The Surveillance Industry and Human Rights

Submission to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

by Sarah McKune*

March 2, 2019

*The author is a U.S. lawyer and independent consultant with expertise in international human rights law, intellectual property law, and export controls. She is also a Fellow with the Citizen Lab at the Munk School of Global Affairs and Public Policy, University of Toronto. The author submits this work in her independent capacity; opinions reflected herein are solely those of the author and do not represent the positions of any entity with which she is affiliated.

It is now well-established that digital surveillance technologies are frequently used in a manner that undermines internationally-recognized human rights.[1] It is of course true — as spyware companies reflexively assert when challenged regarding their rights impact[2] — that digital surveillance tools can facilitate law enforcement and intelligence efforts to investigate and prevent serious crimes, including terrorism. It is equally true that many regimes have *simultaneously* used those digital surveillance tools to target entities or individuals who are critical of their governance,[3] despite the nonconformity of such practice with international human rights law. One use of the tool, to counter crime for the benefit of society, does not erase other uses of the tool that violate human rights. Yet the lack of progress within the digital surveillance industry to credibly address its own serious human rights impacts suggests that significant intervention is required to prompt this relatively young industry to mature.

This submission highlights certain **systemic conditions** that have enabled rights abuses and impunity within the digital surveillance trade. Such conditions have allowed digital surveillance companies to proliferate and earn substantial revenue[4] while avoiding genuine accountability structures, transparency, human rights due diligence, and remediation mechanisms. The submission concludes by laying out **recommendations** for areas that stakeholders – including the United Nations, states, companies, and civil society – should address to promote a maturation of the digital surveillance industry on the basis of international human rights standards.

A. Systemic Conditions Enabling Rights Abuses and Impunity within the Digital Surveillance Trade

1. *Lack of normative consensus by states on treatment of digital vulnerabilities and digital espionage.*

In addressing private sector participation in government digital surveillance operations, it is important to first note that the legitimacy of state retention of digital vulnerabilities and engagement in digital espionage is far from settled. Under international human rights law, states "should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality."[5] Each of these principles is sorely tested by existing state digital surveillance practices – particularly surveillance that relies on the use of zero-day (undisclosed and unpatched) vulnerabilities, such as those incorporated in NSO Group's

[1] See, e.g., Citizen Lab, *Targeted Threats*, https://citizenlab.ca/category/research/targeted-threats/; Privacy International, *The Global Surveillance Industry*, July 2016, https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf; Access Now, *Alert: FinFisher Changes Tactics to Hook Critics*, May 2018, https://www.accessnow.org/cms/assets/uploads/2018/05/FinFisher-changes-tactics-to-hook-critics-AN.pdf.
[2] See, e.g., Ronen Bergman, "Weaving a cyber web," Ynetnews, January 11, 2019, https://www.ynetnews.com/articles/0,7340,L-5444998,00.html; David Kushner, "Fear This Man," *Foreign Policy*, April 26, 2016, https://foreignpolicy.com/2016/04/26/fear-this-man-cyber-warfare-hacking-team-david-vincenzetti/.
[3] Supra n. 1.
[4] See, e.g., Francisco Partners, "NSO Group Acquired by its Management," February 14, 2019, https://www.franciscopartners.com/news/nso-group-acquired-by-its-management ("[NSO Group] has grown rapidly and finished 2018 with revenues of $250 million, and dozens of licensed customers.").
[5] Resolution adopted by the Human Rights Council on 23 March 2017, "The right to privacy in the digital age," A/HRC/RES/34/7, https://undocs.org/A/HRC/RES/34/7, at para. 2.

"Trident" exploit chain.[6] Only a handful of governments have publicly addressed treatment of digital vulnerabilities, including the question of whether to retain previously unknown vulnerabilities for offensive use, or to disclose them to the relevant hardware and software companies to patch in order to prevent compromise of public-facing digital platforms.[7] Moreover, government embrace of offensive use of digital vulnerabilities, with few clear restraints on such activity, has given a green light to the private surveillance industry: they may take a no-holds-barred approach to utilizing digital vulnerabilities in surveillance tools, and need not engage in responsible disclosure of vulnerabilities, so long as they sell their tools and services to the "right" buyer.

In essence, states have shifted the target of inquiry from the legitimacy of *use* of invasive digital surveillance techniques, to the legitimacy of the *user* of those techniques. Indeed, the international community has thus far focused primarily on sales as the key point of intervention in addressing digital surveillance tools, with changes to export control frameworks meant to cover such tools beginning in late 2013.[8] Such an approach has significant drawbacks from an international human rights law perspective: rights-based parameters for surveillance capabilities, and for state and private sector engagement in digital espionage, remain relatively unexplored; state implementation of export controls is inconsistent, affected by competing priorities such as equipping law enforcement and intelligence partners, support for industry, and economic impacts; and, a focus on sales requires reliance on profit-motivated companies to assess the legitimacy of their clients, despite the inherent conflicts of interest in and limitations to such assessment.

