UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Who's Watching Little Brother?

A Checklist for Accountability in the Industry Behind Government Hacking

2 March 2017

Sarah McKune and Ron Deibert*

A Checklist for Accountability in the Industry Behind Government Hacking

- ☑ Identify commercial spyware companies' practices of concern.
- ☑ Define the goals of accountability measures.
- ☑ Continue to adapt export controls.
- ☑ Engage in criminal or civil litigation.
- ☑ Invoke consumer protection laws.
- ☑ Challenge contract violations and intellectual property infringements engaged in by commercial spyware companies.
- ☑ Develop an accountability framework specific to the private market for digital surveillance.
- ☑ Explore industry self-regulation.
- ☑ Build out communities of practice to raise public awareness and document abuses.

*Sarah McKune is Senior Legal Advisor at the Citizen Lab, Munk School of Global Affairs, University of Toronto. Ron Deibert is Professor of Political Science and Director of the Citizen Lab at the University of Toronto's Munk School of Global Affairs. The authors wish to thank Bill Marczak, Adam Molnar, Christopher Parsons, John Scott-Railton, and Erik Zouave for their valuable input which informed preparation of this article.

Citizen Lab research has frequently uncovered dark truths of the digital ecosystem. For instance, some of the most popular web and mobile applications, used by millions of people, employ weak or no encryption standards, or contain hidden keyword filtering and surveillance, while transmitting sensitive user data back to companies with little or no public transparency about with whom data is shared. Internet filtering technology is regularly installed on national ISPs to block access to important news, political criticism, and the work of human rights groups, despite the value of that information to the general public. And, perhaps most concerning: the relentless digital targeting by governments of individuals, just like you and me, who choose to speak out about issues of concern or attempt to promote peaceful change. Those targeted include activists, journalists, academics, researchers; sometimes collectively organized as NGOs, religious organizations, social movements; and any person or group that simply wants to express opinions on matters of public importance – collectively, "civil society."

Citizen Lab has written regularly about the digital crisis facing civil society, exposing threats against targets ranging from Tibetans to Ethiopian journalists, from the Syrian opposition to UAE activists, and beyond. While digital media have empowered civil society to learn, educate, organize, and make themselves heard by those in power, the vulnerabilities inherent in our technologies have also exposed civil society to serious risks. The ability of threat actors (particularly those with links to states) to know everything about you and your networks, to *even predict* your future actions, and to respond accordingly, is unparalleled. Not even physical borders keep one safe anymore.

Where some see insecurity, others see a welcome market opportunity. Indeed, business is booming for a specialized market to facilitate the digital attacks, monitoring, and intelligence-cum-evidence-gathering conducted by government entities or their proxies. Private companies with the advanced technical expertise and real passion for digital compromise assist governments in staying on the cutting edge of scientific and technological developments and deploying the latest digital attack techniques. (Encryption? Circumvention? Anonymity? No problem.) Most of us have no idea who these companies are, how they vet their clients, whether they have any knowledge of human rights issues, or whether they answer to anyone other than their CEOs or shareholders.

Sure, some of these companies have come to light, following challenging research and reporting on their products and services. Hacking Team. Gamma Group / FinFisher. NSO Group. An accumulating body of evidence over the last several years has shown how the vendors of commercial spyware are not averse to selling their wares to some of the world's most notorious autocratic regimes. Private companies have equipped regimes known to lack rule of law, abuse human rights, or engage in violent internal conflict, enhancing the ability of such regimes to further weaken and punish their citizenry and opposition. Spyware manufactured by Italy's Hacking Team and the UK/Germany-based Gamma Group, for example, was determined to be the weapon of choice for a dubious group of countries, including the United Arab Emirates, Morocco, Sudan, and Ethiopia. In one particularly egregious

example, Ahmed Mansoor, an activist in the UAE, was targeted over the course of five years with *multiple* forms of advanced commercial spyware, including that offered by Gamma Group, Hacking Team, and NSO Group. The NSO Group spyware even incorporated three distinct zero-day exploits capable of compromising the operating system of any iPhone; such zero-day exploits are reported to sell for as much as a million dollars.

Far from using this spyware solely to track what might be considered legitimate targets, these countries and their shadowy agencies have repeatedly used them to get inside the computers of human rights activists, journalists, opposition politicians, and even health advocates supporting a soda tax in Mexico. Some of the victims of these campaigns have found themselves arrested and tortured. Leaked emails from certain companies reveal that, despite public assurances by executives, the vendors seem cavalier about these type of abuses, have few internal checks in place to prevent them, and, indeed, knowingly court the clandestine agencies responsible for such abuses. Despite these alarming incidents, however, the dynamics of and participants in the market at large remain opaque.

We do know this: Government hacking is an increasingly utilized law enforcement and intelligence technique. In some cases it is a necessary component of critical investigations that bear on public security. With standardized end-to-end encryption of consumer communications platforms becoming more prevalent, law enforcement and intelligence agencies are targeting endpoint devices, further driving up the demand for lawful intercept products and services. But not all governments utilize due process in authorizing digital attacks. Not all governments target individuals for reasons permissible under international human rights law. Indeed, government misuse of spyware and other advanced dual-use technologies has become a regular and foreseeable occurrence. Incidents of digital attacks against civil society are on the rise, in violation of international and in some cases domestic law. What is to be done?

****

While government hacking raises many issues of concern that require public debate,[1] in this brief we focus primarily on the question of how to create accountability in the private market that *supplies* the digital surveillance tools used by many governments. In our view, checks on this market are both an essential element in curbing misuse of surveillance tools, and an appropriate

[1] For further discussion on human rights and government hacking, see Fabio Pietrosanti and Stefano Aterno, "Italy unveils a legal proposal to regulate government hacking," Boing Boing, February 15, 2017, http://boingboing.net/2017/02/15/title-italy-unveils-a-law-pro.html; Access Now, *A Human Rights Response to Government Hacking*, September 2016, https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf; and Electronic Frontier Foundation (EFF), "Government Hacking and Subversion of Digital Security," https://www.eff.org/issues/government-hacking-digital-security. Additionally, critical assessment of the closely-linked issue of vulnerabilities disclosure is crucial to this debate. See, e.g., EFF, "What to Do About Lawless Government Hacking and the Weakening of Digital Security," August 1, 2016, https://www.eff.org/deeplinks/2016/08/what-do-about-lawless-government-hacking-and-weakening-digital-security.

reflection of the responsibilities incumbent upon companies that would seek to profit from fulfilling state law enforcement and intelligence demands.

We present our thoughts and recommendations on elements of accountability for the commercial spyware trade in the form of a checklist. Some of the elements presented, such as export controls, have been debated at length; others, such as consumer protection and litigation strategies, have not. Our central thesis is that *there is no single mechanism best suited to addressing the problems associated with the spyware trade*; instead, we are better served by engaging a constellation of practices. When combined, these other practices can be thought of as a "web of constraints" around the commercial spyware market. While abuses of commercial spyware will likely never be eliminated entirely, this web of constraints can help build a community of practice, and legal and normative progress, that mitigate against them moving forward.

☑ Identify commercial spyware companies' practices of concern.

Identifying the practices of concern may seem like an obvious point, but the starting point for greater accountability must begin with the questions: what practices of this trade are we actually seeking to challenge? What is it about commercial spyware that is so inimical to human rights, and in some cases existing domestic law? Which companies are supplying potentially harmful products and services? Who are their clients? And what are the harms?

Unfortunately, the commercial spyware market is shrouded in secrecy. Many companies do not openly advertise their products or clients, choosing instead low-key approaches to selling that involve third-party resellers, closed trade shows, or informal networks of brokered contacts. The lack of transparency is compounded by the clients themselves, which are typically law enforcement, defense, and intelligence agencies, many of which operate in secrecy or are lacking in oversight and public accountability. What little we know about this industry has come from Citizen Lab case studies and reports, investigative reports undertaken by journalists and advocacy groups such as Privacy International, or leaks of company data, such as the July 2015 leak involving Hacking Team.

Notwithstanding the lack of transparency in this business, which certainly obstructs such inquiries, a record of practice has been uncovered so far that is still fairly detailed. This record raises issues well beyond company due diligence over end users and product sales. Questionable practices employed thus far by commercial spyware companies may be summarized within the following broad categories:

- Use of unfair or deceptive practices to create user confusion regarding the nature or presence of the company's software, in order to facilitate "social engineering" and induce and maintain a target's exposure.

- Use of legitimate third-party services through misrepresentation and/or in violation of relevant terms of service to build out spyware infrastructure.
- Actively undermining the security of consumer-facing digital platforms for private gain.

When presented with evidence of these practices, it is not uncommon to hear company representatives transfer the blame for any negative repercussions to their clients. While it is absolutely correct that comprehensive solutions to this problem will require states to curb their demand and address human rights abuses, it is equally true that *companies themselves have an independent obligation to respect human rights*.[2] It is disingenuous of the private actors involved in this market to assert that they have no role or responsibility in the impact of their products, or that human rights initiatives should focus exclusively on states. These products are, by design, intended to deceive individuals: infecting their personal devices, avoiding detection, and collecting and transmitting private data, all without the user's knowledge or informed consent. Such practices are, fundamentally, in violation of individuals' right to privacy under international law – which corporations have a duty to respect – and raise a host of other concerns under domestic legal frameworks. It is furthermore apparent that these products generate significant negative externalities, including the loss of consumer confidence in third-party goods and services targeted by exploits (e.g., Adobe PDF, JavaScript, Microsoft Word, etc.); and deterioration of the security of the web as a whole, as the advances pioneered by commercial spyware manufacturers, once released into the digital ecosystem, raise the bar on intrusion techniques and are eventually adopted by other malicious actors. Businesses making substantial profits on such a model cannot credibly assert that the negative externalities of their products are appropriately borne by others.

The final point in our checklist returns to suggestions on how to better identify commercial spyware manufacturers' practices of concern. As research into this trade continues, and legal or other challenges are mounted, we can expect that this early attempt at describing these practices of concern will be further refined.

☑ Define the goals of accountability measures.

