23 June 2021) <https://www.wired.com/story/french-spyware-executives-indicted-aiding-torture/>.
[109] FIDH (2021), "Surveillance and Torture in Egypt and Libya: Amesys and Nexa Technologies Executives Indicted," *FIDH* (22 June 2021) <https://www.fidh.org/en/region/north-africa-middle-east/egypt/surveillance-and-torture-in-egypt-and-libya-amesys-and-nexa>; FIDH (2021), "Q/A Surveillance and Torture in Egypt and Libya: Amesys and Nexa Technologies Executives Indicted," *FIDH* (22 June 2021) <https://www.fidh.org/en/region/north-africa-middle-east/egypt/q-a-surveillance-and-torture-in-egypt-and-li

complicity is further compounded by the fact that the executives knew that their spyware would be used to surveil dissidents.[110] This represents an important first instance in which mercenary spyware sellers may be held accountable for the human rights abuses which are perpetrated with the use of their products.[111] It is also a recognition of the important link between spyware and enforced disappearances.

VI. Mitigation of risks and dangers

Actions by a confluence of actors are necessary to mitigate the risks and dangers of mercenary spyware technology. States and spyware companies have obligations which they must discharge to protect dissidents and others from the devastating impacts of surveillance technology. Other businesses must also mitigate the risks that their products can pose to individuals if they are exploited by the spyware industry. Further, civil society plays an important role in revealing cases of abuse, advocating for accountability, and in supporting human rights defenders targeted with mercenary spyware. In the following section, we outline best practices for these actors.

a. States

States should implement a moratorium on the sale, transfer, and use of mercenary spyware technology until there is sufficient regulation of the industry. There is consensus on this point among civil society actors. This was recommended by the United Nations (UN) Special Rapporteur on the promotion and protection of the right to

bya-amesys-and-nexa>; Radhamely De Leon (2021), "4 Surveillance Company Executives Indicted for Allegedly Aiding Torture," *Motherboard* (23 June 2021) <https://www.vice.com/en/article/m7e3zv/4-surveillance-company-executives-indicted-for-allegedly-aiding-torture>.

[110] Sarah Elzas (2021), "French Executives Face Torture Charges for Selling Spy Gear to Libya, Egypt," *RFI* (22 June 2021) <https://www.rfi.fr/en/france/20210622-french-executives-face-torture-charges-for-selling-spy-gear-to-libya-egypt-amesys-nexa-human-rights>.

[111] Amnesty International (2021), "Executives of Surveillance Companies Amesys and Nexa Technologie Indicted for Complicity in Torture," *Amnesty International* <https://www.amnesty.org/en/latest/news/2021/06/executives-of-surveillance-companies-amesys-and-nexa-technologies-indicted-for-complicity-in-torture/>.

freedom of opinion and expression in 2019.[112] Other human rights experts at the UN pressed the importance of a moratorium in 2021, noting that it is "highly dangerous and irresponsible to allow the surveillance technology and trade sector to operate as a human rights-free zone."[113] This same point has been argued by civil society organizations, including Amnesty International and Access Now.[114] Costa Rica became the first country to support this type of moratorium in April 2022.[115] These actors decry how the use of spyware has increased the ability of governments to violate human rights of dissidents and other actors in civil society without much scrutiny. Without regulation, the spyware industry has proliferated with devastating impacts. A moratorium is essential to prevent further proliferation of human rights abuses before effective and impactful regulations are implemented.

In July 2021, civil society organizations and independent experts signed an open letter calling for a comprehensive legal framework to be implemented if a moratorium is lifted.[116] Robust regulations are needed to regulate the import, export, and use of surveillance technology. UN Special Rapporteur David Kaye and Marietje Shaake have warned that "[w]e are on the precipice of a global surveillance tech catastrophe, an avalanche of tools shared across borders with governments failing to constrain their