The heavy reliance by some states on private sector involvement to conduct digital espionage also requires further normative analysis. States engage in digital espionage purportedly in furtherance of national security objectives, raising questions as to whether digital espionage is an "inherently state function" that should remain the exclusive province of government entities.[9] In comparison, with respect to the analogous industry of private military and security companies (PMSCs), the UN Working Group on the use of mercenaries proposed an international convention affirming the existence of "inherently state functions" over which the state must maintain a monopoly. These are functions that the state "cannot outsource or delegate to PMSCs under any circumstances. Among such functions are direct participation in hostilities, waging war and/or combat operations, taking prisoners, law-making, *espionage, intelligence, knowledge transfer with military, security and policing application* . . ." (emphasis added).[10] This concept of

---

[6] Bill Marczak and John Scott-Railton, *The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender*, Citizen Lab, August 24, 2016, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

[7] See Sven Herpig and Ari Schwartz, "The Future of Vulnerabilities Equities Processes Around the World," Lawfare, January 4, 2019, https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world.

[8] See Garrett Hinck, "Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research," Lawfare, January 5, 2018, https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research; Wassenaar Arrangement, List of Dual-Use Goods and Technologies and Munitions List, December 2018, available at https://www.wassenaar.org/control-lists/ (provisions 4.A.5., 4.D.4., 4.E.1.c., and 5.A.1.j.).

[9] See generally Scott M. Sullivan, *Private Force / Public Goods*, 42 Conn. L. Rev. 853 (2010).

[10] Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination, 25 August 2010, A/65/325, https://undocs.org/A/65/325, at Annex, Art. 2.

performance of an inherently state function appears equally applicable to digital surveillance services. Digital intrusions by non-state actors are uniformly recognized as illegal;[11] it is the involvement of the state that provides the veneer of legitimacy for such activities. Thus, the active participation by digital surveillance companies in state espionage[12] – whether by designing the method to achieve persistent access to a target, training government personnel in how to effectively employ the tool, or trouble-shooting the range of problems government personnel encounter while utilizing those tools against live targets – strongly resembles the performance of an inherently state function. Private sector involvement in inherently state functions creates a multitude of risks, including insufficient oversight of and accountability mechanisms for activities tied to the use of force.[13]

State treatment of digital vulnerabilities and engagement in digital espionage present complex questions, some of which may be beyond the scope of the Special Rapporteur's report regarding the surveillance industry and human rights. They are, however, factors that play a critical role in the growth of the digital surveillance industry, its lack of transparency, and its resistance to oversight and accountability.

2. *Lack of transparency in the digital surveillance industry.*

The digital surveillance industry is characterized by its lack of transparency. Research has provided some insight into participating companies and their products.[14] However, the full breadth of the industry and the capabilities on offer remain unclear. Private companies have successfully shielded their own work from view on the basis of the secrecy associated with the law enforcement or intelligence operations of their government clientele. Companies implicated

[11] See, e.g., Council of Europe, *Convention on Cybercrime*, November 23, 2001, Arts. 2-6, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185; U.S. Computer Fraud and Abuse Act, 18 U.S.C. § 1030, https://www.law.cornell.edu/uscode/text/18/1030.

[12] Espionage is generally understood as the *collection* of sensitive, non-public information. See Raphael Bitton, "Article: The Legitimacy of Spying Among Nations," 2014, 29 Am. U. Int'l L. Rev. 1009 ("The article's account of international espionage begins from the observation that states restrict access to various spaces that serve as points of access to information and that espionage seeks to penetrate such spaces to collect information. Espionage between states is therefore an undercover state-sponsored intrusion into the restricted space of another state or organization for the sake of collecting information."); Christian Schaller, "Spies," in *The Law of Armed Conflict and the Use of Force: The Max Planck Encyclopedia of Public International Law*, 1173-1177, Oxford (UK): Oxford University Press, 2017, at p. 1173 ("Spies are commonly understood as individuals secretly engaged in the collection of particularly sensitive information for intelligence purposes, usually serving the interests of a State, international organization, or corporate entity. Within this meaning espionage is just a specific method of obtaining information . . . ."); Glenn P. Hastedt, ed., *Spies, Wiretaps, and Secret Operations: An Encyclopedia of American Espionage*, Santa Barbara: ABC-CLIO, 2011, at xxi ("The second step in the intelligence process is collection. It is here that espionage enters the intelligence cycle. It is one way of obtaining the information identified as important in the first stage."). Accordingly, regardless of whether a private company is ultimately privy to the intelligence collected, by actively involving itself in the collection stage – e.g., creating vulnerability exploits designed to work on a platform of interest to the client, designing software that will surreptitiously enable remote access and collect data, and constructing network infrastructure through which to transmit data in an untraceable manner – the company is effectively participating in espionage. For its part, the government client is simply deploying a method of espionage administered by the company, in support of the government intelligence process.

