REGULATING COMMERCIAL SPYWARE

Asaf Lubin[*]

August 2023

Only a binding multistakeholder legal framework can effectively regulate a legitimate and efficiently controlled market for spyware.

Our phones and computers, and the applications we run on them, all suffer from bugs and vulnerabilities.[1] This reality has led to a lucrative and ever-growing commercial spyware market. Spyware companies employ scores of former intelligence professionals and government hackers to churn up these weaknesses and turn them into surveillance products that provide clients with the power of unauthorized access.[2] The business model of this market is quite simple: Be the first to find the

[*] Dr. Asaf Lubin is a Visiting Professor of Law at Columbia Law School (fall 2023), and an Associate Professor of law at Indiana University Maurer School of Law. The work benefited from insightful and helpful conversations with Anupam Chander, Mailyn Fidler, Amy C. Gaudion, Greg Nojeim, Jason Pielemeier, Alan Rozenshtein, Matthew Waxman, and Adriana Edmeades, as well as colleagues at the State Department, Hebrew University of Jerusalem, and NSO Group. Earlier versions of this paper, or ideas from it, were presented at the UCLA Institute for Technology, Law, and Policy Workshop on Calibrating Data Surveillance, the 2023 Association of American Law School Annual Meeting, as well as the Consultation on Ethical and Rights-Respecting Technology hosted by the Berkman Klein Center for Internet and Society, the Global Network Initiative, the Carr Center for Human Rights, and the Edmond & Lily Safra Center for Ethics at Harvard University. A significantly longer version of this paper, titled "Private Markets, Public Vulnerabilities," is accessible on SSRN at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323985.

[1] See Bryan Choi, "Crashworthy Code," *Washington Law Review* 94 (2019): 46 ("Today, software code faces the same crossroad. Bugs and vulnerabilities are so rampant across the industry that the question of cybercrashes and cyberattacks is not 'whether' but 'when.'"); Alan Z. Rozenshtein, "Wicked Crypto," *University of California Irvine Law Review* 9 (2019): 1206 ("As is apparent to anyone whose computer has ever been infected by a virus or whose smartphone incessantly pesters about 'critical security' system updates, electronic devices are shot through with software vulnerabilities. These vulnerabilities allow unauthorized third parties, whether criminal hackers or government investigators, to overcome whatever security measures are in place and access user data.").

[2] The client could use the software to acquire "passwords, contact lists, calendar events, text messages, and live voice calls from popular mobile messaging apps. The operator can even turn on the phone's camera and

vulnerability, generate an interactive use interface around it, and sell it to the highest bidder. Lather, rinse, repeat.

The clients for these solutions are predominantly government agencies. As more and more of our communication technologies become end-to-end encrypted, intelligence collection and evidence gathering in criminal and national security investigations become harder and harder to execute. Spyware solutions are thus essential in the age of "going dark."[3] The ability to remotely and covertly access laptops and smartphones, with relative technological ease, means that law enforcement investigators now have the power to wiretap the criminals' own pockets. When done within a rule-of-law system, such investigations are vitally important in stopping and preventing acts of terrorism and violent extremism, the proliferation of child pornography online, and other categories of serious physical and online crimes.[4]

Outside of a rule-of-law framework, however, these tools pose significant risks. Recent investigative reporting has shown the scope and degree of abuses produced by these technologies. Around the world, government actors rely on spyware to target human rights activists, journalists, and political dissidents, with almost no accountability. Governments in countries such as Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates have all utilized surveillance tools to commit gross human rights abuses.[5]

---

microphone to capture activity in the phone's vicinity." Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, & John Deibert, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," Citizen Lab Research Report No. 113, University of Toronto, Sept. 18, 2018, https://perma.cc/F6S5-XHWK, 7.

[3] "Going dark refers to the phenomenon by which government agencies have a legal right to access particular communications but lack the technical ability to do so, often because technology companies have deployed strong encryption to shield the information." Susan Hennessey, "Lawful Hacking and the Case for a Strategic Approach to 'Going Dark'," Brookings Institution, Oct. 7, 2016, https://perma.cc/GFU5-HXU3. See also James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" FBI, Oct. 16, 2014, https://perma.cc/PR3Z-WCA3 (calling for legal and technological solutions to the going dark problem); cf. Jonathan L. Zittrain, Matthew G. Olsen, David O'Brien, & Bruce Schneier, "Don't Panic: Making Progress on the 'Going Dark' Debate," Berkman Klein Center for Internet and Society, 2016, https://perma.cc/W8X5-MZLZ (questioning "whether the 'going dark' metaphor accurately describes the state of affairs"), 2.