---

[112] UN Human Rights Council (2019), "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," 41st Sess, UN Doc A/HRC/41/35 at para 66(a) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement>.
[113] OHCHR (2021), "Spyware Scandal: UN Experts Call for Moratorium on Sale of 'Life Threatening' Surveillance Tech," *OHCHR* (12 April 2021) <https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening?LangID=E&NewsID=27379>.
[114] Amnesty International et al. (2021), "Joint Open Letter by Civil Society Organizations and Independent Experts Calling on States to Implement an Immediate Moratorium on the Sale and Transfer and Use of Surveillance Technology," *Amnesty International* <https://www.amnesty.org/en/documents/doc10/4516/2021/en/>.
[115] 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/costa-rica-first-country-moratorium-spyware/>.
[116] Amnesty International et al. (2021), "Joint Open Letter by Civil Society Organizations and Independent Experts Calling on States to Implement an Immediate Moratorium on the Sale and Transfer and Use of Surveillance Technology," *Amnesty International* <https://www.amnesty.org/en/documents/doc10/4516/2021/en/>.

export or use."[117] Currently, there are very few standards and regulations in place, so that mercenary spyware is being bought and sold with little oversight or regard for the human rights practices of its customers. Attempts to legislate and regulate so far have been criticized as being a positive step forward, but not ambitious enough to address the breadth of the problem.[118] Comprehensive regulations must thus be enacted to outline the contours of acceptable use of mercenary spyware in a way that respects the rights to privacy, freedom of expression and assembly, and physical security.[119]

Robust global export controls should govern cross-border transfers of surveillance technology. This legislation should define surveillance technology broadly so that it captures the various types of spyware on the market.[120] It must also be flexible enough to capture new surveillance technologies as they emerge.[121] Export licences for these

---

[117] David Kaye and Marietje Schaake (2021), "Global Spyware Such as Pegasus is a Threat to Democracy. Here's How to Stop It," *The Washington Post* (19 July 2021) <https://www.washingtonpost.com/opinions/2021/07/19/pegasus-spyware-nso-group-threat-democracy-journalism/>.

[118] For instance, the European Union's 2021 Dual Use Regulation was criticized for "deficiencies in the regulatory structure" (Siena Anstis and Sophie Barnett (2022), "Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses," *Journal of Human Rights Practice* at 16). Similarly, the *Wassenar Agreement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* "only includes 42 participant states and is strongly Western-focused" (Siena Anstis and Sophie Barnett (2022), "Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses," *Journal of Human Rights Practice* at 16) and has been criticized for "lack[ing] guidelines or enforcement measures that would directly address human rights violations caused by surveillance tools" (UN Human Rights Council (2019), "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," 41st Sess, UN Doc A/HRC/41/35 at para 34 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement>).

[119] Justin Hendrix (2021), "Marietje Schaake on the Threat the Global Spyware Industry Poses to Democracy," *Tech Policy Press* (27 July 2021) <https://techpolicy.press/marietje-schaake-on-the-threat-the-global-spyware-industry-poses-to-democracy/>.

[120] Human Rights Watch et al. (2021), "Human Rights Organisations' Response to the Adoption of the New EU Dual Use Export Control Rules," *Human Rights Watch* at 6–7 <https://www.hrw.org/sites/default/files/media_2021/03/Reforms%20to%20EU%20Surveillance%20Tech%20Export%20Rules_Joint%20NGO%20Statement_20210324_0.pdf>.

[121] Siena Anstis and Sophie Barnett (2022), "Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses," *Journal of Human Rights Practice* at 16.

technologies should be contingent on the recipient's compliance with human rights obligations.[122] Human rights due diligence requirements should also be a feature of this legislation, and there should be "little or no discretion for state authorities to authorize exports to regimes likely to use surveillance technology to violate human rights domestically or transnationally."[123] Export licences for surveillance technology should be made publicly available to ensure public oversight.[124]

These regulations must contribute to limiting authoritarian states' access to spyware so that their ability to conduct domestic and transnational repression is curtailed. States have so far been reluctant to address the growing use of spyware by authoritarian regimes in ways that violate fundamental human rights. However, regulating the spyware industry in a way that protects human rights necessarily involves limiting the ability of authoritarian governments to abuse mercenary spyware.