[13] See generally Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination, 25 August 2010, A/65/325, https://undocs.org/A/65/325, at section II.

[14] See, e.g., Privacy International, *Surveillance Industry Index*, http://sii.transparencytoolkit.org/.

in rights-related scandals have asserted the existence of contractual confidentiality provisions[15] and national security considerations[16] as barriers to disclosure of any information. While some states release limited information concerning the export of digital surveillance tools,[17] this practice is far from uniform, and within the EU efforts to establish more substantive reporting through export regulations have stalled.[18]

The broader ecosystem of private financing that fuels much of the industry compounds its lack of transparency and accountability. Some of the larger companies that offer a range of products and services beyond surveillance tools – such as Verint[19] and Elbit Systems[20] – are publicly traded, and accordingly report information concerning their corporate structure, operations, and revenues. Yet many companies, including those implicated in rights abuses, are backed by private investment.[21] Private equity firms, venture capital firms, or angel investors operate with little public accountability, yet directly spur the growth of digital surveillance services of questionable legality. These private investors typically assume significant roles in the strategic direction of a company, claiming board seats and applying their expertise to enhance the company's business and maximize its value. Such activity, which could be determinative in a company's approach to human rights, takes place behind closed doors, inaccessible to public scrutiny.

The case of NSO Group is illustrative. Private equity firm Francisco Partners – which "invests in opportunities where its deep sectoral knowledge and operational expertise can help companies realize their full potential"[22] – acquired a reported 70 percent stake[23] in the company for USD

[15] See, e.g., Human Rights Watch, "Ethiopia: New Spate of Abusive Surveillance," December 6, 2017, https://www.hrw.org/news/2017/12/06/ethiopia-new-spate-abusive-surveillance ("Finally, [Cyberbit] stated that while it cannot confirm or deny any specific transaction or client, the company appreciates the concerns raised and is 'addressing it subject to the legal and contractual confidentiality obligations Cyberbit Solutions is bound by.'").
[16] See, e.g., Ronen Bergman, "Weaving a cyber web," Ynetnews, January 11, 2019, https://www.ynetnews.com/articles/0,7340,L-5444998,00.html ("For most of this period, NSO maintained a policy typical of intelligence bodies that espouse secrecy, which is to respond in one way only – with silence.").
[17] See Privacy International, "An Open Source Guide to Researching Surveillance Transfers," August 23, 2018, https://privacyinternational.org/feature/2225/open-source-guide-researching-surveillance-transfers.
[18] European Parliament, "Legislative Train Schedule: Review of Dual-Use Export Controls," http://www.europarl.europa.eu/legislative-train/theme-europe-as-a-stronger-global-actor/file-review-of-dual-use-export-controls; Access Now, "EU: Leak reveals states are ready to put human rights defenders at risk to protect surveillance industry," October 29, 2018, https://www.accessnow.org/eu-leak-reveals-states-are-ready-to-put-human-rights-defenders-at-risk-to-protect-surveillance-industry/; Lucie Krahulcova, "The European Parliament is fighting to strengthen the rules for surveillance trade," Access Now, December 8, 2017, https://www.accessnow.org/european-parliament-fighting-strengthen-rules-surveillance-trade/.
[19] Verint, "Investor Relations," https://www.verint.com/investor-relations/.
[20] Elbit Systems, "Investor Relations," http://ir.elbitsystems.com.
[21] See, e.g., David Leigh, "Offshore company directors' links to military and intelligence revealed," *The Guardian*, November 28, 2012, https://www.theguardian.com/uk/2012/nov/28/offshore-company-directors-military-intelligence; Lorenzo Franceschi-Bicchierai, "Hacking Team Is Still Alive Thanks to a Mysterious Investor From Saudi Arabia," *Motherboard*, January 31, 2018, https://motherboard.vice.com/en_us/article/8xvzyp/hacking-team-investor-saudi-arabia.
[22] Francisco Partners, "NSO Group Acquired by its Management," February 14, 2019, https://www.franciscopartners.com/news/nso-group-acquired-by-its-management.
[23] Shoshanna Solomon, "NSO founders, management buy stake in firm from Francisco Partners," *Times of Israel*, February 14, 2019, http://www.timesofisrael.com/nso-founders-management-buy-stake-in-firm-from-francisco-partners/.