[4] See, e.g., Frank Andrews, "Pegasus: NSO Group's Long History of Trials and Denials," *Middle East Eye*, July 20, 2021 (listing the justifications for the spyware market as provided by officials from NSO Group).

[5] "Unchecked Spyware Industry Enables Abuses," Human Rights Watch, July 30, 2021, https://perma.cc/XP4U-4GMD.

Carine Kanimba, a U.S. citizen, knows firsthand what such misuses feel like. Paul Rusesabagina, Carine's father and a dissident of Rwanda who lived in San Antonio, Texas, was targeted by such surveillance tools.[6] Using access to data on his phone, Paul was lured by a Rwandan intelligence operative to visit Dubai, where he was kidnapped and sent back to Kigali.[7] There he was convicted and sentenced to 25 years in prison.[8] Carine, who was herself the target of spying by Rwanda, gave chilling testimony to the U.S. House Permanent Select Committee on Intelligence in July 2022. She noted:

> I am frightened by what the Rwandan government will do to me and my family next. It is horrifying to me that they knew everything I was doing, precisely where I was, who I was speaking with, my private thoughts and actions, at any moment they desired. Unless there are consequences for the countries and their enablers which abuse this technology to hurt innocent people, none of us are safe.[9]

The threat of commercial spyware to the rule of law comes not only from authoritarian regimes or those notorious for their human rights abuses. Consider in this regard the Israeli security firm NSO Group. NSO Group has been in the spotlight in recent years due to an endless stream of revelations and allegations that its primary spyware product, Pegasus, has been used to target human rights defenders, anti-corruption lawyers, diplomats, opposition leaders, and political pollsters all over the world.[10] Pegasus relies on "a chain of zero day exploits" to break security and encryption on iOS and Android devices, which then allows the operator to gain unlimited access to data on the targeted mobile phones.[11]

As NSO Group's cofounder and the former CEO of the company, Shalev Hulio, acknowledged, "[T]he big, dirty secret is that governments are buying this stuff—not just authoritarian governments but all

---

[6] "Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware," Hearing Before the House of Representatives Permanent Select Committee on Intelligence, 116th Congress (Witness Statement of Carine Kanimba), July 27, 2022, https://perma.cc/S7M7-LT5Z.

[7] Id.

[8] Id.

[9] Id.

[10] Omer Benjakob, "The NSO File: A Complete (Updating) List of Individuals Targeted With Pegasus Spyware," *Haaretz,* April 5, 2022.

[11] See, e.g., Marczak et al., supra note 2; Stephanie Kirchgaessner, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani, & Michael Safi, "Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon," *The Guardian,* July 18, 2021; Stephanie Kirchgaessner, "Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests," *The Guardian,* July 18, 2021; Lucas Ropek, "Presidents, Prime Ministers, and a King Among Potential NSO Spying Targets, Including French Leader Macron," *Gizmodo,* July 20, 2021.

types of governments."[12] In that same interview, he went on to say that NSO Group had a "monopoly in Europe" with "almost all governments" across the continent using its tools.[13]

The European Parliament established a committee of inquiry (the PEGA Committee) to investigate the use of Pegasus and other equivalent spyware by European Union (EU) member states.[14] Members of the PEGA Committee have concluded that spyware "is running amok in Europe"[15] with the EU acting as an exporter of spyware "to third countries with undemocratic regimes and a high risk of human rights violations."[16] In its recently adopted final report,[17] the PEGA Committee came to an even more troubling conclusion: "EU Member State governments have been using spyware on their own citizens for political purposes and to cover up corruption and criminal activity. Some went even further and embedded spyware in a system deliberately designed for authoritarian rule."[18] The report summarized the human rights risks associated with an unregulated market of commercial spyware:

> The abuse of spyware does not just violate the right to privacy of individuals. It undermines democracy and democratic institutions by stealth. It silences opposition and critics, eliminates scrutiny and has a chilling effect on free press and civil society. It further serves to manipulate elections. The term "mercenary spyware" reflects very well the nature of the product and of the industry. Even failed attempts to infect a smart phone with spyware have political ramifications, and can harm the individual as well as

[12] Ronan Farrow, "How Democracies Spy on Their Citizens," *New Yorker,* April 18, 2022.

[13] Id.