Transparency should be a central feature of the export control regulations of surveillance technologies. This is crucial to be able to track the proliferation of these technologies as well as to ensure state accountability.[125] These regulations should include disclosure requirements "identifying companies that are producing surveillance technology, to whom they are selling, and what products are being sold."[126] State

---

[122] UN Human Rights Council (2019), "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," 41st Sess, UN Doc A/HRC/41/35 at para 58 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement>.
[123] Siena Anstis and Sophie Barnett (2022), "Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses," *Journal of Human Rights Practice* at 16.
[124] Siena Anstis and Sophie Barnett (2022), "Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses," *Journal of Human Rights Practice* at 16; Human Rights Watch et al. (2021), "Human Rights Organisations' Response to the Adoption of the New EU Dual Use Export Control Rules," *Human Rights Watch* at 7 <https://www.hrw.org/sites/default/files/media_2021/03/Reforms%20to%20EU%20Surveillance%20Tech%20Export%20Rules_Joint%20NGO%20Statement_20210324_0.pdf>.
[125] Siena Anstis and Sophie Barnett (2022), "Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses," *Journal of Human Rights Practice* at 16.
[126] David Kaye and Marietje Schaake (2021), "Global Spyware Such as Pegasus is a Threat to Democracy. Here's How to Stop It," *The Washington Post* (19 July 2021) <https://www.washingtonpost.com/opinions/2021/07/19/pegasus-spyware-nso-group-threat-democracy-journalism/>.

procurement of spyware should be made public, and should involve input from stakeholders, including civil society actors. Moreover, states should only procure spyware from companies that do not sell to regimes that abuse their products.[127] Governments should also encourage public oversight by being responsive to freedom of information requests related to the use of spyware.[128]

The legal regime should establish independent oversight over the deployment of spyware to ensure accountability.[129] Because so many states are implicated in the spyware industry as buyers and users, it is essential that an independent oversight mechanism plays a role in ensuring that states and spyware companies comply with legislation and human rights obligations. The Citizen Lab has argued that there is a "principle of misuse" which posits that "when the technology is sold to a government without sufficient oversight, it will eventually be misused."[130] An oversight mechanism should therefore investigate instances of misuse, with the power to compel the production of evidence so that they can carry out their investigations effectively. This body should have the authority to impose punishment on wrongdoers, and regulate which actors can have access to surveillance technologies based on their compliance with human rights obligations.[131] Moreover, when the oversight mechanism finds cases

---

[127] Amnesty International et al. (2021), "Joint Open Letter by Civil Society Organizations and Independent Experts Calling on States to Implement an Immediate Moratorium on the Sale and Transfer and Use of Surveillance Technology," *Amnesty International* <https://www.amnesty.org/en/documents/doc10/4516/2021/en/>.

[128] Justin Hendrix (2021), "Marietje Schaake on the Treat the Global Spyware Industry Poses to Democracy," *Tech Policy Press* (27 July 2021) <https://techpolicy.press/marietje-schaake-on-the-threat-the-global-spyware-industry-poses-to-democracy/>.

[129] Molly K. Land and Jay D. Aronson (2020), "Human Rights and Technology: New Challenges for Justice and Accountability," *Annual Review of Law and Social Science* 16 at 235 <https://www.annualreviews.org/doi/pdf/10.1146/annurev-lawsocsci-060220-081955>.

[130] John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-NIshihata, and Ron Deibert (2017), "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," *The Citizen Lab* <https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/>.

[131] UN Human Rights Council (2019), "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," 41st Sess, UN Doc A/HRC/41/35 at para 52 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement>; Amnesty International et al. (2021), "Joint Open Letter by Civil Society Organizations and Independent

of misuse, the legislation should provide an accessible avenue for the victims to obtain remedies.[132]

b. Spyware Companies

Under the *United Nations Guiding Principles on Business and Human Rights*, companies—including cyber-surveillance companies—must respect internationally recognized human rights.[133] This responsibility requires companies to undertake due diligence to ensure that their products and services are not used by their clients in a way that infringes human rights.[134] Surveillance companies such as NSO Group have stated that they are respecting human rights in "all aspects of [their] work";[135] however, they have continued to perpetrate abuse despite the implementation of human rights policies. The evidence is clear that NSO Group, for example, has repeatedly sold spyware to repressive regimes despite widespread reporting on the misuse of their spyware.

This disregard for human rights demonstrates that self-regulation by spyware companies will be ineffective without robust legal safeguards that are implemented at the state and international level. Therefore, there needs to be both domestic and international regulations, as well as transparency and disclosure requirements which are enshrined in law, in addition to independent oversight of the offensive security

---

Experts Calling on States to Implement an Immediate Moratorium on the Sale and Transfer and Use of Surveillance Technology," *Amnesty International* <https://www.amnesty.org/en/documents/doc10/4516/2021/en/>.

[132] Siena Anstis and Sophie Barnett (2022), "Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses," *Journal of Human Rights Practice* at 19.