$115 million in March 2014, through its Francisco Partners III LP investment fund.[24] Francisco Partners installed operating partner Eran Gorev – the former president and CEO of surveillance company NICE Systems – on the board of NSO Group,[25] presumably to guide the company in growing its business. It is unclear what knowledge the limited partners of the Francisco Partners III fund – including numerous pension and retirement funds and other institutional investors[26] – had regarding the presence in their investment portfolios of the spyware company.[27] After numerous reports of abuse of NSO Group's technology and two failed attempts at a sale of the company,[28] in February 2019 it was announced that NSO founders and management, together with private equity firm Novalpina Capital, had bought out Francisco Partners' stake.[29] Yet even as Francisco Partners walks away from the company, it has never publicly reckoned with the human rights impacts of its nearly five-year guidance of NSO Group, the same period in which

[24] Bloomberg L.P., *Francisco Partners III LP current portfolio*, retrieved February 8, 2019 from Bloomberg terminal.

[25] Francisco Partners, "NSO Group Acquired by its Management," February 14, 2019, https://www.franciscopartners.com/news/nso-group-acquired-by-its-management.

[26] The limited partners of Francisco Partners III LP included: Oregon Public Employees Retirement System; California Public Employees' Retirement System; Florida Retirement System; California State Teachers' Retirement System; University of Texas Investment Management Company; Colorado Public Employees' Retirement Association; School Employees Retirement System of Ohio; West Midlands Pension Fund; Regents of the University of California; University of Michigan; Pennsylvania State Employees' Retirement System; Ohio Police & Fire Pension Fund; Cheyenne Capital Fund LP; Virginia G. Piper Charitable Trust; Acacia Life Insurance Co.; SEB Pensionsforsikring A/S; Trustees of Grinnell College; BP PLC; Ameritas Life Insurance Corp; Prudential Insurance Co of America; Allstate Life Insurance Co; Allstate Insurance Co; Boeing Co; Ford Motor Co; HP Inc; British Columbia Investment Management Corp; Crankstart Foundation; Michigan State University; STRS Ohio; Permanent University Fund; and Lockheed Martin Corp. Many of these entities were repeat investors with Francisco Partners. Bloomberg L.P., *Francisco Partners III LP private equity fund holders*, retrieved February 8, 2019 from Bloomberg terminal.

[27] For example, one limited partner, the University of Michigan, noted in its 2009 follow-on investment report that "Francisco Partners III, L.P. . . . will invest in mature technology and technology-related companies in the communications, hardware, information technology services and software sectors." University of Michigan Regents Communication, "Item for Information," September 2009, http://www.regents.umich.edu/meetings/09-09/2009-09-IX-4.pdf. The scope of the investment strategy as described does not give the impression that the portfolio would include "cybersecurity" investments – particularly a young company such as NSO Group (founded in 2010) that specializes in controversial vulnerability exploits and surveillance infrastructure. Additionally, a Francisco Partners investor presentation from 2017 made to the Nebraska Investment Council included a slide showcasing its current technology investments, but rather than referring to NSO Group itself, the slide referred only to OSY Technologies – the parent of NSO Group's holding company Q Cyber Technologies. (Q Cyber Technologies SARL, the holding company to which NSO Group belongs, is a subsidiary of OSY Technologies SARL, which is itself a subsidiary of Square 2 SARL. The three companies are incorporated in Luxembourg; Eran Gorev is listed as a manager of both Q Cyber Technologies and OSY Technologies. Dun & Bradstreet, One-Stop Reports: Q Cyber Technologies SARL; OSY Technologies SARL, retrieved from Hoover's database, February 26, 2019.) Interestingly, OSY Technologies is the only portfolio company listed on the slide that appears in a basic font, lacking any logo. See Francisco Partners, "Francisco Partners Overview," p. 4, available at https://nic.nebraska.gov/sites/nic.nebraska.gov/files/doc/7.b.%20%20%20%20%20%20%20%20%20%20%20%20%20Francisco%20Partners%20Presentation.pdf.

[28] Alex Plough, Yifan Yu, and Mariana Valle, "Israeli Spyware Firm NSO Group Confronts Controversial Past As It Seeks $500 Million Buyout Loan," *Forbes*, February 25, 2019, https://www.forbes.com/sites/debtwire/2019/02/25/israeli-spyware-firm-nso-group-confronts-controversial-past-as-it-seeks-500-million-buyout-loan.

[29] Shoshanna Solomon, "NSO founders, management buy stake in firm from Francisco Partners," *Times of Israel*, February 14, 2019, http://www.timesofisrael.com/nso-founders-management-buy-stake-in-firm-from-francisco-partners/.

Pegasus spyware abuses came to light.

The limited information that has emerged about this industry is the result of the efforts of NGOs, academics, journalists, and lawyers, who have overcome significant hurdles in uncovering details of the opaque digital surveillance trade. Disturbingly, some groups and individuals who have engaged in research and raised concerns regarding the use of surveillance technologies have found themselves subjected to intimidation and disparagement; threats of legal action; and even "dirty ops" campaigns, in which private intelligence operatives attempted to lure individuals into making damaging statements that were surreptitiously recorded.[30] Such malicious tactics underscore the urgent need for greater transparency in the surveillance industry.