It is important to outline our *goals* with respect to the commercial spyware market, in order to guide our efforts, establish a baseline for developing measures for accountability, and benchmark progress. Since concerns around abuse of commercial spyware are relatively new, these goals have not yet been fully and clearly articulated by advocacy groups and policymakers. Below, we highlight what we believe should be the principal goals. We encourage others to expand upon and refine them:

[2] As the UN Guiding Principles on Business and Human Rights make clear, business enterprises have the responsibility to respect internationally-recognized human rights, in their own activities as well as activities linked to their operations, products or services. See Section II, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, United Nations, 2011, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

- Reallocate the negative externalities associated with the commercial spyware market. Too often, the only price companies pay for misuse of their products is a public relations problem that can be managed or ignored. Our goal should be to shift costs from the public to the spyware companies themselves, in order to generate changes in company risk-opportunity calculations, practices, and overall attitude.

- Prevent sales of commercial spyware to agents of: any state engaged in systematic violence or repression in violation of international human rights law; any state demonstrated to have used commercial spyware against individuals or entities engaged in legitimate expression or activity protected under international human rights law; or any non-state actor.

- Develop greater transparency surrounding the market for commercial spyware, including supplier identities, product features, sales, trade shows, and deployment – the building blocks of accountability.

- Ensure civil society participation – including the human rights and security research communities – in dialogue and legislative processes regarding the commercial spyware market, which will contribute to effective solutions and a system of checks and balances.

- Ensure the public has access to effective remedies in the event of abuse, as well as protective measures to prevent digital compromise.

☑ Continue to adapt export controls, recognizing both the utility and limitations of this mechanism, as well as the need for additional regulatory measures.

The exploding demand for commercialized hacking services, combined with mounting evidence of abuse, has led to growing pressures for regulation and control. One of the first manifestations of these efforts came in the form of modifications made in 2013 to the Wassenaar Arrangement, a multilateral export control regime that covers dual-use technologies.[3] In response to several high-profile cases of abuse of mass surveillance and commercial spyware, the 41 country members of the Wassenaar Arrangement agreed to add clauses restricting items related to "IP network communications surveillance systems" and "intrusion software."[4] Member countries are committed to implement such controls at the national level once adopted within the Wassenaar framework.

---

[3] "The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies," http://www.wassenaar.org/.

[4] See Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List," December 8, 2016, http://www.wassenaar.org/wp-content/uploads/2016/12/WA-LIST-16-1-2016-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf (control list in effect as of March 2017).

How and why export controls became the venue for the first efforts to tackle regulation of commercial spyware likely have many causes, but among them may be a curious artefact of popular discourse. Following the first revelations of abuse against human rights activists by governments using commercial spyware, mainstream media and a handful of policymakers began to use the term “digital arms” and “digital weapons” to describe the wares of the commercial spyware industry. Of course, software cannot literally kill someone in the way bullets and missiles do (at least not yet). But the means by which agencies get inside a target’s computers can certainly contribute to physical retaliation against a target. And, the fact that military and intelligence agencies purchase spyware from the very same shadowy market inhabited by conventional arms dealers, made the analogy of “digital weapons” and “digital arms” intuitively attractive.

But language matters; it can shape reality and the horizon of possible options. Describing the commercial spyware market as one for “digital weapons” lends itself naturally to the idea of “arms control” for those who want to do something about it, and to a specific focus on “items.” And from there, it is but a short step to thinking in terms of the familiar forums where munitions, weapons, arms and other items of warfare have been traditionally regulated – to forums like the Wassenaar Arrangement.

Yet export controls, albeit essential, are by themselves insufficient to regulate the commercial spyware industry and prevent human rights abuses. Export 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. Indeed, Italian authorities initially approved a grant of a “global authorization” to Hacking Team, which permitted the company to export its spyware to destinations such as Kazakhstan;[5] and the Israeli authorities gave approval to NSO Group to export sophisticated iOS zero-day exploits to the United Arab Emirates, where they were subsequently used against a peaceful dissident and other political targets.[6] Moreover, export controls do not typically establish the level of public reporting on sales, products and services that society needs to understand the trade and hold it accountable. Additionally, as many critics have pointed out, export controls can have negative impacts on the provision of legitimate computer security business and research. Finally and perhaps most importantly, they subject regulatory efforts to the artificial constraint of designating an *item* for control, as opposed to focusing on the questionable *practices* of this industry.

[5] Lorenzo Franceschi-Bicchierai, “Hacking Team Has Lost Its License to Export Spyware,” Motherboard, April 6, 2016, http://motherboard.vice.com/read/hacking-team-has-lost-its-license-to-export-spyware.
[6] “Israeli government okayed sale of spyware that exploits iPhones,” Times of Israel, September 7, 2016, http://www.timesofisrael.com/israeli-government-okayed-sale-of-spyware-that-exploits-iphones/.

The heated debates that ensued surrounding the 2013 Wassenaar language demonstrate the perils of attempting to use export controls to regulate items offered by the commercial spyware industry. Designation of such items is a challenge, given the difficulty of specifying ever-developing technologies of concern and relevant exceptions in regulatory language. The Wassenaar language includes complex descriptions of "IP network communications surveillance systems" and items "specially designed or modified for the generation, operation or delivery of, or communication with, 'intrusion software.'" While countries of the European Union implemented those changes,[7] efforts to implement in the United States stalled after the Department of Commerce's Bureau of Industry and Security issued a controversial proposed rule in 2015.[8] The language of that proposed rule provoked serious backlash from the community of security professionals: many critics felt that beneficial security research would be inappropriately caught up by the export control regime, and that the license application process would delay exchange of time-sensitive, critical information concerning security vulnerabilities and digital threats (concerns also raised in the European context but which came to a head in the U.S. debates). This backlash, which included opposition not only from individual security researchers but also major information and communications technology (ICT) companies, such as Microsoft, prompted U.S. Congressional involvement that sent the proposed rule to the scrap heap, as well as demands that the U.S. State Department renegotiate the surveillance technology controls at the Wassenaar meeting held in December 2016.[9] At the same time, the conversation shifted away from the underlying human rights issues to an important but quite distinct discussion of the needs of the security industry. The human rights concerns that generated the Wassenaar additions in the first place, such as the use of spyware against regime critics, have yet to be credibly satisfied.

Going forward, export controls will require continued engagement and refinement. It remains to be seen how the Trump administration will address the aforementioned Wassenaar controls, which were left in place with only minor modifications following the December 2016 Wassenaar meeting. Meanwhile, the EU is debating a major proposal[10] to modernize its export control

---

[7] See Commission Delegated Regulation (EU) No. 2016/1969, 12 September 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R1969&from=EN (EU control list in force as of March 2017). See also European Commission, "Trade: Dual-use export controls," http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/.

[8] Proposed Rule: Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. 97, *Federal Register: The Daily Journal of the United States*, May 20, 2015, https://www.federalregister.gov/documents/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

[9] See Wassenaar: Cybersecurity and Export Control, Hearing before the Subcommittee on Information Technology, House, January 12, 2016, https://oversight.house.gov/hearing/wassenaar-cybersecurity-and-export-control/.

[10] See European Commission, Proposal for a Regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast), COM(2016) 616, September 28, 2016, http://eur-lex.europa.eu/resource.html?uri=cellar:1b8f930e-8648-11e6-b076-01aa75ed71a1.0013.02/DOC_1&format=PDF, and Annexes 1 to 6, http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154977.pdf; see also European

system; that proposal includes a specific focus on “cyber-surveillance technology,” greater emphasis on human rights, and recognition that controls should not undermine Internet security research. But beginning the process of attempted regulation of spyware within the rigid framework of export controls may have inadvertently tainted our mindset on how to tackle the problem: it has focused debate on the Sisyphean task of delineating items of concern. We need to think broader than just items, to how to control the *behavior* of private actors in this industry with more flexible regulatory measures and incentive structures.

In actuality, the need for intervention in the spyware trade extends well beyond the point of sale: it has much less to do with a static item than with the opaque practices of private actors that seek to insert themselves in government surveillance and espionage operations, developing and servicing technological solutions tailored to that purpose. To address such practices, and in tandem with export control efforts, the following tactics merit further consideration.

☑ Engage in criminal or civil litigation against threat actors that use spyware against civil society, and any vendors that are complicit in such acts, to the extent permissible under relevant law.

Litigation on the basis of existing criminal and civil law is an underexplored but potentially critical option available to targeted individuals and groups in seeking remedy. It may be utilized either by governments via criminal prosecution, or by victims of spyware, against entities that have engaged in digital intrusion and espionage without appropriate legal basis, and, in some circumstances, against the private sector actors that supported such activity. Litigation is not without its challenges: it involves complex evidence-gathering, procedural hurdles, and significant resources required to sustain a typical multi-year lawsuit. Yet the prospect of exposure to criminal penalties or civil damages is a potent deterrent. It forces the relevant actors to consider the propriety, legality, and costs of their behavior, rather than continue generating negative externalities unchecked.

We recognize that the cross-border nature of the spyware trade has created numerous legal and regulatory gaps and complexities, and that any discussion of legal remedy will require detailed analysis of the laws of the relevant jurisdiction(s). In this brief, we highlight relevant U.S. legal principles as a jumping-off point for discussion, with the goal of identifying key areas of inquiry. We emphasize that it is uncertain how courts will apply existing law to spyware-related claims, given the relative lack of precedent and novelty of known and attributable use of commercial spyware against users, as well as the frequent involvement of sovereigns. However,

---

Commission, “Trade: Dual-use export controls,” http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/; European Commission, “Trade: Export Control Forum 2016 - report and documents,” December 12, 2016, http://trade.ec.europa.eu/doclib/events/index.cfm?id=1562; Lucie Krahulcova, “EU wants to limit export of surveillance technologies without hurting security research,” Access Now, December 12, 2016, https://www.accessnow.org/eu-wants-limit-export-surveillance-technologies-without-hurting-security-research/.

such approaches merit additional exploration as potential constraints on the market for commercial spyware. They should be supported through legislation designed to facilitate access to remedy and clearly establish jurisdiction.