[133] UN Human Rights Council (2011), "Guiding Principles on Business and Human Rights," UN Doc HR/PUB/11/04, art 12 <https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf>.

[134] UN Human Rights Council (2011), "Guiding Principles on Business and Human Rights," UN Doc HR/PUB/11/04, art 13 <https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf>.

[135] NSO Group, "Human Rights Policy" <https://www.nsogroup.com/governance/human-rights-policy/>.

sector. Without legislation and associated enforcement mechanisms, it is unlikely that these companies will fulfill their human rights obligations or will be held accountable for human rights violations.

c. Other Businesses

Businesses beyond the spyware industry also have a role to play in mitigating the risks associated with spyware. Some businesses may have a heightened responsibility to mitigate these risks because their product may provide a platform which facilitates surveillance. For example, Apple's iPhones provide a conduit for surveillance companies to reach targets when they are infected with spyware.[136] Similarly, devices may be infected with spyware through malicious links sent on Meta's WhatsApp platform.[137]

To mitigate risks, businesses must take appropriate measures to protect their products' users from spyware attacks.[138] Businesses should act quickly and transparently to address vulnerabilities in their systems that can increase risk to their users and should notify the targets of state or state-related spyware attacks and direct them to appropriate resources. For example, in 2019, WhatsApp discovered that NSO Group had been exploiting a vulnerability on their platform to target users. WhatsApp quickly patched the vulnerability, and worked with the Citizen Lab to identify "over 100 cases of abusive targeting of human rights defenders and journalists in at least 20 countries

[136] See e.g. Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jiwazi, Siena Anstis, Kristin Berdan, and Ron Deibert (2021), "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware," *The Citizen Lab* <https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/>.
[137] The Citizen Lab (2019), "NSO Group/Q Cyber Technologies: Over One Hundred New Abuse Cases," *The Citizen Lab* <https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/>.
[138] Privacy International (2021), "Taming Pegasus: A Way Forward on Surveillance Tech Proliferation," *Privacy International* (27 July 2021) <https://privacyinternational.org/news-analysis/4602/taming-pegasus-way-forward-surveillance-tech-proliferation>.

across the globe" and notify targets.[139] Similarly, when the Citizen Lab alerted Apple in 2021 that NSO Group's spyware was exploiting security vulnerabilities in their software to conduct surveillance, Apple quickly patched these vulnerabilities and notified the victims.[140] Apple also pledged to donate $10 million dollars, as well as "free technical, threat intelligence and engineering assistance" to organizations engaged in pushing back against digital surveillance.[141] There are also legal avenues that businesses can take to increase accountability for the spyware industry. Businesses should bring forward lawsuits against spyware companies that misuse their products to target individuals.[142] Apple and Meta have both brought forward lawsuits against NSO Group, which may contribute to deterring spyware companies from exploiting their systems in the future.[143] Penney and Schneier argue that such lawsuits "may lay the foundation of new possibilities for corporate accountability, beyond mere public shaming via media coverage."[144]

d. Civil Society

---

[139] The Citizen Lab (2019), "NSO Group/Q Cyber Technologies: Over One Hundred New Abuse Cases," *The Citizen Lab* <https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/>.
[140] Nicole Perlroth (2021), "Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones," *The New York Times* (6 December 2021) <https://www.nytimes.com/2021/11/23/technology/apple-nso-group-lawsuit.html>; Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jiwazi, Siena Anstis, Kristin Berdan, and Ron Deibert (2021), "FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild," *The Citizen Lab* <https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/>.
[141] Nicole Perlroth (2021), "Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones," *The New York Times* (6 December 2021) <https://www.nytimes.com/2021/11/23/technology/apple-nso-group-lawsuit.html>.
[142] Jonathon W. Penney and Bruce Schneier (2021), "Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group," 36 *Berkeley Technology Law Journal* at 138.
[143] Jonathon W. Penney and Bruce Schneier (2021), "Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group," 36 *Berkeley Technology Law Journal* at 138; Apple (2021), "Apple Sues NSO Group to Curb the Abuse of State-Sponsored Spyware," *Apple Newsroom* (23 November 2021) <https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/>.
[144] Jonathon W. Penney and Bruce Schneier (2021), "Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group," 36 *Berkeley Technology Law Journal* at 138.