3. *Significant overlap between state defense and intelligence agencies and the private digital surveillance industry.*

While the lack of transparency in this industry makes it difficult to assess the extent of the overlap, reporting suggests that many individuals who participate in the spyware trade come from or have connections to state defense or intelligence entities. For example, alumni of the Israel Defense Force's elite intelligence unit, Unit 8200, reportedly developed the technology underlying NSO Group's Pegasus spyware,[31] and founded NICE Systems[32] and Elbit Systems' cyber division.[33] Indeed, Unit 8200 is considered by both the government and private sector as an incubator for top technical talent who will launch lucrative cybersecurity companies after their service.[34] It has also come to light that former NSA staff were employed by the government of the UAE to engage in an invasive digital surveillance operation known as Project Raven, using "methods learned from a decade in the U.S intelligence community to help the UAE hack into the phones and computers of its enemies."[35] These individuals were first contracted through

[30] See, e.g., Bill Marczak, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert, "Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?," Citizen Lab, March 9, 2018, at section 7 ("Communication with Sandvine and Francisco Partners"), https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/; Raphael Satter, "APNewsBreak: Undercover agents target cybersecurity watchdog," Associated Press, January 26, 2019, https://www.apnews.com/9f31fa2aa72946c694555a5074fc9f42; Raphael Satter, "AP Exclusive: Undercover spy exposed in NYC was 1 of many," Associated Press, February 11, 2019, https://www.apnews.com/9bdbbfe0c8a2407aac14a1e995659de4; Amarelle Wenkert, "NSO Is the Common Link in International Covert Operation, Report Says," CTech by Calcalist, February 11, 2019, https://www.calcalistech.com/ctech/articles/0,7340,L-3756120,00.html.

[31] Ronen Bergman, "Weaving a cyber web," Ynetnews, January 11, 2019, https://www.ynetnews.com/articles/0,7340,L-5444998,00.html.

[32] Ruti Levy, "Who Makes Millions Off Israel's Top Cyber Spy Agency?," *Haaretz*, April 21, 2017, https://www.haaretz.com/israel-news/business/who-makes-millions-off-israel-s-top-cyber-spy-agency-1.5458636.

[33] Richard Behar, "Inside Israel's Secret Startup Machine," *Forbes*, May 11, 2016, https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine.

[34] Ruti Levy, "Who Makes Millions Off Israel's Top Cyber Spy Agency?," *Haaretz*, April 21, 2017, https://www.haaretz.com/israel-news/business/who-makes-millions-off-israel-s-top-cyber-spy-agency-1.5458636; Tim Johnson, "How Israel became a leader in cybersecurity and surveillance," *Miami Herald*, February 21, 2017, https://www.miamiherald.com/news/nation-world/national/article134016704.html; Richard Behar, "Inside Israel's Secret Startup Machine," *Forbes*, May 11, 2016, https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine; Gil Kerbs, "The Unit," *Forbes*, February 8, 2007, https://www.forbes.com/2007/02/07/israel-military-unit-ventures-biz-cx_gk_0208israel.html.

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

the U.S.-based company CyberPoint; some later went on to work for the UAE company DarkMatter, after the UAE government chose to transfer the operation to the local company.[36]

The impact of this overlap requires further analysis. When skill-sets and mind-sets cultivated for the purpose of state signals intelligence are redirected to the private sector, there is a risk of transplanting invasive digital surveillance techniques from a context in which they may have some legitimacy and oversight, to contexts that lack legitimacy and oversight altogether. Moreover, individuals paid at significantly higher rates for work in the private sector may have incentive to avoid questioning the new ends to which their skills are put.[37] In the case of the UAE's Project Raven, according to the description of the former NSA analyst involved, there was little consideration paid to critical contextual differences in application of her skills:

> *Under orders from the UAE government, former operatives said, Raven would monitor social media and target people who security forces felt had insulted the government.*
>
> *"Some days it was hard to swallow, like [when you target] a 16-year-old kid on Twitter," [former NSA analyst Lori Stroud] said. "But it's an intelligence mission, you are an intelligence operative. I never made it personal." . . .*
>
> *Stroud discovered that the program took aim not just at terrorists and foreign government agencies, but also dissidents and human rights activists. The Emiratis categorized them as national security targets.*

It was only after Stroud discovered the targeting of U.S. persons in the surveillance operation – an arbitrary distinction under international human rights law – that she began to question the work.[38] Additionally, close ties between state and industry could influence the decisions of key government officials (regulators, policymakers, judges, etc.) concerning surveillance technology, who may regard growth in the sector as a higher priority than curbing its human rights impacts.[39] Finally, the reliance of the private surveillance industry on the specialized knowledge of state signals intelligence alumni is further reason to view companies' participation in digital espionage activities as performance of a function that originates with, and should remain the monopoly of, the state.