[14] European Parliament Committee Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware, "Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware" (Rapporteur: Sophie in't Veld), May 5, 2023, https://perma.cc/2NV8-T8HF (hereinafter PEGA Report).

[15] Lyubov Pronina, "Spyware Is Running Amok in Europe, EU Lawmaker Warns," *Bloomberg Law,* Nov. 8, 2022.

[16] PEGA Report, supra note 14, at 3–4.

[17] Press Release, "Spyware: MEPs Sound Alarm on Threat to Democracy and Demand Reforms," European Parliament, May 8, 2023, https://perma.cc/E7EH-6V6C. The PEGA Committee adopted the report "with 30 votes in favour, 3 against, and 4 abstaining, and a text outlining recommendations for the future with 30 votes in favour, 5 against, and 2 abstaining." On June 15, 2023, the European Parliament adopted the recommendations, see "European Parliament recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware," Resolution 2023/2500(RSP), https://perma.cc/MB2M-CMTT (hereinafter PEGA Recommendations).

[18] PEGA Report, supra note 14, at 140.

> democracy. Participation in public life becomes impossible without the certainty of being free and unobserved.[19]

The mounting evidence from around the world as to the scope of abuse from Pegasus has rekindled and reframed the debate over the ethics and legality of the surveillance tech trade.[20] In the past few years, UN human rights special rapporteurs, members of the European Parliament, and civil society have joined together, calling for an immediate and global moratorium on the sale, transfer, and use of these technologies.

In this paper I argue against these kinds of moratoriums. While fully recognizing the harms that spyware poses, I contend that calls for banning the tools are not only impractical, but they pose a danger to public safety and the future integrity of our information and telecommunication technologies. I further demonstrate the limitations of alternative legal responses that have been tried, including industry self-regulation, ad hoc litigation, and ex post blacklisting and sanctions. For each of these approaches, I demonstrate why they are similarly inapt, as stand-alone measures, in mitigating spyware risks.

As an alternative to these flawed approaches, I make the case for an international system to standardize the commercial spyware industry, which I call the Commercial Spyware Accreditation System (or CSAS for short). This binding multistakeholder legal framework and forum offers a menu of modular solutions. While I believe the complete framework should be adopted wholesale, I embrace the idea that parts of my solution could be taken up gradually by a group of like-minded states looking to set up a legitimate and efficiently controlled market for spyware.

This paper has three sections. The first section provides a detailed account of current proposals, both in the United States and in the European Union, to address the human rights abuses from unregulated use of commercial spyware. The core takeaway from this section is quite simple: What all of this activity demonstrates is that there has never been a more opportune time politically to propose an international framework for commercial spyware that could be meaningfully picked up by a large number of powerful states. The second section discusses the limits of each of the existing proposals for regulation, particularly focusing on moratoriums, industry self-regulation, and ad hoc litigation and sanctions. Each of these frameworks is insufficient or inadequate to address the risks posed by the spyware trade. The third section shifts the focus to my proposed CSAS model and offers it as a modular solution for countries to explore.

---

[19] Id.

[20] See, e.g., Kali Robinson, "How Israel's Pegasus Spyware Stoked the Surveillance Debate," Council on Foreign Relations, March 8, 2022.

A U.S.-EU RACE TO REBOOT COMMERCIAL SPYWARE REGULATION

Both the United States and the European Union have advanced new domestic and international regulations and enforcement in response to the unfolding saga surrounding Pegasus and NSO Group. A new transatlantic race to reboot regulations is brewing. This race demonstrates a degree of maturity and sophistication in the quality of discourse around spyware regulation, the likes of which haven't been seen in previous attempts.

A study of the measures adopted or considered both in the United States and in Europe reveals five common categories of responses to spyware abuses: (a) industry self-regulation, (b) ad hoc enforcement and sanctions, (c) private action, (d) moratoriums and tech bans, and (e) international cooperation. In this section I demonstrate how each of these categories has been attempted to date. The takeaway is clear: There is a growing consensus by a large number of powerful states in the international community that the trade in commercial spyware cannot continue unchecked. A wide assortment of responses has in fact already been tried. In the next section I will explain why none of these measures has so far succeeded in curtailing abuses from spyware, leading to my CSAS proposal in the final section.