Civil society, including research groups, non-governmental organizations, and journalists, are critical to ensuring accountability for the use of spyware. Research groups such as the Citizen Lab and Amnesty International, and news organizations involved in the Pegasus Project have been central in bringing state abuses of spyware technology to light. Indeed, UN Special Rapporteur David Kaye noted that "our knowledge of the problem exists mainly because of the digital-forensic work of non-governmental researchers and tenacious reporting by civil society organizations and the media."[145]

Civil society organizations should continue to push for a moratorium on the sale, transfer, and use of mercenary spyware as well as for the subsequent enactment of norms and rules on the deployment of spyware that meet the standards set by international human rights law. These organizations should continue to be central actors in raising issues in domestic and international settings. Civil society also has a crucial role to play in raising awareness on digital security issues by engaging with activists and others working on issues relating to enforced disappearances, including activists' family and friends. Moreover, civil society organizations must be granted sufficient resources to continue to effectively carry out this work.

VII. Recommendations

We propose the following recommendations to the Working Group on Enforced or Involuntary Disappearances.

Recommendation 1: Highlight the role of spyware in perpetrating human rights abuses in the upcoming thematic study and condemn the abuse of spyware by states.

[145] UN Human Rights Council (2019), "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," 41st Sess, UN Doc A/HRC/41/35 at para 1 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement>.

Spyware has shown to be an important feature of enforced or involuntary disappearances. This is highly concerning, as the market for surveillance technology has grown quickly over the past decade, which has made dissidents and their relatives more vulnerable to surveillance. It has also increased the insecurity of exiled dissidents abroad, since spyware facilitates digital transnational repression. As spyware is one of the tools that enables enforced disappearances, it is crucial to emphasize the role of this new technology in the upcoming thematic study to alert the international community to the dangers of spyware, and to avoid further normalization of the abuse of spyware. We recommend that the Working Group condemns this abuse by governments and spyware companies. We also recommend that the Working Group encourages a moratorium on the sale, transfer, and use of spyware until the adoption of comprehensive domestic and international legislation and regulation to curb these abuses.

Recommendation 2: In meetings with states and in international fora, explain how the work of human rights defenders—including those working on enforced disappearances—is seriously endangered by spyware and contradicts the obligations of states under the *Declaration on the Protection of all Persons from Enforced Disappearance.*

New surveillance technologies pose a serious risk to human rights defenders and their work. Spyware is used to surveil, track, and collect information on potential victims of enforced disappearances. Spyware has also been used to impede investigations and legal challenges in relation to enforced disappearances. Spyware is thus a tool which can both lead to enforced disappearances and make it more difficult for relatives of a forcibly disappeared person to investigate their disappearance. More broadly, spyware facilitates human rights violations, including violations of freedom of expression and assembly, privacy, and the right to life, liberty and security.

We recommend that the Working Group emphasizes the abuses and dangers raised by the unchecked proliferation of mercenary spyware during country visits and in other discussions with governments. During these discussions, the Working Group should

stress state obligations under the *Declaration on the Protection of all Persons from Enforced Disappearance*. Notably, Article 2(2) of the *Declaration* outlines that states "shall act at the national and regional levels and in cooperation with the UN to contribute by all means to the prevention and eradication of enforced disappearances."[146] States should be informed that one of the crucial means to prevent enforced disappearances is the regulation of the spyware industry, by making spyware less accessible and ensuring consequences for misuse. States are also not permitted to "practice, permit or tolerate enforced disappearances" and must take measures to prevent enforced disappearances in their jurisdictions.[147] States should be pressed to protect individuals—in particular, dissidents and their relatives—in their jurisdictions from unlawful surveillance that may be linked to enforced disappearances.

We recommend that the Working Group emphasizes the capacity for spyware to facilitate human rights violations, including in relation to enforced disappearances, when addressing governments and international bodies and to highlight this issue to the UN Human Rights Council. We recommend that the Working Group facilitate further research into how spyware may be impairing the work of human rights defenders, particularly in relation to enforced disappearances, and connect human rights defenders with appropriate resources to address the threat of spyware, such as Access Now's Digital Security Helpline.

Recommendation 3: Investigate what further support human rights defenders working on enforced disappearances need in addressing the risks raised by spyware.

---

[146] *Declaration on the Protection of all Persons from Enforced Disappearance*, 18 December 1992, Gen Ass Resolution 47/133, art 2(2) <https://www.ohchr.org/en/instruments-mechanisms/instruments/declaration-protection-all-persons-enforced-disappearance>.