Criminal prosecution

The Budapest Convention on Cybercrime (2001) – ratified by much of Europe, the United States, and as of 2015, Canada[11] – requires that parties adopt, *inter alia*, measures to criminalize intentional "access to the whole or any part of a computer system without right"[12] and "interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system."[13] National computer crime laws of this sort are commonplace. In the United States, key laws include the Computer Fraud and Abuse Act (CFAA)[14] and the Electronic Communications Privacy Act (ECPA).[15] These laws are not without controversy, given the CFAA's history of application to researchers engaged in the study of vulnerabilities or security practices that impact public platforms,[16] and the ECPA's outdated parameters for law enforcement access to user data.[17] They do, however, provide a basis on which to challenge digital intrusion activities of politically-motivated and state-linked actors. Likewise, criminal laws typically account for conspiracy and complicity – plotting to commit, or aiding and abetting the commission of crimes (also reflected in the Budapest Convention[18]) – concepts that may implicate the highly customized services of commercial spyware companies. For example, the CFAA includes as a punishable offense conspiracy to commit any of the actions prohibited under the statute.[19] This provision may reach not only the actors utilizing the spyware, but also the commercial spyware companies that assist their clients in crafting,

[11] Council of Europe, "Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime," http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.
[12] Council of Europe, *Convention on Cybercrime*, November 23, 2001, Art. 2, available at http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.
[13] Ibid. at Art. 3.
[14] 18 U.S.C. § 1030, https://www.law.cornell.edu/uscode/text/18/1030.
[15] The ECPA consists of the Wiretap Act, 18 U.S.C. § 2510 et seq., https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119; the Stored Communications Act, 18 U.S.C. § 2701 et seq., https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121; and the Pen-Register Act, 18 U.S.C. § 3121 et seq., https://www.law.cornell.edu/uscode/text/18/part-II/chapter-206.
[16] See EFF, "Computer Fraud And Abuse Act Reform," https://www.eff.org/issues/cfaa; American Civil Liberties Union, "Sandvig v. Lynch — Challenge to CFAA Prohibition on Uncovering Racial Discrimination Online," June 29, 2016, https://www.aclu.org/cases/sandvig-v-lynch-challenge-cfaa-prohibition-uncovering-racial-discrimination-online.
[17] See Electronic Privacy Information Center, "Electronic Communications Privacy Act (ECPA): Reform Proposals," https://epic.org/privacy/ecpa/.
[18] *Convention on Cybercrime*, Art. 11. In the U.S., 18 U.S.C. § 2(a) provides, "Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal." 18 U.S.C. § 2(a), https://www.law.cornell.edu/uscode/text/18/2.
[19] 18 U.S.C. § 1030(b), https://www.law.cornell.edu/uscode/text/18/1030.

facilitating, or "troubleshooting" targeted digital attacks.[20] We know from prior research and reporting that such support has brought companies into possession of significant details regarding a planned intrusion, or involved their active cooperation in an attack.[21]

In the U.S., prosecutorial powers have been deployed to counter industrial espionage and attacks on critical infrastructure carried out through digital means by state-linked actors.[22] Those powers are buttressed by the availability of sanctions against "persons engaging in significant malicious cyber-enabled activities."[23] Lacking, however, are coordinated campaigns against malicious actors specifically targeting civil society. Indeed, the frequent extraterritorial application of spyware technology against diaspora groups and other "hostile" civil society actors beyond the physical reach of a state – some of which even incorporates ICT infrastructure in the jurisdiction of the target[24] – raises serious questions about the resolve of governments to protect citizens from foreign espionage and information operations, and what sovereignty means in such a context. These concerns were only amplified by the brazen hacking of the Democratic National Committee and Clinton campaign chairman John Podesta in 2016, attributed to the Russian government. Invoking computer crime laws more frequently on behalf of civil society, rather than against it, would go far in improving digital security for the public. Taking a stand against the use of advanced commercial spyware against civil society actors through criminal prosecution would send an important message on this front.

Additionally, the repercussions under the U.S. Wiretap Act for manufacturers of spyware used in cross-border digital espionage require further assessment and engagement by the Federal Bureau of Investigation and Department of Justice (DoJ). Importantly, section 2512 imposes criminal penalties upon "any person who intentionally . . . *manufactures, assembles,* possesses, *or sells* any electronic, mechanical, or other device, *knowing or having reason to know* that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and *that such device or any component thereof has*

---

[20] See *Welenco, Inc. v. Corbell*, 2015 U.S. Dist. LEXIS 112971 (E.D. Cal. Aug. 25, 2015) ("A claim under section [1030](b) requires evidence of an agreement and common activities in furtherance of the unlawful act."); see also *Advanced Fluid Systems, Inc. v. Huber*, 28 F.Supp.3d 306 (M.D. Pa. June 18, 2014); *NetApp, Inc., v. Nimble Storage, Inc.*, 41 F.Supp.3d 816 (N.D. Cal. May 12, 2014); *Enargy Power Co. Ltd. v. Xiaolong Wang*, 2013 WL 6234625 (D. Mass. Dec. 3, 2013).

[21] See, e.g., Bill Marczak and Sarah McKune, "What we know about the South Korea NIS's use of Hacking Team's RCS," Citizen Lab, August 9, 2015, https://citizenlab.org/2015/08/what-we-know-about-the-south-korea-niss-use-of-hacking-teams-rcs/; Lorenzo Franceschi-Bicchierai, "Hacking Team's 'Illegal' Latin American Empire," Motherboard, April 18, 2016, https://motherboard.vice.com/en_us/article/hacking-team-illegal-latin-american-empire.

[22] See the indictment issued against China-based actors, *U.S. v. Wang Dong et al.*, Criminal No. 14-118 (W.D. Pa. May 1, 2014), https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf, and that issued against Iran-based actors, *U.S. v. Fathi et al.*, No. 16 Crim. 48 (S.D.N.Y.), https://www.justice.gov/usao-sdny/file/835061/download.

[23] See U.S. Department of the Treasury, "Sanctions Related to Significant Malicious Cyber-Enabled Activities," https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx.

[24] https://citizenlab.org/2014/02/hacking-teams-us-nexus/

been or will be sent through the mail or *transported in interstate or foreign commerce*."[25] In a 2014 case, the DoJ used this statute to convict a Danish citizen located in Pakistan for the sale and advertising of a mobile spyware application known as "Stealthgenie," which was marketed primarily to individuals seeking to spy on their romantic partners. The DoJ asserted jurisdiction on the basis of the defendant's use of computer servers located in Virginia.[26] The defendant pled guilty and was ordered to pay a U.S. $500,000 fine, marking "the first-ever criminal conviction concerning the advertisement and sale of a mobile device spyware app"[27] and thus establishing precedent for spyware company liability.

To be sure, a safe harbor provision exists in this section of the Wiretap Act that would preclude its application to commercial spyware manufacturers supplying U.S. law enforcement. Section 2512 does not apply to "an officer, agent, or employee of, or *a person under contract with, the United States, a State, or a political subdivision thereof*, in the normal course of the activities of the United States, a State, or a political subdivision thereof."[28] However, this safe harbor makes no reference to *foreign* government entities, which may deploy commercial spyware against targets in the U.S. or by utilizing U.S. infrastructure – raising what appears to be a novel issue under U.S. law.[29] Additionally, it is noteworthy that the statute refers not only to devices but also to "any component thereof": such language is broad enough to encompass not only operator software provided directly to clients, but also components of the software surreptitiously installed on target machines, or elements of the command-and-control infrastructure, such as proxy chains. Thus, if a commercial spyware manufacturer under contract with a foreign government entity has any reason to know that its client is conducting activity in the U.S.,[30] or if the manufacturer has itself incorporated U.S. infrastructure in the design of the spyware (as, for

---

[25] 18 U.S.C. § 2512(1)(b) (emphasis added).

[26] See U.S. Department of Justice, "Man Pleads Guilty for Selling 'StealthGenie' Spyware App and Ordered to Pay $500,000 Fine," November 25, 2014, https://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine; *U.S. v. Akbar*, Civil No. 1:14-cv-1273 (E.D. Va. September 26, 2014), available at https://cdn.arstechnica.net/wp-content/uploads/2014/09/akbar.pdf; *U.S. v. Akbar*, Criminal No. 1:14-cr-276 (E.D. Va. August 7, 2014), available at http://www.wired.com/wp-content/uploads/2014/09/Akbar_indictment.pdf.

[27] U.S. Department of Justice, "Man Pleads Guilty for Selling 'StealthGenie' Spyware App and Ordered to Pay $500,000 Fine," November 25, 2014, https://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine.

[28] 18 U.S.C. § 2512(2)(b) (emphasis added).

[29] The Wiretap Act "is designed to prohibit 'all wiretapping and electronic surveillance by persons other than *duly authorized* law enforcement officials engaged in investigation of specified types of major crimes.'" *Greenfield v. Kootenai County*, 752 F.2d 1387, 1388 (9th Cir. 1985) (quoting S. Rep. No. 1097, 90th Cong., 2d Sess.) (emphasis added). It is possible that courts might consider a foreign agency conducting a legitimate investigation in coordination with U.S. law enforcement as within the ambit of this safe harbor. But it appears contrary to the intent of the statute to turn a blind eye to support of unannounced digital intrusions by foreign government actors – particularly those targeting individuals for political reasons.

[30] The legislative history of the ECPA confirms that Congress intended the Act to apply to "'interceptions' conducted within the territorial United States" (Wiretap Act) or "access within the territorial United States" (Stored Communications Act). H.R. Rep. No. 99-647, 99th Cong., 2d Sess. (June 19, 1986), at 32-33.

example, Hacking Team did[31]), it may run afoul of section 2512.[32] U.S. courts have also held that suppliers cannot shield themselves from liability under section 2512 by simply relying on disclaimers or references to the need to abide by applicable laws,[33] or asserting they did not know their products were illegal or to be used unlawfully.[34] The utility of this section of the Wiretap Act in challenging digital intrusions against civil society, however, can only be proven if U.S. government agencies choose to pursue known incidents.[35]

Laws regarding "refugee espionage," a concept originating among the Nordic countries, may also be relevant to curbing spyware abuses.[36] Countries such as Norway and Sweden have criminalized the unauthorized collection of "information that can be used to exert pressure on the refugee or relatives of the refugee, for the purpose of threat or persecution."[37] Given the demonstrated and repeated use of commercial spyware against diaspora communities[38] to extend the reach of repressive regimes extraterritorially, governments should consider adopting or enhancing legislation regarding refugee espionage, and further explore the role played by spyware in such espionage.