4. *Lack of effective self-regulatory or internal initiatives in the digital surveillance industry to operationalize the corporate responsibility to respect human rights.*

The silence of the digital surveillance industry regarding the UN Guiding Principles is noteworthy. It is telling that, while communications with industry participants,[40] analyses

---

[36] Ibid.
[37] See, e.g., ibid. ("Many analysts, like Stroud, were paid more than $200,000 a year, and some managers received salaries and compensation above $400,000.").
[38] Ibid. ("'I don't think Americans should be doing this to other Americans,' [Stroud] told Reuters.").
[39] See, e.g., Hagar Shezaf and Jonathan Jacobson, "Revealed: Israel's Cyber-spy Industry Aids World Dictators Hunt Dissidents and Gays," *Haaretz*, October 20, 2018, https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027.
[40] See, e.g., Letter from Prof. Ronald Deibert, Citizen Lab, to Mr. Dipanjan (DJ) Deb, Francisco Partners, November 1, 2018, https://citizenlab.ca/wp-content/uploads/2018/11/November-1-2018-Letter-to-FP.pdf; Letter from Prof. Ronald Deibert, Citizen Lab, to Mr. Dipanjan (DJ) Deb and Mr. Andrew Kowal, Francisco Partners, May 29, 2018, https://citizenlab.ca/wp-content/uploads/2018/05/Letter-to-Francisco-Partners-May-29-2018.pdf; Letter from Prof.

concerning the digital surveillance industry,[41] and other ICT company corporate responsibility frameworks such as the Global Network Initiative[42] have highlighted the importance of the UN Guiding Principles, digital surveillance companies have refused to invoke their existence. Companies have instead asserted their adoption of alternative models, for example, alleged compliance with "U.S. Know Your Customer guidelines" (Hacking Team);[43] purportedly appointing human rights officers to company boards and creating codes of conduct (FinFisher);[44] or "working with a group of Washington-based consultants and law firms to craft [] export and ethics policies,"[45] including "a best-in-class business ethics framework and bringing in independent experts to ensure the company was operating in accordance with the highest ethical standards"[46] (NSO Group and Francisco Partners). Consistent among these approaches is an emphasis on inward-facing evaluation, and the lack of any component of transparency or accountability, such as mechanisms to publicly report on or respond to complaints of abuses. The weakness of relying on self-selected and self-enforced standards to address a company's human rights impacts, rather than the UN Guiding Principles, is apparent in the track records of digital surveillance companies, which have continued to supply products and services to known abusers of surveillance software.[47]

Only one recent statement out of this sector references the UN Guiding Principles: Novalpina Capital, NSO Group's new shareholder, noted that "we believe that NSO Group should be – and can be – operated in accordance with the UN Guiding Principles on Business and Human

---

Ronald Deibert, Citizen Lab, to Mr. David Vincenzetti, Hacking Team, August 8, 2014, https://citizenlab.ca/2014/08/open-letter-hacking-team/.

[41] See, e.g., Shift and the Institute for Human Rights and Business, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*, European Commission, https://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf, at 33; Human Rights Watch, *Human Rights Watch Submission re Human rights defenders and civic space in the context of business activities to the UN Working Group on Business and Human Rights*, September 8, 2017, https://www.hrw.org/news/2017/09/08/human-rights-watch-submission-re-human-rights-defenders-and-civic-space-context; Letter from Prof. Ronald Deibert, Citizen Lab, to the United Nations Working Group on Human Rights and Transnational Corporations and Other Business Enterprises, December 8, 2011, https://www.ohchr.org/Documents/Issues/TransCorporations/Submissions/AcademiaAndIndependentResearchers/CitizenLabUniversityTorontoMunkSchoolGlobalAffairs.pdf.

[42] See Global Network Initiative, Principles on Freedom of Expression and Privacy, https://globalnetworkinitiative.org/gni-principles/, at Preamble; "GNI Publishes Updates to the Core Commitments of our Membership," March 20, 2017, https://globalnetworkinitiative.org/gni-publishes-updates-to-the-core-commitments-of-our-membership/.

[43] Hacking Team, "Customer Policy," http://www.hackingteam.it/policy.html; compare to U.S. Department of Commerce Bureau of Industry and Security, Supplement No. 3 to Part 732 – BIS's "Know Your Customer" Guidance and Red Flags, available at https://www.bis.doc.gov/index.php/documents/regulation-docs/411-part-732-steps-for-using-the-ear/file.