[147] *Declaration on the Protection of all Persons from Enforced Disappearance*, 18 December 1992, Gen Ass Resolution 47/133, arts 2(1), 3 <https://www.ohchr.org/en/instruments-mechanisms/instruments/declaration-protection-all-persons-enforced-disappearance>.

We recommend that the Working Group engages in consultation with human rights defenders to find what further support is needed to protect themselves against spyware attacks and related human rights violations. Upstream preventative measures may include providing technical training and support to human rights defenders and other vulnerable targets of spyware attacks.[148] Technological, legal, and investigative support should be given to the relatives of forcibly disappeared persons, as spyware can be used to intimidate them or otherwise impede their efforts to find forcibly disappeared persons. It is also vital to increase access to justice for victims of spyware misuse, including those who have been targeted in relation to an enforced disappearance. Concrete steps that can be taken by the Working Group include pushing for the establishment of legal avenues for complaints both domestically and internationally.[149] These avenues should be both efficient and affordable so as not to create additional barriers to victims of spyware misuse.[150]

Recommendation 4: Join research and advocacy groups in pushing governments to regulate the global spyware industry.

Research and advocacy groups have been at the forefront of the movement to uncover abuses related to the global spyware industry. Not only has their work revealed the nefarious implications of these new surveillance technologies, but they have worked closely with technology companies and victims of spyware. As such, they have important insight into how best to regulate the spyware industry. We recommend that the Working Group collaborates with these groups in the push for regulation of the global spyware industry at the domestic and international levels.

---

[148] Chiara Castro (2021), "Meet the People Helping Activists to Fight Against Digital Surveillance," *Tech Radar* (5 May 2021) <https://www.techradar.com/features/meet-the-people-helping-activists-to-fight-against-digital-surveillance>.
[149] FIDH, "The Surveillance Industry and Human Rights: FIDH Submission," *OHCHR* at Part 1(iii) <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/FIDH.pdf>.
[150] FIDH, "The Surveillance Industry and Human Rights: FIDH Submission," *OHCHR* at Part 1(iii) <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/FIDH.pdf>.

The Working Group has previously denounced both state reliance on national security concerns such as terrorism to justify engaging in enforced disappearances, as well as the silence of other states in the face of this impunity.[151] Similarly, national security concerns have repeatedly been used to justify the unlawful use of spyware, with little response from other states. This has contributed to the proliferation of human rights abuses, including enforced disappearances. In pushing for regulation, the Working Group should join advocacy groups in emphasizing the need for transparency and accountability mechanisms as central features of regulation. These would be important measures to address impunity in relation to enforced disappearances.

VIII. Conclusion

Spyware is a growing threat to democracy and human rights around the world, and contributes to egregious abuses, including enforced disappearances. The international community must grapple with the devastating impacts of spyware on human rights defenders and others as the threat of government surveillance is no longer constrained by geographical boundaries. Left unchecked and unregulated, spyware will continue to be used to flout human rights, as international and domestic laws are failing to keep up with technological developments. We urge the Working Group to adopt the above recommendations: to highlight the role of spyware in the upcoming thematic study; explain how spyware negatively impacts human rights defenders and their work; investigate how to further support human rights defenders who are at risk of surveillance; and join research and advocacy groups in advocating for comprehensive regulations of the global spyware industry. As noted by Marietje Schaake, we must "find ways to govern technology in democracy's image."[152]

---

[151] UN Human Rights Council (2021), "Enforced or involuntary disappearances: Report of the Working Group on Enforced or Involuntary Disappearances," 48th Sess, UN Doc A/HRC/48/57 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/215/21/PDF/G2121521.pdf?OpenElement>; UN Human Rights Council, "Working Group on Enforced or Involuntary Disappearances: Report of the Working Group on Enforced or Involuntary Disappearances," 42nd Sess, UN Doc A/HRC/42/40 at para 58 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/229/25/PDF/G1922925.pdf?OpenElement>.

[152] Justin Hendrix (2021), "Marietje Schaake on the Treat the Global Spyware Industry Poses to Democracy," *Tech Policy Press* (27 July 2021)

<https://techpolicy.press/marietje-schaake-on-the-threat-the-global-spyware-industry-poses-to-democracy/>.