Civil litigation

---

[31] See Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, John Scott-Railton, and Sarah McKune, "Hacking Team's US Nexus," Citizen Lab, February 28, 2014, https://citizenlab.org/2014/02/hacking-teams-us-nexus/.

[32] Interestingly, Hacking Team appears to have contemplated this scenario.

[33] *U.S. v. Wynn*, 633 F. Supp. 595 (C.D. Illinois, April 23, 1986) (A defendant "cannot avoid conviction under Section 2512 simply by surrounding himself with disclaimers and closing his eyes to the nature and use of the devices."); see also *U.S. v. Biro*, 143 F.3d 1421 (11th Cir. June 17, 1998).

[34] *U.S. v. Spy Factory Inc.*, 960 F. Supp. 684 (S.D.N.Y. 1997) ("[T]he Government need not show that the defendants knew the devices were illegal, but rather that defendants intentionally possessed and sold items whose design they knew or had reason to know rendered them primarily useful for surreptitious interceptions. . . . Thus, counsel's argument that 'there was nothing and no one to alert [defendant Ford] that a claimed portion of his employer's product line had allegedly strayed beyond the permissible bounds because the products in question were capable of being employed by customers not under his control or in his presence, for non-consensual purposes,' . . . has no legal significance."); *U.S. v. Christensen*, 801 F.3d 970 (9th Cir. Aug. 25, 2015) ("The crime lies in intentionally manufacturing the device, knowing that it could be primarily used for wiretapping. The statute does not require intent or knowledge that the device would actually be used unlawfully.").

[35] Notably, while courts have generally construed 18 USC 2512 as providing for criminal penalties, and restricted pursuit of civil claims under 18 USC 2520 to violations of 18 USC 2511, in 2016 the Sixth Circuit recognized the potential for civil claims for violation of 2512 under certain circumstances. See infra n. 42.

[36] See UN High Commissioner for Refugees (UNHCR), *Comments by the United Nations High Commissioner for Refugees (UNHCR) on the Memorandum of 6 December 2013, proposing Criminalization of Refugee Espionage*, February 2014, available at: http://www.refworld.org/docid/5829ad6c4.html.

[37] Ibid.; see also "Man arrested for 'refugee espionage' in Sweden," *The Local Sweden*, February 27, 2017, http://www.thelocal.se/20170227/man-arrested-for-refugee-espionage-in-sweden (reporting arrest of a man "believed to have illegally obtained intelligence about people related to Tibet in Sweden on behalf of another country," on charges of refugee espionage).

[38] See Citizen Lab, *Communities @ Risk: Targeted Digital Threats Against Civil Society*, November 11, 2014, at 26, https://targetedthreats.net/media/1-ExecutiveSummary.pdf.

It is likewise imperative that the individuals and groups directly affected by commercial spyware are able to raise civil claims themselves, in order to seek remedy and deter malicious digital targeting. Some computer crime statutes include avenues for civil remedy, making them available for exercise not only by government prosecutors but also by victims of spyware. Under U.S. federal law, the CFAA,[39] the Stored Communications Act,[40] and the Wiretap Act[41] each permit civil actions for damages suffered as a result of certain digital intrusion activities involving, respectively, unauthorized access to computers or stored electronic communications, or interception of electronic communications.[42] Tort law establishing a cause of action for

[39] 18 U.S.C. § 1030(g), https://www.law.cornell.edu/uscode/text/18/1030. Notably, the CFAA has extraterritorial reach: courts have applied the statute to conduct originating from the U.S. that affects computers outside the U.S., as well as conduct that originates overseas but affects computers within the U.S. See *Enargy Power Co. Ltd. v. Xiaolong Wang*, 2013 WL 6234625 (D. Mass. Dec. 3, 2013); *Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A.*, 267 F.Supp.2d 1268, 1322 (S.D. Fla. 2003), aff'd in part, rev'd in part sub nom. *Four Seasons Hotels v. Consorcio Barr S.A.*, 138 Fed. App'x 297 (11th Cir. 2005); *United States v. Ivanov*, 175 F.Supp.2d 367, 370–71 (D. Conn. 2001).

[40] 18 U.S.C. § 2707, https://www.law.cornell.edu/uscode/text/18/2707.

[41] 18 U.S.C. § 2520, https://www.law.cornell.edu/uscode/text/18/2520.

[42] Civil claims under these statutes would typically proceed against a primary violator, rather than against a supplier/manufacturer on the basis of secondary liability (e.g., for aiding and abetting). Under certain circumstances, however, a claim may also exist against the underlying manufacturer.

Federal courts have generally held that the ECPA (of which the Wiretap Act and Stored Communications Act are part) does not provide a civil cause of action for secondary liability. See, e.g., *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1089-90 (N.D. Cal. 2015). However, the Sixth Circuit has recently distinguished that a spyware manufacturer that supplied an individual alleged to have intercepted a communication in violation of the Wiretap Act, may itself be directly liable under section 2511, if it acquired the communication contemporaneously with its transmission. Such contemporaneous acquisition may take place when the spyware enables real-time monitoring that is transferred through the spyware manufacturer's servers. *Luis v. Zang*, 833 F.3d 619, 631-33 (6th Cir. 2016). "Put differently, the complaint's focus on Awareness's continued operation of the WebWatcher program— even after that program is sold to a user— convinces us that Luis has plausibly pleaded that Awareness intercepted his communications." Ibid. at 633. The court additionally found that the marketing materials associated with the spyware were sufficient to support a reasonable inference that the manufacturer intercepted the communications through such transfer. Ibid. at 631. Finally and importantly, the court went further to hold that a spyware manufacturer may also be civilly liable for violations of section 2512 of the Wiretap Act: "a defendant such as Awareness— which allegedly violates § 2512(1)(b) by manufacturing, marketing, and selling a violative device— is subject to a private suit under § 2520 only when that defendant also plays an active role in the use of the relevant device to intercept, disclose, or intentionally use a plaintiff's electronic communications." Ibid. at 637. According to the court, when a claim "is not limited to 'the mere selling' of the device at issue," but rather, asserts that the spyware company "manufactured, marketed, sold, and *actively operated* the violative device, all while *knowing* that its device was to be used primarily for the surreptitious interception of electronic communications," the company is "far more culpable," such that its actions give rise to a civil claim under section 2520 for having "engaged in" a violation of section 2512. Ibid. at 639.

Separately, with respect to the CFAA, civil claims may proceed against co-conspirators for violation of 18 U.S.C. § 1030(b), when evidence exists of "an agreement and common activities in furtherance of the unlawful act." *Welenco, Inc. v. Corbell*, 126 F.Supp.3d 1154, 1176 (E.D. Cal. 2015); see also *Trademotion, LLC v. Marketcliq, Inc.*, 857 F.Supp.2d 1285, 1294 (M.D. Fla. 2012). Federal courts have held, however, that the CFAA "does not create a cause of action for aiding and abetting." *Advanced Fluid Sys., Inc. v. Huber*, 28 F.Supp.3d 306, 328 (M.D. Penn. 2014); see also *Flynn v. Liner Grode Stein Yankelevitz Sunshine Regenstreif & Taylor LLP*, 2011 WL 2847712 (D. Nev. 2011).

invasion of privacy[43] is another area to consider, though it varies among legal systems. One form of invasion of the right to privacy recognized in the U.S. is "unreasonable intrusion upon the seclusion of another,"[44] which comprises "an intentional interference with [the claimant's] interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man."[45] U.S. state laws provide for intrusion upon seclusion claims, which have been successfully invoked in cases concerning electronic surveillance.[46] (Canadian courts have also recognized a cause of action for intrusion upon seclusion.[47]) State law regarding spyware[48] and digital trespass[49] may provide additional bases for legal claims.

The first case brought by a private citizen in U.S. federal court alleging misuse of advanced commercial spyware by a government, *Doe v. Federal Democratic Republic of Ethiopia*, is illustrative of the potential and pitfalls of challenging digital surveillance through civil litigation. In this case, filed in 2014 in the U.S. District Court for the District of Columbia and supported by the Electronic Frontier Foundation, pseudonymous plaintiff Kidane sued the Federal Democratic Republic of Ethiopia on the basis of its alleged use of FinFisher spyware to surveil his communications, asserting claims under the Wiretap Act and state law regarding invasion of privacy.[50] The court dismissed the case in May 2016, for reasons stemming from the naming of

---

[43] According to the Restatement (Second) of Torts, which reflects existing U.S. law on the question, "One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other." Restatement (Second) of Torts § 652A (1977).

[44] Restatement (Second) of Torts § 652A (1977).

[45] Restatement (Second) of Torts § 652B (1977). Comment (b) makes clear that the tort of intrusion upon seclusion does not require a showing that information obtained through the intrusion was utilized, and that the tort would be applicable to electronic surveillance: "The invasion may be . . . . by the use of the defendant's senses, *with or without mechanical aid*s, to oversee or overhear the plaintiff's private affairs . . . . . It may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail . . . . The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined."

[46] See, e.g., *Lazette v. Kulmatycki*, 949 F.Supp.2d 748 (N.D. Ohio June 5, 2013); *Koeppel v. Speirs*, 808 N.W.2d 177 (Iowa Dec. 23, 2011) ("An electronic invasion occurs under the intrusion on solitude or seclusion component of the tort of invasion of privacy when the plaintiff establishes by a preponderance of evidence that the electronic device or equipment used by a defendant could have invaded privacy in some way."); *Amati v. City of Woodstock, Illinois*, 829 F. Supp. 998 (N.D. Illinois August 10, 1993); *Nader v. General Motors Corp.*, 307 N.Y.S.2d 647 (N.Y. Jan. 8, 1970).

[47] See *Evans v. The Bank of Nova Scotia*, 2014 ONSC 2135, http://www.canlii.org/en/on/onsc/doc/2014/2014onsc2135/2014onsc2135.html; *Jones v. Tsige*, 2012 ONCA 32, http://www.canlii.org/en/on/onca/doc/2012/2012onca32/2012onca32.html.

[48] See National Conference of State Legislatures, "State Spyware Laws," January 25, 2017, http://www.ncsl.org/research/telecommunications-and-information-technology/state-spyware-laws.aspx.