Industry Self-Regulation

Perhaps the starting point for any discussion of market regulation is to provide the market an opportunity to self-correct. This is the least costly option and involves no binding regulation that could risk competition and innovation. Under this bucket of responses, states could turn to a set of human rights frameworks, namely the United Nations Guiding Principles on Business and Human Rights (the UNGPs) and the Organization for Economic Cooperation and Development's Guidelines for Multinational Enterprises (OECD MNE Guidelines). The UNGPs and the OECD MNE Guidelines, which are "closely connected and aligned,"[21] represent a set of international norms and standards that could guide responsible business behavior. Combined, the two sets of norms "have played an increasingly important role in the compliance landscape for both companies and investors in recent years."[22] They have introduced a set of expectations from business enterprises "to identify, prevent, mitigate, and address business-related human rights impacts"[23] by requiring due diligence, transparency, and accountability. Of course, the effectiveness of these norms depends in part on domestic adoption of legislation and enforcement action that could hold companies to account for violations of these norms.

---

[21] Surya Deva, Chairperson, Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, "Re: Public consultation - Stocktaking exercise on the OECD Guidelines for Multinational Enterprises," Oct. 11, 2021, https://perma.cc/2WVP-3W5B, 1.

[22] Bart van de Laar, "Applying Business and Human Rights International Standards to Investor Due Diligence," SustainAnalytics, Sept. 15, 2022, https://perma.cc/BCY5-Q2MB.

[23] Deva, supra note 21, at 1.

But even where such domestic legislation does not exist, action by investors and consumers might play a role in nudging corporate governance toward greater compliance.

In the surveillance tech context, we have seen a move toward such self-regulation. In September 2020, the State Department's Bureau of Democracy, Human Rights, and Labor published a "first-of-its-kind tool intended to provide practical and accessible human rights guidance to U.S. businesses seeking to prevent their products or services with surveillance capabilities from being misused by government end-users to commit human rights abuses."[24] The guidance seeks to implement both the UNGPs and the OECD MNE Guidelines in the surveillance tech industry.

The State Department guidance comprises a series of best practices that surveillance tech companies are encouraged to implement. These include the implementation of human rights impact assessments for products, services, supply chains, and client selection; the promotion of human rights by design in the research and development stages of the surveillance tool; and adoption of certain contractual and procedural safeguards and transparency requirements in both the presale and postsale stages.

Ad Hoc Enforcement and Sanctions

In July 2021, an international journalism consortium called Forbidden Stories released what they called the Pegasus Project. The project detailed the results of an investigation into a massive data leak that revealed "more than 50,000 phone numbers that [are believed] to have been identified as those of people of interest by clients of NSO Group since 2016."[25] Responding to this report, in November 2021 the Commerce Department added NSO Group and another Israeli commercial spyware company, Candiru, to the Entity List, finding their activities "contrary to the national security or foreign policy interests of the United States."[26] As commentators have noted, the decision—the first of its kind against an Israeli spyware company—not only had real and immediate economic impacts on NSO Group but also carried

---

[24] Press Release, "U.S. Department of State Guidance on Implementing the 'UN Guiding Principles' for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities," Bureau of Democracy, Human Rights, and Labor, Department of State, Sept. 30, 2020, https://perma.cc/LF72-X58X. See also "U.S. Department of State Guidance on Implementing the 'UN Guiding Principles' for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities," Bureau of Democracy, Human Rights, and Labor, Department of State, Sept. 30, 2020, https://perma.cc/JZF3-35L8 (hereinafter Due Diligence Guidance).

[25] Kirchgaessner, "Revealed," supra note 11. There remains a great deal of uncertainty about the source of the leak and the extent to which every single one of those 50,000 phone numbers has actually been the target of Pegasus surveillance. See Omer Kabir & Hagar Ravet, "NSO CEO Exclusively Responds to Allegations: 'The List of 50,000 Phone Numbers Has Nothing to Do With Us'," *Calcalist Tech*, July 20, 2021.

[26] Addition of Certain Entities to the Entity List, 86 Fed. Reg. 60,758, Nov. 4, 2021.

signaling effects that echoed far beyond.[27] John Scott-Railton, senior researcher at Citizen Lab, in his testimony before the House Intelligence Committee in July 2022, offered a similar observation: "The entity list is not an individual sanction, not a comprehensive package. Nobody is losing their rooftop swimming pool. But it shows investors, some of whom are based in the United States … that this industry is risky to them … and we saw it have effect. We saw reports that the debt valuation of NSO precipitously dropped. The company now appears to be in a tailspin."[28]

