Clipping Pegasus's Wings

THE PRESENT LEGAL LANDSCAPE FOR RESTRAINING THE PRIVATE SURVEILLANCE INDUSTRY'S GLOBAL ATTACK ON HUMAN RIGHTS & A ROADMAP TO A BAN

by International Justice Clinic of University of California, Irvine School of Law

#4 Corporate responsibility to respect human rights

By around 2015, only a handful of wealthy governments which enjoyed internal capacity and resources to build spyware were able to use spyware. However, as a recent trend, more and more governments are using spyware by procuring spyware and technical support from private vendors such as NSO Group. David Kaye, our clinic's director and a former Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, pointed out in his 2019 report that "[d]igital surveillance is no longer the preserve of countries that enjoy the resources to conduct mass and targeted surveillance based on in-house tools. Private industry has stepped in, unsupervised and with something close to impunity."[1]

The private actors that are part of the private surveillance ecosystem and are, in principle, subject to existing law and regulation of countries and areas where they are headquartered and where they do business. In addition to these hard laws, state obligations and corporate responsibility are detailed by the United Nations Guiding Principles on Business and Human Rights (UNGPs). The UNGPs were adopted in 2011 by Human Rights Council, the central human rights body in the UN system, in response to the emerging human rights violations originated or facilitated by multi-national corporations' business, often in Global South countries. The Guiding Principles are, while soft law, highly regarded as an instrument to address human rights violations and their risks especially in the areas where states have not taken sufficient actions or do not have the intention to respect and protect individuals' human rights through regulations, just like digital surveillance. While often framed as principles for corporate responsibility, the first pillar of the UNGPs emphasizes the importance of state action to protect individuals against the abuses of third parties such as business entities.

The tenor of the UNGPs is the United Nations' longstanding framework, "Protect, Respect, and Remedy".[2] While it is states' responsibility to "protect" (i.e., protect individuals' human rights

[1] David Kaye, *Surveillance and human rights*, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (May 28, 2019), UN Doc. A/HRC/41/35, para 6, https://undocs.org/A/HRC/41/35.
[2] Office of the United Nations High Commissioner for Human Rights (OHCHR), Guiding Principle on Business and Human Right (2011), http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

from harm), the responsibility to "respect" (i.e., prevent and address human rights abuses) belongs to states as well as private actors. The duty to "remedy" (i.e., provide effective remedies of past or ongoing human rights violations to people affected) also belongs to states and, at least partly, to companies. The Guiding Principles are grounded in recognition of these three general principles, the second of which prescribes steps for private actors to perform their obligations to "Respect" human rights, which we highlight in the following sections.[3]

A. CORPORATE RESPONSIBILITY TO RESPECT HUMAN RIGHTS

a. Foundational Principles

As foundational principles, Guiding Principle 11, 12, 13 of UNGP sets out, in principle:

- Business has a responsibility to "respect human rights," meaning that "they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved." (Principle 11);
- Business's responsibility to respect human rights includes: (a) "to avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur"; and (b) "seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts." (Principle 13)
- Business's responsibility to respect human rights apply to all companies, "regardless of their size, sector, location, ownership and structure;" however, these factors will affect the complexity and scale of the actions a private actor should take to meet the UNGP. (Principle 14)
- "Human Rights" in UNGP refers to those " internationally recognized human rights – understood, at a minimum, as those expressed in the International Bill of Human Rights." This refers the Universal Declaration of Human Rights , International Covenant on Civil and Political Rights (ICCPR), which covers rights particularly affected by with digital surveillance, namely, the rights to privacy and freedom of opinion and expression, and International Covenant on Economic, Social and Cultural Rights (ICESCR). (Principle 12)
- Private companies should set out in the form of a written policy: (a) a "commitment to meet their responsibility to respect human rights"; (b) its "human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights"; (c) "processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute. (Principle 15)

b. Operational Principles

Among Principles 16 to 24, which set out concrete actions companies are expected to take to perform their responsibility to "Respect" and "Remedy", Principles 17 to 22 are about the

[3] *Id.*

human rights due diligence, a key system to process to identify, assess, mitigate human rights risks and remediate human rights violations which companies should put in place.

- Human rights impacts which a company's due diligence mechanism address are those which the company "may cause or contribute to through its own activities, or which may be directly linked to its operations, products or services by its business relationships." (Principle 17(a))
- Human rights due diligence is an ongoing process. Companies should keep assessing the human rights risks given the evolving nature of their business and operating context. (Principle 17(c)) For the risk identification and assessment, companies should (a) "draw on internal and/or independent external human rights expertise;" and (b) involve meaningful consultation with potentially affected groups."
- Companies should take action to mitigate human rights risks in accordance with their risk assessment (Principle 19) and track the effectiveness of their actions. (Principle 20).
- Companies should communicate how they address human rights risks with sufficient details to evaluate whether they have taken adequate response to a particular human rights risk. (Principle 21)
- When companies found past or ongoing adverse human rights impact which they caused or contributed to, "they should provide for or cooperate in their remediation through legitimate processes." (Principle 22)

B. CORPORATE RESPONSIBILITY OF SPYWARE COMPANIES AND THIRD PARTIES

There are a wide variety of private actors involved in digital surveillance, for example, spyware manufacturers and vendors, investors and suppliers of spyware, developer of software of which security would be compromised by way of spyware infection and operation. Each of these actors has different responsibility under UNGP. Given the private actors' role in surveillance by spyware, measures which UNGPs requests on each of these actors are essential, although not sufficient, to mitigate the private spyware threat.

a. Spyware vendors

First and foremost, the UNGP requires companies to avoid infringing on the human rights of others (Principle 11). As we detailed in Chapter 2 of our report ("Pegasus's impact on human rights"), the use of spyware inevitably restricts the rights to privacy (ICCPR Article 17) and freedom of opinion and expression (Article 19). And under the most likely scenario that, in the case of the use of Pegasus or similar spyware, such restrictions cannot meet the stringent test to be qualified as permitted restrictions, meaning per se violating these rights, due to their unique functionalities, e.g., indiscriminate access capability, zero-click attack, self-cleaning up of traces of infection or operations, NSO Group immediately stop developing, selling, or licensing such products to perform the duty under the UNGP.