[49] See generally Richard G. Kunkel, "Protecting Consumers from Spyware: A Proposed Consumer Digital Trespass Act," 28 J. Marshall J. Computer & Info. L. 185 (2010).

[50] For an analysis of the Kidane claims and the potential liability of sovereigns for cross-border hacking, including the viability of such claims under the Foreign Sovereign Immunities Act, see Stephen J. Schultze, "Hacking Immunity: Computer Attacks on U.S. Territory by Foreign Sovereigns," 53 Am. Crim. L. Rev. 861 (2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784591.

a state sovereign as the defendant,[51] and the plaintiff appealed. Oral argument in the appeal was heard on February 2, 2017.[52]

While it is uncertain whether the lower court's ruling will stand on appeal, the *Doe v. Ethiopia* ruling is based on two critical holdings that have the potential to impact future spyware cases. First, the court held that a plaintiff may not bring a private cause of action under section 2520 of the Wiretap Act against a *foreign state* for violation of section 2511(a) of the statute, as that section prohibits "any *person*" (emphasis added) from intentionally intercepting electronic communications without lawful authorization – language the court construed as not including government entities. And second, the court held that the Foreign Sovereign Immunities Act (FSIA) bars tort claims involving a foreign state's cross-border use of spyware, on the grounds that the digital tort did not occur entirely within the territory of the United States, as required to proceed under the FSIA non-commercial tort exception.[53] Each of these conclusions is arguable, as detailed in the appellate briefs.[54] Deeper analysis suggests that the court's interpretation of the definition and use of "person" in the Wiretap Act is inappropriately restrictive, and in its most recent iteration the legislature understood the relevant provisions of the Wiretap Act to apply to governmental entities including foreign states. On the second issue of location of the tort, public policy considerations weigh heavily in favor of interpreting the FSIA non-commercial tort exception to include torts accomplished via digital activity on U.S.-based systems, which will be an increasingly common form of tort in the future and should be discouraged through legal repercussions with teeth.[55]

---

[51] See *Doe v. Federal Democratic Republic of Ethiopia*, Civil Action No. 14-372, Memorandum Opinion and Order (D.D.C. 2016), available at https://www.eff.org/document/memorandum-opinion-and-order. While naming a sovereign entity as defendant may raise legal hurdles under the FSIA, and the Wiretap Act per *Doe*, victims may choose to also name as defendants individual foreign officials involved in the use of spyware against them. The *Doe* court noted that "even though the relevant provision of the Wiretap Act does not apply to foreign states . . . it does apply to the actions of 'individuals,' and would arguably apply to actions committed by those employed by foreign states." *Doe*, at 36. It is of course difficult in many cases to attribute a digital attack to a particular government, let alone the individuals involved in perpetrating that attack (though the U.S. government has named individuals in its China and Iran indictments, based on the intelligence available to it). But to the extent that the individuals involved are unknown, victims may consider naming, in addition to the government entity, the head of the government agency involved as well as fictitious "Doe" defendants, the identities of which may be specified following discovery. See generally Howard M. Wasserman, *Civil Rights Plaintiffs and John Doe Defendants: A Study in § 1983 Procedure*, 25 Cardozo L. Rev. 793 (2003), available at http://ecollections.law.fiu.edu/faculty_publications/72.

[52] Nate Cardozo, "Can Foreign Governments Launch Malware Attacks on Americans Without Consequences?," EFF, February 2, 2017, https://www.eff.org/deeplinks/2017/02/can-foreign-governments-launch-malware-attacks-americans-without-consequences

[53] 28 U.S.C. § 1605(a)(5), https://www.law.cornell.edu/uscode/text/28/1605.

[54] Available at EFF, "Kidane v. Ethiopia," https://www.eff.org/cases/kidane-v-ethiopia.

[55] For further analysis see Alexis Haller, "The Cyberattack Exception to the Foreign Sovereign Immunities Act: A Proposal to Strip Sovereign Immunity When Foreign States Conduct Cyberattacks Against Individuals and Entities in the United States," FSIA Law, February 19, 2017, https://fsialaw.com/2017/02/19/the-cyberattack-exception-to-the-foreign-sovereign-immunities-act-a-proposal-to-strip-sovereign-immunity-when-foreign-states-engage-in-cyberattacks-against-individuals-and-entities-in-the-united-stat/; Stephen J. Schultze, "Hacking Immunity: Computer Attacks on U.S. Territory by Foreign Sovereigns," 53 Am. Crim. L. Rev. 861 (2016), available at

☑ Invoke consumer protection laws to address the unfair or deceptive practices inherent to commercial spyware.

Consumer protection laws and implementing agencies may in various jurisdictions address practices at the core of the commercial spyware trade. The manufacture, service, and use of spyware presents unique complications under the law because spyware is inherently consumer-facing: it undermines users' reasonable expectations of a properly mediated digital exchange, eroding their trust in software and services as well as their safety and privacy online. Unfair and deceptive practices are the modus operandi upon which commercial spyware is built, as spyware is designed to intentionally mislead users regarding the nature of the software or online platforms with which they engage, in order to surreptitiously compromise their devices. We are only beginning to appreciate the serious impact of the spread of spyware on the marketplace and society at large, including loss of consumer confidence and other chilling effects,[56] as well as the shaping of significant product design and resource allocation decisions of major ICT companies.

In the United States, state consumer protection laws have provided a basis for consumer claims regarding software that surreptitiously intercepts sensitive user data.[57] Moreover, at the federal level, the Federal Trade Commission (FTC) Act declares unlawful any "unfair or deceptive acts or practices in or affecting commerce."[58] Consumers may take action directly under state law, or submit spyware-related complaints to the FTC to pursue.[59]

Could the FTC play a more active role in aggressively tackling the commercial spyware trade on behalf of users? The FTC Act provides that the FTC is "empowered and directed to prevent persons, partnerships, or corporations . . . from using . . . unfair or deceptive acts or practices in or affecting commerce."[60] The history of the FTC's engagement on spyware suggests that it is

---

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784591; Scott A. Gilmore, "Suing the Surveillance States: The (Cyber) Tort Exception to the Foreign Sovereign Immunities Act," 46 Colum. Hum. Rts. L. Rev. 227 (2015), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2622184.

[56] See, e.g., Sophos, "Sophos Survey Reveals Consumers Are More Worried About Cybercrime Than Physical World Crime, Yet Awareness Of Phishing Scams And Ransomware Remains Low," December 14, 2016, https://www.sophos.com/en-us/press-office/press-releases/2016/12/consumer-ransomware.aspx.

[57] See, e.g., *In re Carrier IQ, Inc.*, 78 F.Supp.3d 1051 (N.D. Cal. Jan. 21, 2015) (discussing claims under the laws of California, Connecticut, Florida, Maryland, Michigan, Texas, and Washington).

[58] 15 U.S.C. § 45(a)(1), https://www.law.cornell.edu/uscode/text/15/45.

[59] See U.S. Federal Trade Commission (FTC), "Submit a Consumer Complaint to the FTC," https://www.ftc.gov/faq/consumer-protection/submit-consumer-complaint-ftc.

[60] 15 U.S.C. § 45(a)(2), https://www.law.cornell.edu/uscode/text/15/45. The FTC holds a number of powers that could be used to curtail inappropriate practices within the commercial spyware trade. These include: investigatory powers, including issuance of compulsory reporting demands (15 U.S.C. § 46, https://www.law.cornell.edu/uscode/text/15/46); the ability to bring administrative proceedings culminating in cease and desist orders (15 U.S.C. § 45(b), https://www.law.cornell.edu/uscode/text/15/45), civil actions (15 U.S.C. § 57b, https://www.law.cornell.edu/uscode/text/15/57b), and to refer potential

primed for such a role. For example, in 2006 the U.S. Safe Web Act was passed specifically to address "Internet scams" (spam, spyware and fraud) in a cross-border context[61] – the same context that has made spyware regulation and response so difficult on other fronts. Notably, the US Safe Web Act amended the FTC Act to include within the definition of "unfair or deceptive acts or practices" those "acts or practices involving foreign commerce that– (i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States"; and to provide for "restitution to domestic or foreign victims."[62] All of these aspects are promising.

Proactive engagement by the FTC on spyware is particularly important given the concerns raised, and representations made by the Commission, during debates over spyware in the 2000s.[63] While the products and practices of concern around that time[64] were not of the same caliber as commercial spyware currently sold to governments, the debates reflected the ever-expanding problems associated with digital intrusion, their effect on consumers, and questions regarding potential legislative and other solutions. Many states were enacting their own anti-spyware statutes, and there were discussions of the appropriate role of federal legislation on the issue.[65] In lieu of the federal government enacting spyware-specific legislation, however, the FTC assumed the role of spyware watchdog, asserting its powers were sufficient to tackle the problem.[66] Despite these early pronouncements, the FTC has thus far taken only limited action

---

violations of federal criminal law to the Attorney General for criminal proceedings (15 U.S.C. § 46(k), https://www.law.cornell.edu/uscode/text/15/46); and the ability to issue "interpretive rules and general statements of policy" concerning particular practices (15 U.S.C. § 57a, https://www.law.cornell.edu/uscode/text/15/57a), through which the FTC could put spyware companies on notice that certain activities are in violation of the law.

[61] FTC, "Summary of the US SAFE WEB Act," https://www.ftc.gov/sites/default/files/documents/reports/us-safe-web-act-protecting-consumers-spam-spyware-and-fraud-legislative-recommendation-congress/summary-us-safe-web-act.pdf; see also FTC, *The US SAFE WEB Act: Protecting Consumers from Spam, Spyware, and Fraud: A Legislative Recommendation to Congress*, June 2005, https://www.ftc.gov/sites/default/files/documents/reports/us-safe-web-act-protecting-consumers-spam-spyware-and-fraud-legislative-recommendation-congress/ussafeweb.pdf.

[62] 15 U.S.C. § 45(a)(4).

[63] See FTC, *Spyware Workshop: Monitoring Software on Your PC: Spyware, Adware, and Other Software*, Staff Report, March 2005, https://www.ftc.gov/sites/default/files/documents/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-and-other-software-report/050307spywarerpt.pdf.

[64] See Consumer Software Working Group, "Examples of Unfair, Deceptive or Devious Practices Involving Software: Version 1.0," https://www.cdt.org/files/privacy/spyware/20040419cswg.pdf.