To further institutionalize the process of blacklisting and sanction designations for spyware companies, in December 2022 Congress passed and President Joe Biden signed the James M. Inhofe National Defense Authorization Act (NDAA) for Fiscal Year 2023.[29] The act introduced three key measures. First, the act obligates the director of national intelligence (DNI) in coordination with the directors of the Central Intelligence Agency, the National Security Agency, and the Federal Bureau of Investigation to produce an annual report that lists the most significant foreign companies that engage in the spyware

[27] Charles Capito, Brandon L. Van Grack, & Logan Wren, "Recent Additions to Entity List Part of Broader U.S. Effort Targeting Spyware," *Lawfare,* Nov. 29, 2021 ("Designating a company on the Entity List, which is administered by the Commerce Department's Bureau of Industry and Security, can cripple a company because it empowers the U.S. government to restrict parties from accessing U.S.-origin products or technology. In effect, a company on the Entity List is banned from directly or indirectly obtaining items subject to the Export Administration Regulations (such as telecommunications equipment) without U.S. government approval. The Entity List provides specific license requirements for each listed entity, typically requiring that the entity obtain a license to access every item subject to the Export Administration Regulations…. The listing could [thus] harm NSO Group by inhibiting its ability to use certain computing and software services or by rendering the company less attractive to investors"). In June 2022, it was reported that Israeli officials were "pushing the Biden administration" to remove NSO Group from the list, while the company hired "two U.S. law firms to work on the blacklist issue independently from the Israeli government." See Barak Ravid, "Scoop: Israelis Push U.S. to Remove NSO From Blacklist," *Axios,* June 8, 2022.

[28] House Hearing on Foreign Spyware, C-Span, July 27, 2022, from minute 39:15 to 39:47, https://perma.cc/WK68-KDL8

[29] James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, H.R. 7776 (hereinafter NDAA FY23). These measures add to efforts that were already launched in the 2022 National Defense Authorization Act. That NDAA required the State Department, in consultation with the director of national intelligence, to "identify contractors that have knowingly assisted or facilitated certain cyberattacks or conducted surveillance activities on behalf of relevant foreign governments against the United States or for the purposes of suppressing dissent or intimidating critics." Letter from Susie Feliz, Assistant Secretary for Legislative and Intergovernmental Affairs at the Department of Commerce, and Naz Durakoglu, Assistant Secretary for Legislative Affairs at the Department of State, to Rep. Jim Himes and Rep. Jackie Speier, Nov. 16, 2022, https://perma.cc/8JHU-6M4Y, 3. This process of identifying contractors and producing such list is ongoing.

trade.[30] Second, and in addition to the report, the DNI is required to produce a classified watchlist of foreign commercial spyware companies that the director "determines are engaged in activities that pose a counterintelligence risk to personnel of the intelligence community,"[31] in preparation for the imposition of sanctions against them. Finally, the act granted the DNI the authority to "prohibit any element of the intelligence community from procuring, leasing, or otherwise acquiring on the commercial market, or extending or renewing a contract to procure, lease, or otherwise acquire, foreign commercial spyware."[32] The act proceeds to provide a set of considerations that must be taken into account in the exercise of the DNI's discretion in yielding this authority.[33] Moreover, the DNI's authority to block contracting extends beyond covered entities, to include any "company that has acquired, in whole or in part, any foreign commercial spyware."[34]

Outside of the United States, sanctions and blacklisting have not been embraced. The European Commission, for example, "has so far not undertaken an analysis of the situation nor an assessment of

[30] Id., NDAA FY23, at 1122. A covered entity is defined by the act as a "foreign company that either directly or indirectly develops, maintains, owns operates, brokers, markets, sells, leases, licenses, or otherwise makes available spyware." Id. at 1121. The annual report will include, among other things (a) the type of spyware associated with the covered entity; (b) the counterintelligence risks posed by that spyware; (c) the place where the covered entity is domiciled; (d) the relationship between the covered entity and any foreign government, including any export controls or processes it is subjected to; and (e) details about the covered entity's business dealings, including subsidiaries, resellers, or other agents acting on behalf of the covered entity, information about the covered entity's financing (including how it acquired its capital, and the organizations and individuals with substantial investments in it), and a list of the covered entity's foreign customers and an assessment of the way that each of them has utilized the spyware. Id. at 1122–1123.

[31] Id. at 1123.

[32] Id.