Even if there were situations where spyware use meets permitted interference, NSO Group or other vendors which sell spyware with equivalent functionalities with Pegasus are required

under the UNGP to ensure that its clients are using their products only in a way that it meets the stringent test to be qualified to be permitted restriction of freedom of expression and privacy. More specifically, these companies can, in essence, sell or license lawful products only to governments that demonstrated with evidence that they have at minimum, all the following safeguards and longstanding, strong rule of law and human rights compliance. Spyware vendors should keep monitoring that clients keep meeting these conditions and stop the license when any of the conditions is not met. Further, to enable the ex-post notification (b. below) and oversight (c. below), spyware vendors must design spyware, as default, to leave sufficient traces of infection and operation of surveillance.

a. independent and impartial judicial pre-authorization of *all* cases of spyware use, regardless of domestic or extraterritorial use;[4]
b. ex-post notification to all individuals against whom spyware is used about the surveillance, including duration, scope and manner of the processing of the data obtained;
c. effective and independent oversight which (i) monitors every process of each spyware use, including judicial pre-authorization, actual spyware use, and termination of the use, (ii) investigates alleged misuse of spyware, and (iii) publicly discloses the result of such oversight for public scrutiny;[5]
d. prohibition of data sharing and data repurposing;[6]
e. prohibition of use of evidence which is directly or indirectly obtained through the misuse of spyware.[7]

Private surveillance companies have also utilized human rights language in a way that is deceiving and deceptive. For instance, NSO Group insists that their product helps governments fight terrorism despite the plethora of evidence showing the tool is used to spy on dissenters, activists, and journalists.

b. Investors of spyware vendors

The UNGP requires private actors not only avoid "causing" but "contributing to" human rights violations through their own activities. Investors thus have the responsibility to ensure that their portfolio companies are all performing their duty to respect human rights by adhering to UNGP. Investment in NSO Group, especially those by the US and UK firms, has attracted media

[4] See Human Rights Committee, Concluding Observations on Italy (May 1, 2017), CCPR/C/ITA/CO/6, para. 37. See also, Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age (August 3, 2018), A/HRC/39/29, para. 39 ([the judicial branch] "needs to make sure that there is clear evidence of a sufficient threat and that the surveillance proposed is targeted, strictly necessary, and proportionate and authorize (or reject) ex ante the surveillance measures;" Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age (June 30, 2014), A/HRC/27/37, para. 30.
[5] See, for example, Human Rights Committee, Concluding Observations on Macao, China (27 July 2022), CCPR/C/CHN-MAC/CO/2, paras. 33; Human Rights Committee, Concluding Observations on Georgia (September 13, 2022), CCPR/C/GEO/CO/5, para. 40. See also, The right to privacy in the digital age (2018), *supra* note 4, paras. 39 and 40; The right to privacy in the digital age (2014), *supra* note 4, para. 37 and 38.
[6] See Human Rights Committee, *Madhewoo v Mauritius*, CCPR/C/131/D/3163/2018, paras. 7.4 and 7.6; Concluding Observations on Canada (August 13, 2015), CCPR/C/CAN/CO/6, "C. Counter-terrorism."
[7] See Human Rights Committee, General Comment No. 20: Article 7 (Prohibition of torture, or other cruel, inhumane or degrading treatment or punishment (March 19, 1992), para. 12.

attention due to scrutiny about its human rights record.[8] As the latest development, the Biden administration warned, although it is based mainly on its national security interest, US companies which consider potential investment into spyware vendors that such an acquisition would be subject to stringent review by the US government.[9]

[8] See, for example, Andrew Selsky, Oregon Might Dump Controversial Spyware Investment, AP NEWS (December 17, 2021), https://apnews.com/article/technology-business-oregon-spyware-berkeley-7ed2f216d4d462998080d166cc823aae; Business and Human Rights Resource Centre (February 19, 2019), Novalpina Capital Buys Spyware Co. NSO Group, Commits to Greater Transparency but Rights Groups Call out Unaddressed Issues, https://www.business-humanrights.org/en/latest-news/novalpina-capital-buys-spyware-co-nso-group-commits-to-helping-it-become-more-transparent/; and Oregon State Treasury, Oregon Investment Council Agenda and Meeting Notes (April 24, 2022), https://www.oregon.gov/treasury/invested-for-oregon/Documents/Invested-for-OR-47OIC-Agenda-and-Minutes/2022/03-09-22-OIC-Public-Book-FINAL.pdf.

[9] The Guardian, White House issues warning to US firms interested in acquiring Israeli surveillance tech (June 29, 2023), https://www.theguardian.com/us-news/2023/jun/29/israel-nso-surveillance-spyware-pegasus-simonds-biden-national-security.