[65] See, e.g., Center for Democracy & Technology, "Ghosts in Our Machines: Background and Policy Proposals on the 'Spyware' Problem," November 2003, https://www.cdt.org/files/privacy/031100spyware.pdf; Fred Von Lohmann, "H.R. 964: Another Misguided Spyware Bill," EFF, April 26, 2007, https://www.eff.org/deeplinks/2007/04/h-r-964-another-misguided-spyware-bill.

[66] See FTC, *Spyware Workshop: Monitoring Software on Your PC: Spyware, Adware, and Other Software*, Staff Report, March 2005, at 20, https://www.ftc.gov/sites/default/files/documents/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-and-other-software-report/050307spywarerpt.pdf; Roy Mark, "FTC to

concerning spyware,[67] and has not addressed the serious problems presented by vulnerability exploits that could affect hundreds of millions of consumer devices (e.g., the NSO Group exploits targeting Apple's iOS). It is apparent that the FTC (in concert with other elements of the U.S. government such as Congress[68]) must take more initiative to truly demand accountability from advanced commercial spyware companies, which in turn will require more resources. Importantly, the FTC's recently-established Office of Technology Research and Investigation has indicated its interest[69] in privacy and security research, including issues related to vulnerabilities and the Internet of Things; further engagement with the FTC by civil society regarding commercial spyware and digital vulnerabilities will be essential.

☑ Challenge the contract violations and intellectual property infringements engaged in by commercial spyware companies.

It is common practice for spyware developers to design their products to spoof legitimate programs and platforms, or intercept, inject, or otherwise compromise legitimate web traffic, in order to surreptitiously deliver malware, preying on user trust in third parties. They may also rely on unsuspecting third parties in building out their own infrastructure, such as certificate authorities or hosting companies used to complete a proxy chain that hides the true location of clients' command-and-control servers,[70] thus coopting such companies into the service of digital espionage. Such practices may be in contravention of relevant contractual agreements or terms of service, which often include provisions prohibiting activity that violates applicable laws or constitutes misuse. ICT companies whose products and services are spoofed or undermined,

---

Congress: Lose the Anti-Spyware Plans," Internet News, November 5, 2004, http://www.internetnews.com/xSP/article.php/3432111.

[67] See FTC, "Spyware and Malware," https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/spyware-and-malware; Julie Brill, "The Federal Trade Commission and the Future of Privacy and Data Security," Keynote Remarks at the Berkeley Center for Law & Technology, University of California, Berkeley, September 15, 2015, at 2, https://www.ftc.gov/system/files/documents/public_statements/804391/150924berkeleybcltremarks_.pdf (describing the FTC's progress in enforcement actions to protect consumers from "deceptive and unfair data practices"); see also FTC, *The U.S. SAFE WEB Act: The First Three Years: A Report to Congress*, December 2009, https://www.ftc.gov/sites/default/files/documents/reports/u.s.safe-web-act-first-three-years-federal-trade-commission-report-congress/p035303safewebact2009.pdf (Appendix B of the document lists "FTC Enforcement Actions With Public Cross-Border Components" filed between January 2007 and October 2009. Only one of the enforcement actions, *FTC v. CyberSpy Software, LLC*, concerns spyware. Notably, this is the same case cited *six years later* by former Commissioner Brill as the example of FTC action against spyware, in her 2015 speech cited above.).

[68] An FTC investigation can be initiated upon concurrent resolution of both houses of Congress. 15 U.S.C. § 46a, https://www.law.cornell.edu/uscode/text/15/46a.

[69] See Lorrie Cranor, "Your research can help the FTC protect consumers," January 17, 2017, https://www.ftc.gov/news-events/blogs/techftc/2017/01/your-research-can-help-ftc-protect-consumers; Lorrie Cranor, "FTC goes to DEF CON," August 1, 2016, https://www.ftc.gov/news-events/blogs/techftc/2016/08/ftc-goes-def-con.

[70] See, e.g., Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, John Scott-Railton, and Sarah McKune, "Hacking Team's US Nexus," Citizen Lab, February 28, 2014, https://citizenlab.org/2014/02/hacking-teams-us-nexus/.

with the potential for reputational and financial impact, have an important stake in rejecting these practices of the commercial spyware industry.

These ICT companies may be in a better position than consumers to challenge the spyware trade. Not only are they typically better-resourced than individual users, but also, the legal arguments on which they may rely for remedy, based on intellectual property or contract law, are well-developed, recognized, and tested in jurisdictions around the world. For example, in 2013 Mozilla sent a cease and desist letter to Gamma Group, after it caught the spyware company using its marks and other intellectual property to "give users the false impression that, as a program installed on their computer or mobile device, [the spyware is] related to Mozilla and Firefox, and is thus trustworthy both technically and in its content."[71] Such activities merit high-level intervention for, as Mozilla noted, they "are deceptive, harm users, cause consumer confusion, and jeopardize [company] reputation."[72] Notably, in the U.S. certain intellectual property-related claims can also support action under the Racketeer Influenced and Corrupt Organizations Act (RICO).[73] Civil remedies available under RICO are of a caliber that could permanently shutter business operations of a defendant: they include treble damages, as well as "prohibiting any person from engaging in the same type of endeavor as the enterprise engaged in, the activities of which affect interstate or foreign commerce; or ordering dissolution or reorganization of any enterprise[.]"[74]

Membership associations in which ICT companies participate could also generate significant impact. Coordination of efforts among multiple companies to reject use of their good names, products, and services by the spyware trade would limit the options available to spyware developers in crafting means of digital intrusion, and instill a stronger awareness among spyware developers of the bounds of permissible behavior. The Global Network Initiative (GNI) and the Software Alliance (BSA) are two such associations that could credibly address the impact of the spyware trade on members' products and services, and advance potential responses. They may also consider bringing concerns about the vulnerabilities equities process

[71] Alex Fowler, "Protecting our brand from a global spyware provider," The Mozilla Blog, April 30, 2013, https://blog.mozilla.org/blog/2013/04/30/protecting-our-brand-from-a-global-spyware-provider/.
[72] Ibid.
[73] RICO prohibits conducting the affairs of an enterprise through a "pattern of racketeering activity," which is defined as "at least two acts of racketeering activity" within a ten-year period. These predicate acts include, inter alia: mail fraud (18 U.S.C. § 1341, https://www.law.cornell.edu/uscode/text/18/1341) and wire fraud (18 U.S.C. § 1343, https://www.law.cornell.edu/uscode/text/18/1343), which penalize the use of the U.S. mail or of wire communications, respectively, in furtherance of any "scheme or artifice to defraud"; trafficking in counterfeit goods or services (18 U.S.C. § 2320, https://www.law.cornell.edu/uscode/text/18/2320) or counterfeit labels, documentation, or packaging (18 U.S.C. § 2318, https://www.law.cornell.edu/uscode/text/18/2318); and criminal infringement of a copyright (18 U.S.C. § 2319, https://www.law.cornell.edu/uscode/text/18/2319). Such claims could arguably arise out of the use by spyware manufacturers of third-party marks or other identifying information in order to deceive targeted users into believing that malicious spyware is a legitimate, genuine program.
[74] 18 U.S.C. § 1964, https://www.law.cornell.edu/uscode/text/18/1964.

to the attention of the government;[75] such concerns are most likely to gain traction if high-profile industry participants make the case for why the existing treatment of vulnerabilities has serious repercussions for the economy and the user.

Lastly, businesses, and the associations of which they are a part, could withdraw their services (e.g., email accounts, domains, cloud services) from spyware companies and individuals associated with them when evidence emerges that spyware companies abuse these services as part of their espionage operations – a response well within the scope of typical terms of service. While these withdrawals will not preclude spyware companies from seeking out other options, they will set abusive behaviors back and raise company transaction costs while they regroup and assess alternatives.

☑ Draw on existing international normative and legal frameworks, including those pertinent to private military and security contractors, to develop an accountability framework specific to the private market for digital surveillance.

Existing international normative and legal frameworks provide essential foundation on which to address accountability in the commercial market for spyware. The development and use of advanced commercial spyware implicates a number of rights recognized under international human rights law, such as the rights to privacy and freedom of opinion and expression, as enshrined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. Indeed, privacy and freedom of expression are themselves enabling rights for a host of other protected human rights (freedoms of association, religion, movement, etc.). Any efforts to address the repercussions or normalize the use of spyware should be grounded in compliance with international human rights law.

Key frameworks on which to draw include:

- The UN Guiding Principles on Business and Human Rights, which make clear that business enterprises have the responsibility to respect internationally-recognized human rights, in their own activities as well as activities linked to their operations, products or services.
- Efforts undertaken within the UN to specifically address the right to privacy in the digital age, including the work of the Office of the United Nations High Commissioner for Human Rights (OHCHR),[76] and General Assembly resolutions on the issue. The most

[75] Mozilla has already presented recommendations on this topic to the U.S. government. See Heather West, "Mozilla Asks President Obama to Help Strengthen Cybersecurity," Mozilla, October 25, 2016, https://blog.mozilla.org/netpolicy/2016/10/25/mozilla-asks-president-obama-to-help-strengthen-cybersecurity/.

[76] See U.N. Human Rights Council, "The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights," U.N. Doc. A/HRC/27/37, June 30, 2014, http://www.un.org/ga/search/viewm_doc.asp?symbol=A/HRC/27/37.

recent resolution adopted by the General Assembly called on states to provide for "oversight mechanisms capable of ensuring transparency . . . and accountability for State surveillance of communications, their interception and the collection of personal data," as well as individual access to effective remedy. It also called upon business enterprises to fulfill their responsibility to respect human rights, "including the right to privacy in the digital age."[77]

- The work of the UN Special Rapporteurs, particularly the mandate holders on the rights to freedom of expression[78] and privacy.[79] Indeed, Frank La Rue, the former Special Rapporteur on freedom of expression, noted early on: "Offensive intrusion software such as Trojans, or mass interception capabilities, constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. . . . [T]he legal basis for [intrusion software's] use has not been publicly debated in any State, with the exception of Germany."[80] La Rue also noted that the "global industry focused on the exchange of surveillance technologies" is "virtually unregulated," and that states "have a responsibility to hold companies accountable" for participation in rights-infringing activities.[81]
- Developing international norms regarding cyberspace, as reflected in work such as that of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE). For example, in 2015 the UN GGE recommended a non-binding norm that "States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions."[82]

---

[77] U.N. General Assembly resolution 71/199, *The right to privacy in the digital age*, U.N. Doc. A/RES/71/199, December 19, 2016, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/71/199.