[33] Id. at 1123–1124. (The list of considerations includes "(i) the assessment of the intelligence community of the counterintelligence threats or other risks to the United States posed by foreign commercial spyware; (ii) the assessment of the intelligence community of whether the foreign commercial spyware has been used to target United States Government personnel; (iii) whether the original owner or developer retains any of the physical property or intellectual property associated with the foreign commercial spyware; (iv) whether the original owner or developer has verifiably destroyed all copies of the data collected by or associated with the foreign commercial spyware; (v) whether the personnel of the original owner or developer retain any access to data collected by or associated with the foreign commercial spyware; (vi) whether the use of the foreign commercial spyware requires the user to connect to an information system of the original owner or developer or information system of a foreign government; and (vii) whether the foreign commercial spyware poses a counterintelligence risk to the United States or any other threat to the national security of the United States.")

[34] Id. at 1124.

the companies that are active on the spyware market within the EU."[35] Similarly, the "European Council has not responded publicly or substantively to the scandal."[36]

Nonetheless, the PEGA Committee has called for the formation of "a dedicated standing parliamentary committee" within the European Parliament that will have "access to classified information from the Commission, for the purpose of parliamentary oversight" around spyware exporting licenses.[37] The PEGA Committee has further called for an "EU-US spyware strategy, including a joint whitelist and/or blacklist of spyware vendors."[38]

Private Action

As news cycles continued to open with more and more NSO Group headlines, Amazon cast the first stone when it deactivated NSO Group's cloud infrastructure, claiming that NSO Group's operations violated its terms of service.[39] Action next came from WhatsApp (owned by Meta) and Apple. These companies asserted that NSO Group used their servers to hack end users' mobile devices, thereby triggering the two companies' rights of action under the federal Computer Fraud and Abuse Act (the main federal anti-hacking statute), the California Comprehensive Computer Data Access and Fraud Act, and common law breach of contract and trespass to chattels.[40]

In November 2021, the U.S. Court of Appeals for the Ninth Circuit rejected an argument made by NSO Group's advocate that it "could claim foreign sovereign immunity" on the basis that it served foreign

---

[35] PEGA Report, supra note 14, at 136.

[36] Id. at 137.

[37] PEGA Recommendations, supra note 17, at para. 63.

[38] Id. at para. 67. (The joint list will focus on vendors "whose tools have been abused or are at risk of being abused to maliciously target government officials, journalists and civil society, and who operate against the security and foreign policy of the Union, by foreign governments with poor human rights records, (not) authorised to sell to public authorities, common criteria for vendors to be included on either list, arrangements for common EU-US reporting on the industry, common scrutiny, common due diligence obligations for vendors and the criminalisation of the sale of spyware to non-state actors.")

[39] Laura Hautala, "Amazon Kicks NSO Group Activity Off Its Cloud Service After Spying Reports," *CNET*, July 19, 2021.

[40] *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, Case No. 19-cv-07123-PJH (Oct. 29, 2019), https://perma.cc/W7RB-VS23; *WhatsApp Inc. v. NSO Grp. Techs.*, 472 F. Supp. 3d 649 (N.D. Cal. Nov. 8, 2022); *Apple Inc. v. NSO Grp. Techs. Ltd.*, Case No. 3:21-cv-09078 (Nov. 23, 2021), https://perma.cc/ARB5-MHS9.

government clients. The unanimous and definitive decision of the court green-lighted the case to go to trial on the merits, at least in the WhatsApp litigation, which remains pending.[41]

These lawsuits represent a broader trend. For example, spyware victims in the United Kingdom and other European countries have sought to bring action against NSO Group and its government users in recent years.[42] This trend centers not only around NSO Group. In *Alhathloul v. Darkmatter Group*, the civil society organization Electronic Frontier Foundation brought action against Emirati spyware firm DarkMatter, along with three of its executives, former U.S. intelligence professionals, for allegedly hacking the iPhone of a prominent Saudi women's rights activist, Loujain al-Hathloul.[43]

Moratoriums and Tech Bans

UN human rights special rapporteurs,[44] civil society organizations,[45] and the country of Costa Rica[46] have all called for an immediate and global moratorium on the sale, transfer, and use of spyware technologies. The European Parliament has similarly adopted a recommendation for a global, though far narrower ban. The PEGA Committee has recommended a ban on the sale of zero-day vulnerabilities in a system, "for any purpose other than strengthening the security of that system."[47] In other words, if

---

[41] NSO Group is arguing the same sovereign immunity claim against Apple. For further analysis of this case, see Jen Patja Howell, *The Lawfare Podcast*: Orin Kerr and Asaf Lubin on Apple v. NSO Group, *Lawfare,* Dec. 3, 2021.