[44] Jasmin Klofta, Frederick Obermeier, and Bastian Brinckmann, "Selling spyware to trap dissidents," VoxEurop, February 22, 2013, https://voxeurop.eu/en/content/article/3449501-selling-spyware-trap-dissidents.

[45] Josh Rogin, "Washington must wake up to the abuse of software that kills," *Washington Post*, December 12, 2018, https://www.washingtonpost.com/opinions/2018/12/12/washington-must-wake-up-abuse-software-that-kills.

[46] Francisco Partners, "NSO Group Acquired by its Management," February 14, 2019, https://www.franciscopartners.com/news/nso-group-acquired-by-its-management.

[47] See, e.g., Sarah McKune, Ron Deibert, Bill Marczak, Geoffrey Alexander, and John Scott-Railton, "Commercial Spyware: The Multibillion Dollar Industry Built on an Ethical and Legal Quagmire," Citizen Lab, December 6, 2017, https://citizenlab.ca/2017/12/legal-overview-ethiopian-dissidents-targeted-spyware/.

Rights."[48] This statement in effect suggests that up to this point, NSO Group has not committed to the UN Guiding Principles. It remains to be shown whether Novalpina Capital will see such a change through.

Robust multistakeholder initiatives, rooted in the UN Guiding Principles and in which industry plays a key role, could be instrumental in encouraging a "race to the top" to fulfill the corporate responsibility to respect human rights. When companies engage in industry-wide dialogue regarding human rights impacts and how to address them, competitive disadvantages associated with acting alone are reduced, and proposed solutions can reflect the unique characteristics and requirements of the industry. The involvement of stakeholders from civil society and government in such dialogue is likewise essential, to work with industry on rights-based approaches and ensure proper oversight and remediation.

The PMSC sector offers a model for consideration: the International Code of Conduct for Private Security Service Providers' Association (ICoCA).[49] ICoCA membership is based on adherence to a code of conduct that requires companies to "endorse the principles of the Montreux Document and the [] 'Respect, Protect, Remedy' framework [the precursor to the UN Guiding Principles endorsed by the Human Rights Council]," and to "affirm that they have a responsibility to respect the human rights of, and fulfil humanitarian responsibilities towards, all those affected by their business activities . . . ."[50] ICoCA has established company certification,[51] monitoring,[52] and complaints processes.[53] Critically, ICoCA's board of directors – which holds oversight powers[54] – incorporates equal representation from each of the three pillars of government, industry, and civil society.[55]

Like PMSCs, if the digital surveillance industry is to mature, it must become capable of addressing its own negative externalities. If industry participants consider that they cannot address human rights impacts without ultimately rendering their business unprofitable, perhaps that is a sign that digital espionage functions should remain inherent to the state and out of the hands of the private sector.

---

[48] See Richard Silverstein, "UK Investment Firm Claims Israeli Cyber-War Firm It Bought Adheres to UN Ethical Guidelines," Tikun Olam, February 21, 2019, https://www.richardsilverstein.com/2019/02/21/uk-investment-firm-claims-cyber-war-firm-it-bought-adheres-to-un-ethical-guidelines/.

[49] International Code of Conduct for Private Security Service Providers' Association (ICoCA), https://www.icoca.ch/en.

[50] *The International Code of Conduct for Private Security Service Providers*, https://www.icoca.ch/en/the_icoc, at Preamble.

[51] ICOCA Principles & Procedures: Article 11: Certification, https://www.icoca.ch/sites/default/files/uploads/ICoCA-Procedures-Article-11-Certification.pdf.

[52] ICOCA Procedures: Article 12: Reporting, monitoring and assessing performance and compliance, https://icoca.ch/sites/default/files/uploads/ICoCA-Procedures-Article-12-Monitoring.pdf.

[53] ICOCA Principles & Procedures: Article 11: https://www.icoca.ch/sites/default/files/uploads/ICoCA-Procedures-Article-13-Complaints.pdf

[54] See ICOCA Articles of Association, https://www.icoca.ch/sites/default/files/resources/Articles%20of%20Association.pdf, at Arts. 11-13.

[55] See ibid. at Art. 7.

B. Recommendations

In order to address the systemic conditions that have enabled rights abuses and impunity within the digital surveillance trade, and promote compliance with international human rights law, stakeholders should consider the following approaches.