[78] See, for example, the May 2015 report of UN Special Rapporteur on freedom of expression David Kaye regarding encryption and anonymity, which, inter alia, recommended that "Corporate actors that supply technology to undermine encryption and anonymity should be especially transparent as to their products and customers." U.N. Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye," U.N. Doc. A/HRC/29/32, May 22, 2015, para. 62, http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/29/32.

[79] See, e.g., U.N. General Assembly, "Report of the Special Rapporteur on the right to privacy," U.N. Doc. A/71/368, August 30, 2016, http://www.un.org/ga/search/view_doc.asp?symbol=A/71/368 (identifying security and surveillance as a key thematic priority of the mandate holder). Among other topics, the Special Rapporteur on privacy has indicated that he will develop reports to be presented to the Human Rights Council in March 2017 and March 2018 focused on "privacy-friendly oversight of government surveillance" and "preliminary options within Internet Governance for an international legal instrument on government surveillance," respectively. Joseph A. Cannataci, UN Special Rapporteur on the Right to Privacy, "Planned Thematic Reports and call for consultations," OHCHR, http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx.

[80] U.N. Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue," U.N. Doc. A/HRC/23/40, April 17, 2013, paras. 62-63, http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/23/40.

[81] Ibid. at paras. 75-77.

[82] U.N. General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," U.N. Doc. A/70/174, July 22, 2015, para. 13(i), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

- Principles regarding the application of international law within the highly analogous context of private military and security companies (PMSCs).

Developments within the PMSC context deserve special note given the similarities of the two industries and the challenges they present. At the United Nations, a human rights special procedure, the Working Group on Mercenaries, has been tackling the PMSC issue since the Working Group's creation in 2005, following on the work of the preceding Special Rapporteur. In this context, independent experts have articulated what's needed to address the human rights problems that can arise when profit-motivated private actors, under the wing of yet distinct from the state, take on state security- and intelligence-related tasks.[83] As with the spyware industry, the experts noted that PMSCs (e.g., Academi – formerly Xe, which was formerly Blackwater) and their personnel are rarely held accountable for violations of human rights with which they are involved. The experts' work has included preparation of a draft international convention on PMSCs,[84] laying out international minimum legal standards for regulation, oversight, and accountability. Such standards seek to address the regulatory gap existent within the sector and the significant potential for human rights violations posed by the nature of the business.

At the outset, legal and policy questions arise as to whether commercial spyware companies should in fact *already be properly characterized* as PMSCs, given the sensitive services they provide to government entities. The Working Group on Mercenaries considered PMSCs to include companies providing intelligence and surveillance support to states.[85] Its draft

---

[83] As an organizing principle, the Working Group has elaborated the concept of "inherently State functions" – that is, functions that are "consistent with the principle of the State monopoly on the legitimate use of force and that a State cannot outsource or delegate to PMSCs under any circumstances." Included among such functions are "espionage, intelligence, [and] knowledge transfer with military, security and policing application." U.N. Human Rights Council, "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," U.N. Doc. A/HRC/15/25, July 2, 2010, at Annex: Draft of a possible Convention on Private Military and Security Companies (PMSCs) for consideration and action by the Human Rights Council, Art. 2(i), http://www2.ohchr.org/english/issues/mercenaries/docs/A.HRC.15.25.pdf. Such a concept may likewise be useful in delineating the services of concern in the dual-use technology sector, rather than focusing primarily on technical characteristics of an item.

[84] See ibid.; U.N. Working Group on Mercenaries, "Concept Note on a Possible Legally Binding Instrument for the Regulation of Private Military Security Companies," April 14, 2015, http://www.ohchr.org/Documents/HRBodies/HRCouncil/WGMilitary/Session4/WG_MercenariesCN_14April2015.pdf; "Statement of the Chair of the Working Group on the use of mercenaries for the 4th session of the Open-ended intergovernmental working group to consider the possibility of elaborating an international regulatory framework on the regulation, monitoring and oversight of the activities of private military and security companies," OHCHR, April 20, 2015, http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15881&LangID=E.

[85] See U.N. Human Rights Council, "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 people to self-determination," U.N. Doc. A/HRC/7/7, January 9, 2008, para. 29, http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/7/7 ("The Working Group notes that the PMSC industry currently provides in the international market a broad spectrum of services such as . . . . [inter alia] intelligence, covert operations and surveillance."). The Working Group later reiterated its concern over private sector involvement in intelligence activities, citing a *Washington Post* study of U.S. government intelligence agencies' "'dependency' on private contractors."

convention defines “military services” as including “intelligence” as well as “any kind of knowledge transfer with military applications, material and technical support to armed forces and other related activities.”[86] It defines "security services" to include "any kind of knowledge transfer with security and policing applications, development and implementation of informational security measures and other related activities."[87] These definitions are broad enough to encompass many of the activities of concern within the spyware trade, though further clarification is necessary to properly delineate the areas subject to regulation.

At the national level, South Africa and Switzerland have enacted regulations requiring registration and oversight of PMSCs that may cover companies providing surveillance tools and services. In South Africa, the *Private Security Industry Regulation Act* defines "security service" to include "manufacturing, importing, distributing or advertising monitoring devices"[88] as well as “installing, servicing or repairing security equipment”[89] – where “security equipment” includes “electronic monitoring device[s] or surveillance equipment.”[90] In Switzerland, the *Federal Act on Private Security Services Provided Abroad* covers, inter alia, “advising or training members of armed or security forces,” and "intelligence activities, espionage, and counterespionage" carried out by private companies.[91]

Regardless of whether policymakers choose to address the spyware trade within an established PMSC framework, approaches to PMSC regulation should inform regulation of dual-use technology. For example, elements of the draft international convention proposed by the UN

See U.N. General Assembly, “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,” U.N. Doc. A/65/325, paras. 7-8, August 25, 2010, http://www.un.org/ga/search/viewm_doc.asp?symbol=A/65/325.

[86] U.N. Human Rights Council, “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,” U.N. Doc. A/HRC/15/25, July 2, 2010, at Annex: Draft of a possible Convention on Private Military and Security Companies (PMSCs) for consideration and action by the Human Rights Council, Art. 2(b), http://www2.ohchr.org/english/issues/mercenaries/docs/A.HRC.15.25.pdf.

[87] U.N. Human Rights Council, “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,” U.N. Doc. A/HRC/15/25, July 2, 2010, at Annex: Draft of a possible Convention on Private Military and Security Companies (PMSCs) for consideration and action by the Human Rights Council, Art. 2(c), http://www2.ohchr.org/english/issues/mercenaries/docs/A.HRC.15.25.pdf.

[88] Private Security Industry Regulation Act, No. 56 of 2001, Republic of South Africa Government Gazette, January 25, 2002, at Chapter 1, http://www.gov.za/documents/private-security-industry-regulation-act.

[89] Ibid.

[90] Ibid.

[91] Federal Act on Private Security Services provided Abroad, Federal Assembly of the Swiss Confederation, September 27, 2013, at Art. 4(a)(8),(9), https://www.eda.admin.ch/content/dam/eda/en/documents/aussenpolitik/sicherheitspolitik/Bundesgesetz-ueber-die-im-Ausland-erbrachten-privaten-Sicherheitsdienstleistungen-BPS_EN.pdf; see also Federal Department of Foreign Affairs, *Guidelines to the Federal Act on Private Security Services provided Abroad*, May 2016, https://www.eda.admin.ch/content/dam/eda/en/documents/aussenpolitik/sicherheitspolitik/wegleitung-BPS-ausland_EN.pdf.

Working Group on Mercenaries that appear equally applicable and essential to regulation of the commercial spyware trade include:

- A definition of the behavior to be regulated, which can focus on a service or set of activities of concern and incorporate end user/use considerations, rather than delineating a specific item for control.
- Reaffirmation of the responsibility of states with respect to the private companies that are registered or operate in their jurisdictions, or with which they contract.
- As appropriate, prohibitions on delegation of certain state functions to private companies, or designation of particular state security-related activities in which a private company must not engage.
- Requirements for national regimes of regulation and oversight of companies, which cover, *inter alia*: company registration and state registries of PMSCs; licensing; company reporting; state monitoring and investigation; and training of PMSC personnel. Mandated transparency[92] at the national level will be an essential component of any accountability structure.
- Principles regarding applicable jurisdiction, imposition of criminal and civil liability, and access to remedy.
- A complementary structure for international oversight and monitoring.

Despite challenges – including opposition from some governments to increased regulation of an industry on which they frequently rely and which generates significant economic returns[93] – progress in the PMSC context illustrates a way forward on efforts to regulate private sector participation in state security functions.

In an ideal world, solutions to the problems presented by the commercial spyware industry will be coordinated internationally, drawing on international law and norms. Only global solutions will prevent opportunistic behavior and exploitation of regulatory gaps by industry participants – for example, the relocation of companies to states that do not participate in the Wassenaar Arrangement. National governments, as well as regional and international institutions, should seek to develop new international frameworks of control tailored to the phenomenon of commercial spyware and its responsible use. One possible starting point may be to create an

[92] For further discussion of mandated transparency, see Ronald Deibert, "What to do about 'dual use' digital technologies?," November 29, 2016, https://deibert.citizenlab.org/2016/11/dual-use/.

[93] For example, a number of developed countries have opposed UN resolutions concerning regulation of PMSCs. See, e.g., U.N. General Assembly, "Third Committee: Summary record of the 51st meeting," U.N. Doc. A/C.3/68/SR.51, November 26, 2013, paras. 58-59, http://www.un.org/ga/search/viewm_doc.asp?symbol=A/C.3/68/SR.51, reflecting opposition from the EU, Australia, Canada, Israel, Japan, South Korea, and the US, among others ("A clear distinction must be drawn between the use of mercenaries and the lawful activities of private military and security companies; the fact that the Working Group on the use of mercenaries was mandated to consider both of those issues led to confusion. . . . The European Union encouraged the Working Group to remain open-minded regarding possible forms of regulation and oversight of those companies. In the absence of a common understanding on important definitions and approaches to that issue, the States members of the European Union would, as in previous years, vote against the draft resolution.").

international or regional working group akin to the UN Working Group on Mercenaries to investigate, and make holistic, rights-based recommendations regarding, the current circumstances of the spyware market. Such effort would be a logical follow-on to steps already taken by the EU to establish flexible export controls for dual-use technologies, as well as to progress made in the context of PMSC industry self-regulation (see below).