[42] Ronan Farrow, "A Hacked Newsroom Brings a Spyware Maker to U.S. Court," *New Yorker,* Nov. 30, 2022, https://perma.cc/UR98-69N2. The article further discusses a recent case from the Knight First Amendment Institute that was brought on behalf of employees of El Faro, a prominent news organization in El Salvador, that has been reporting on governmental corruption, and whose employees were allegedly spied on using Pegasus. See *Dada v. NSO Group*, No. 3:22-cv-07513 (N.D. Cal.).

[43] *Alhathloul v. Darkmatter*, Case 3:21-cv-01787-IM (D. Or. Por. Div.).

[44] "Spyware Scandal: UN Experts Call for Moratorium on Sale of 'Life Threatening' Surveillance Tech," UN Human Rights Council, Aug. 12, 2021, https://perma.cc/5Y4S-ZLDN (hereinafter UN Proposed Moratorium).

[45] "Joint Open Letter by Civil Society Organizations and Independent Experts Calling on States to Implement an Immediate Moratorium on the Sale, Transfer, and Use of Surveillance Technology," July 27, 2021, https://perma.cc/V7PM-KQ4Q. The letter is signed by 156 civil society organizations and 26 independent experts.

[46] "Stop Pegasus: Costa Rica Is the First Country to Call for a Moratorium on Spyware Technology," Access Now, April 13, 2022, https://perma.cc/Q2Y4-E3HN.

[47] PEGA Recommendations, supra note 17, at para. 76.

adopted, the recommendation would prohibit any trade in such vulnerabilities for law enforcement purposes.

Narrower moratoriums have already been imposed. Israel, for example, has imposed a moratorium vis-à-vis particular countries. In December 2021, under growing bilateral pressure from allies, primarily the United States and France, the Israeli Ministry of Defense announced the tightening of regulations on export controls.[48] As part of the new regulations, Israel dramatically cut the number of client countries spyware companies can potentially sell to from 110 to 37.[49] The significant decline in the number of potential buyers meant that "many Israeli spyware companies, most famously NSO [Group], have taken a severe financial hit."[50]

The Biden administration, for its part, has recently adopted a limited ban through an executive order on "Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security."[51] The executive order is limited in a number of crucial ways. First, the executive order applies only to foreign spyware companies, meaning that it explicitly excludes made-in-the-USA spyware. Second, the executive order prohibits procurement by the federal government of only that spyware which poses "significant counterintelligence or security risks to the US Government" or "significant risks of improper use by a foreign government or a foreign person."[52] Finally, the executive

[48] Judah Ari Gross, "In Wake of NSO Scandal, Defense Ministry Tightens Restrictions on Cyber Exports," *Times of Israel,* Dec. 6, 2021.

[49] Mark Mazzetti, Ronen Bergman, & Matina Stevis-Gridneff, "How the Global Spyware Industry Spiraled Out of Control," *New York Times,* Dec. 8, 2022.

[50] Id.

[51] "Executive Order on Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security," White House, March 27, 2023, https://perma.cc/9ZEM-QVCW.

[52] These risks are to be assessed on the basis of "credible information" about whether the spyware company knew or should have known about a predefined list of situations, and whether it took appropriate measures to prevent them. The situations include (a) where its tools were used against the U.S. government or data about the U.S. government was disclosed based on these tools; (b) where its tools were sold to human-rights-abusing countries (as defined by the State Department's annual human rights reports); (c) where the company misused, without authorization, data from the spyware operation; and (d) where the tools were used to collect information about activists, academics, journalists, dissidents, political figures, or members of nongovernmental organizations or marginalized communities in order to intimidate such persons, curb dissent or political opposition, otherwise limit freedoms of expression, peaceful assembly, or association, or enable other forms of human rights abuses or suppression of civil liberties; or to monitor a U.S. person, without such person's consent, in order to facilitate the tracking or targeting of the person without proper legal authorization, safeguards, and oversight. Id.

order only prohibits procurement of such spyware for operational use. It does not, however, prohibit the procurement for other uses (for example, training or research and development).