- The international community should engage in substantive dialogue, with a view to promoting normative consensus, regarding the following topics:
    - State treatment of digital vulnerabilities, including expectations concerning the disclosure of such vulnerabilities in defense of public digital security, and processes for oversight. Such dialogue could be assisted by the creation of a UN working group specifically tasked to address the issue of treatment of digital vulnerabilities in accordance with international human rights law, and including members from the technical community.
    - Rights-based parameters for digital espionage, in light of a global climate in which the targeting of any person, anywhere, for any reason is technically and practically feasible.
    - Whether digital espionage and certain forms of participation by the private sector within that sphere should be considered "inherently state functions."
    - State responsibilities with respect to the digital surveillance companies domiciled or operating within their jurisdiction.
    - Methods to prevent the inappropriate transfer of state signals intelligence tactics and technology to the private sector.
    - How to address the competing priorities of states in administering export controls over digital surveillance items.
    - Protections for security research and other forms of inquiry into the digital surveillance trade.
- States should issue detailed policies on their treatment of digital vulnerabilities, as well as safe harbors for security research and responsible disclosure, soliciting public comment and incorporating public feedback on such policies.
- States should establish legal and regulatory frameworks in furtherance of the following objectives:
    - Prohibit forms of private sector participation in state digital espionage that amount to the performance of an "inherently state function."
    - Provide clear bases for jurisdiction over, and legal action against, government-linked entities engaged in extraterritorial, unauthorized digital surveillance.[56]
    - Provide clear bases for jurisdiction over, and legal action against, companies that facilitate digital surveillance against individuals or entities in violation of their internationally-recognized human rights.

[56] For example, United States courts, applying the Foreign Sovereign Immunities Act (FSIA), have held that extraterritorial digital surveillance is beyond the scope of the non-commercial tort exception to the FSIA, thus precluding jurisdiction over government entities that target individuals within the United States in violation of their internationally-recognized human rights. *Doe v. Federal Democratic Republic of Ethiopia*, 851 F.3d 7 (D.C. Cir. 2017), reh'g denied, 2017 U.S. App. LEXIS 10084 (D.C. Cir. June 6, 2017). Legislation to correct such deficiencies and provide remedy against malicious digital activity is essential to curbing inappropriate digital espionage practices.

- Enact regulation designed specifically to ensure transparency, accountability, and respect for human rights in the digital surveillance industry, such as requirements for company: registration and public reporting (including export reporting); human rights training, due diligence, and compliance; and mechanisms for receipt of complaints and remedial action. Such regulation can draw on learning from, and proposals made in, the PMSC sector.
- Link state procurement and various forms of state support (grants, trade promotion, etc.) to company human rights performance.[57]

- Participants in the digital surveillance industry – including spyware companies as well as the individuals and entities that invest in them – should explicitly commit to application of the UN Guiding Principles on Business and Human Rights in their industry. Industry participants should engage in multistakeholder dialogue regarding industry-wide operationalization of the UN Guiding Principles, with particular attention to transparency standards, human rights due diligence, and remediation mechanisms. At a minimum, stakeholders should address:
  - Disclosure requirements of private equity firms or other private investors to limited partners and/or government regulators regarding investments in dual-use technology companies.
  - Industry minimum standards for rejecting potential clients (e.g., previous involvement in spyware abuses, or track record of the use of torture), as well as for human rights policies and due diligence.
  - Establishment of internal human rights compliance programs with a "tone-at-the-top" of respect for human rights.
  - Essential technical design features of surveillance software and infrastructure to enable tracking of deployment, alerts to red flags of misuse, and, in the event of misuse, shutdown of the tool.
  - Required and prohibited activities of companies in engaging with clients, such as requirements for verification and human rights training of clients, and prohibitions on assistance to clients with targeting or certain forms of customization of a tool.
  - Essential contractual provisions to enforce respect for human rights, including: prohibition on use of a tool in violation of the *Universal Declaration of Human Rights*, the *International Covenant on Civil and Political Rights*, and applicable domestic laws in both the state of deployment and the state where a target is located; discontinuation of service in the event of misuse; regular human rights audits by the company of client use of its tool; specific activities in which the company will not engage for the client; specific client activity that will result in the waiver of client confidentiality.
  - Company notification requirements (e.g., reporting to a government agency or human rights ombudsperson) in the event of misuse of its surveillance tools.
  - Requirements for public transparency reporting, including with respect to company sales, surveillance capabilities offered, and instances of misuse.
  - Certification, monitoring, and oversight mechanisms, potentially using the ICoCA as a model.

[57] See, e.g., Report of the Working Group on the issue of human rights and transnational corporations and other business enterprises, 2 May 2018, A/HRC/38/48, https://undocs.org/A/HRC/38/48, at para. 99 ("States should require businesses to demonstrate an awareness of and commitment to the [UN] Guiding Principles as a prerequisite for receiving State support and benefits relating to trade and export promotion. . . .").

    - Publicly accessible, responsive, and effective operational-level grievance mechanisms at companies.
- Civil society, including technical communities, should continue their efforts to responsibly disclose digital vulnerabilities, share indicators and contextual details of spyware targeting, and report on findings of misuse of digital surveillance tools to the international community – all in furtherance of greater transparency surrounding the surveillance industry and its human rights impacts.