☑ Explore industry self-regulation.

Efforts within industry to "self-regulate" – by committing to voluntary yet genuine accountability frameworks and human rights-oriented policies and practices – could serve as a complement to other accountability measures. For example, in the PMSC context, governments, the PMSC industry, and civil society actors have together developed principles relevant to, and a multistakeholder framework for, PMSC regulation. Such regulation was the result of step-by-step effort undertaken over the past decade: In 2008, as a result of an initiative led by Switzerland in cooperation with the International Committee of the Red Cross, 17 countries adopted the Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict, which affirmed the applicability of international law to PMSC activities in armed conflict and laid out best practices, including with regard to "monitoring compliance and ensuring accountability." The document is now supported by 54 states and a forum for participant engagement.[94]

In 2010, the International Code of Conduct for Private Security Service Providers was adopted – the work of a multistakeholder initiative launched by Switzerland but bringing together civil society groups, academics, PMSCs, and governments to address the human rights challenges of this sector. The document, which referenced as a starting point both the Montreux Document and the UN Guiding Principles on Business and Human Rights, outlines the operational standards to which PMSC signatories commit in order to fulfill their human rights responsibilities. Beginning in 2013, the Code of Conduct was backed by a process for certification and monitoring of signatories, carried out by the International Code of Conduct for Private Security Providers' Association (ICoCA). ICoCA includes equal representation on its decision-making board of the three pillars of government, industry, and civil society. The association also offers a grievance mechanism, as its board hears complaints on alleged violations of the Code. Finally, most recently, a new ISO standard was released specific to the PMSC industry: ISO 18788: Management system for private security operations (2015) (which itself draws on the aforementioned documents and the UN Guiding Principles on Business and Human Rights).

This progress demonstrates that standard-setting within sensitive government-linked industries is possible, and may promote rights-related norms. While such industry initiatives are voluntary

[94] Montreux Document Forum, "Participating States and International Organisations," http://mdforum.ch/en/participants.

in nature and insufficient in isolation to establish accountability,[95] they are useful in creating industry awareness and buy-in, a more level playing field (a critical concern for the private sector), and best practices, including model contracts. As the spyware industry matures, companies may find it in their interest to engage with each other to coordinate transparent, expected standards of behavior in order to mitigate risk. At the same time, government spending and procurement policies that condition award of government contracts on a company's participation in accountability frameworks,[96] evidence of human rights due diligence measures, and human rights track record could incentivize compliance with rights-based standards.

☑ Build out communities of practice to raise public awareness and document abuses.

One of the indirect ways in which the excesses of the commercial spyware industry can be controlled is through careful public research. For example, over the last several years and over the course of numerous reports, the Citizen Lab has carefully documented targets, victims, malware signatures, command and control servers, and the proliferation of the commercial spyware industry's products and services to numerous government clients. The research led to numerous high-profile media reports on the commercial spyware industry, and helped inform some of the litigation and advocacy campaigns mentioned earlier.

Of course, the Citizen Lab is but one relatively small research centre. However, this research has employed peer-reviewed, reproducible, and transparent methods that could be emulated by others. If normalized and broadened across numerous research centres worldwide, the research could have a compounding effect on public awareness and visible evidence of abuse, and function as a kind of verification for violations of human rights using digital spyware. Careful, evidence-based research is difficult to ignore. It can help inform litigation efforts,

---

[95] As the Working Group's draft convention notes, "Taking into account the adoption of codes of conduct, but considering that self-regulation of private military and security companies is not sufficient to ensure the observance of international humanitarian law and human rights law by the personnel of these companies . . . ." U.N. Human Rights Council, "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," U.N. Doc. A/HRC/15/25, July 2, 2010, at Annex: Draft of a possible Convention on Private Military and Security Companies (PMSCs) for consideration and action by the Human Rights Council, PP 20, http://www2.ohchr.org/english/issues/mercenaries/docs/A.HRC.15.25.pdf.

[96] For example, the U.S. State Department indicated membership in ICoCA would be a "requirement in the bidding process for the successor contract to the Worldwide Protective Services (WPS) program." See "U.S. State Department to Incorporate International Code of Conduct into Worldwide Protective Services Contracts," August 16, 2013, https://www.humanrights.gov/dyn/u.s.-state-department-to-incorporate-international-code-of-conduct-into-worldwide-protective-services-contracts. However, the U.S. Department of Defense notes that it "will not require signature to the ICoC or certification and oversight by the ICoC Association as a condition of any DoD contracts." See Office of the Assistant Secretary of Defense for Logistics & Materiel Readiness, "Private Security Companies," http://www.acq.osd.mil/log/ps/psc.html. A consistent approach in states' procurement policies will be essential to the effectiveness of a voluntary accountability framework.

advocacy, and awareness about digital defenses that can contain the abuses of the commercial spyware industry and build a community of practice that responds extensively and acts as a counterweight to the market.

Many obstacles stand in the way of this community of practice being broadened. Academic disciplines work in silos, and there are institutional constraints standing in the way of the type of interdisciplinary research of the sort in which Citizen Lab engages. For these silos to be broken down requires persistent field-building and cross-disciplinary collaboration that takes time and leadership. One area where this community of practice could be broadened, but faces enormous contrary pressures, is around the practices of so-called national computer emergency response teams (CERTs). CERTs evolved out of universities as a mechanism to share threat information seamlessly across Internet network operators. Over time, unfortunately, some CERTs have been co-opted into national security frameworks, and their operations impacted by the requirements to preserve threat information in the name of national security, with their relations with other national CERTs stilted as a consequence.[97] While reversing these trends will be difficult, the original model of a distributed but transparently coordinated body of CERTs providing threat information to each other could be one to aspire to as a bulwark against targeted digital attacks, regardless of where they occur or from whom they originate.[98]

One area where the community of practice that invigilates against the commercial spyware market could be helpfully broadened would be by the participation of the private sector security industry. Much like the complex involvement of governments, there are challenges in enlisting the private sector security industry in the fight against commercial spyware. The security industry is bound by confidentiality agreements with clients that make sharing of information sensitive, and many have product lines that bleed into the very market under discussion, particularly as services around “hacking back” become normalized as part of the sector. However, the private sector security industry also includes many individuals who care passionately about human rights, and some companies have demonstrated a willingness to share data and resources with groups like the Citizen Lab in an effort to better document abuses. Developing a more mature “pro bono” culture within the security industry analogous to that which exists in the legal profession, in which databases, threat intelligence feeds, and other types of support are shared with researchers and the human rights research community, could bolster defenses of affected civil society groups, ensure relevant indicators of compromise are widely shared with network defenders, and raise the bar against attacks coming from threat actors using commercial spyware.

---

[97] See Tim Maurer, Mirko Hohmann, Isabel Skierka and Robert Morgus, “National CSIRTs and Their Role in Computer Security Incident Response,” New America Foundation, November 29, 2015, https://static.newamerica.org/attachments/11916-national-csirts-and-their-role-in-computer-security-incident-response/CSIRTs-incident-response_2-2016.eea78f5a4748443d8000903e300d5809.pdf.

[98] The “CyberGreen” initiative, spearheaded by Japan’s CERT, may offer one such model. See CyberGreen, http://www.cybergreen.net/; Japan Computer Emergency Response Team Coordination Center, *The Cyber Green Initiative: Improving Health Through Measurement and Mitigation*, August 10, 2014, http://www.cybergreen.net/img/medialibrary/ConceptPaper.nov_.pdf.

Finally, ICT companies may choose to play a role in preventing compromise as a result of spyware or other digital threats. Companies can proactively search for malicious uses of their products and services, alert researchers to threat indicators, educate high risk users about warning signs (such as spoofing and phishing), and even potentially alert targets about spyware campaigns – similar to what Google has done with its "state-sponsored attack" warnings.

While building out a community of practice will not solve the problem of the abuse of commercial spyware, it will help build up a larger network of defenses, and could potentially result in a more robust series of reporting mechanisms in which cases of abuse are identified, documented, publicized, and then mitigated.

****

Over the last several years, a growing body of evidence has come to light showing widespread abuses of advanced commercial spyware and the negative externalities of this unregulated industry. Troublingly, the leaked documents, market brochures, and public reports are likely but the tip of a growing iceberg. Governments, especially those that lack the rule of law or are sliding back into autocratic rule, are facing a more digitally equipped civil society that they want to shape, control, and even eradicate. For these actors, the wares of the commercial spyware market are an irresistible high-tech solution, and the companies are only too willing to find yet another high-paying client. Left unchecked, we can expect this market dynamic will lead to steadily rising cases of the unlawful targeting of dissidents, journalists, human rights organizations and their funders, with deadly consequences.

There are many advocates and policymakers who recognize these dangers and want to do something about them. Unfortunately, the first attempt to regulate commercial spyware got off on the wrong foot given the limitations of the export control model. Public discourse on regulation of the commercial spyware market devolved to an "either/or" proposition: either the flawed model of export controls or an unregulated industry run amok. Meanwhile, other options to control commercial spyware have been left relatively unexplored.

In this article, we have put forth a variety of other methods by which the negative externalities of the commercial spyware market can be limited and even rolled back. Although these approaches will not eliminate the human rights abuses that drive government appetites for commercial spyware in the first place, they will hopefully create a web of constraints against an otherwise unregulated market and bring a degree of accountability to what is now a largely unchecked and easily-abused industry. Almost certainly there will remain in practice numerous instances of legitimate, lawful use of digital interception by government agencies. But when those government agencies cross the line into illegitimate and unlawful targeting against civil society that contravenes internationally recognized human rights, there must be consequences

for those entities as well as the organizations that aid and abet them. We hope we have at least provided a roadmap for what some of those consequences might look like.