International Cooperation

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA) is a multistakeholder agreement between 42 member states that aims to voluntarily promote consistency, transparency, and accountability in the transfer and proliferation of certain kinds of dual-use goods and technologies.[53] By joining the WA, participating states seek "to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists."[54] Essentially, each member state commits to maintaining a national export control over items on the WA control list, with the understanding that decisions "to allow for or deny the export" are the pure prerogative of each state to be made "in accordance with national legislation and policies, on the basis of national discretion."[55] The other core pillar of the WA is that it provides a forum for periodic meetings, held at the WA Secretariat in Vienna, for participating states to discuss collectively the implementation and implications of various exports on their security needs.[56]

---

[53] The participating states of the Wassenaar Arrangement are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Türkiye, Ukraine, the United Kingdom, and the United States. See The Wassenaar Arrangement, "About Us," https://perma.cc/R6XC-RHB3. Given the broad political differences and ideological positions among the members, the ability to achieve consensus through this mechanism is increasingly limited. The "institutional predecessor" of the Wassenaar Arrangement was the Coordinating Committee for the Control of Multinational Trade (COCOM) established in the early days of the Cold War. "COCOM left a legacy of State-to-State cooperation and coordination regarding trade in strategically sensitive goods. Until its dissolution in 1994, COCOM States maintained a common control scheme to prohibit transfers of arms, nuclear-related products and some sensitive dual-use technologies to the Soviet bloc, specifically the Warsaw Pact countries." Heejin Kim, "Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue," *International and Comparative Law Quarterly* 70, no. 2 (2021): 387.

[54] The Wassenaar Arrangement, "About Us." Id.

[55] "A Guide to the Wassenaar Arrangement," New America, Dec. 9, 2013, https://perma.cc/FT55-S4FZ.

[56] "Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies," Fact Sheet Released by the Bureau of Nonproliferation, State Department Archive, March 22, 2000, https://perma.cc/A3EN-4ZPP.

In the wake of the Arab Spring and the reported use of repressive surveillance technologies by authoritarian regimes throughout it, negotiations commenced between WA members around the addition of certain cyber surveillance dual-use technology to the WA control list. In 2012, the members added "mobile telecommunication interception equipment," defined as technologies "used to track, identify, intercept, and record mobile and satellite phones."[57] One example of such technology is International Mobile Subscriber Identity (IMSI) catchers (often known in the United States as "stingrays"). These devices, in common use by law enforcement, act as cell towers and confuse nearby mobile phones to connect to them. Once they connect to phones, IMSI catchers can capture geolocation, traffic information, and text messages, as well as potentially "disrupt the availability of certain internet services."[58]

Another set of technologies—"intrusion software" and "IP network surveillance systems"—was added to the WA list in 2013. This addition was met with significant condemnation from technologists and human rights advocates who were worried that the two new terms were simultaneously over-inclusive and under-inclusive.[59] In particular, the worry was that certain penetration testing technologies and other tools in use by white hat hackers to enhance cybersecurity would be harder to access. At the same time, other spyware tools—the nature of which was not sufficiently captured by the definition of "intrusion software"—might end up not being regulated. Responding to these concerns, WA members negotiated and adopted "decontrol notes and technical clarifications,"[60] which sought to strike a better balance while leaving national licensing authorities with sufficient room for discretion. These notes and

[57] See Kim, supra note 53, at 389.

[58] Id.

[59] Id. at 388.

[60] Id. See also Garrett Hinck, "Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research," *Lawfare,* Jan. 5, 2018.

clarifications were later implemented by both the European Council and Parliament[61] and the U.S. Commerce Department's Bureau of Industry and Security.[62]

But there is also a different solution on the table for advancing international cooperation, one that looks not to amend the WA, but to supplement it. As part of the 2023 NDAA, Congress instructed the DNI to produce a report "on the potential for the United States to lead an effort to devise and implement a common approach with allied countries as the Director determines appropriate, including the Five Eyes Partnership, to mitigate the counterintelligence risks posed by the proliferation of foreign commercial spyware."[63]

This instruction builds on existing efforts initiated by the State Department. At the first Summit for Democracy in December 2021, the United States, together with Australia, Denmark, and Norway (and with support from Canada, France, the Netherlands, and the United Kingdom), announced the Export

---

[61] European Parliament and Council Regulation 2021/821, "Setting Up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit, and Transfer of Dual-Use Items" (Recast), 2021 *Official Journal of the European Communities* L 206 (June 11, 2021). As Kim explains, "after prolonged negotiations between the European Commission, Parliament, and Council, compromise over the text of the proposed amendments was finally reached in November 2020" and adopted in 2021 (see Kim, supra note 53, at 406). As part of this negotiation, many EU members "repeatedly expressed reluctance to go beyond what had been agreed multilaterally at Wassenaar. They made it clear that the unilateral expansion of export controls on cyber surveillance items was unacceptable, and that until such a time comes, the EU should not work 'in isolation'. In other words, the EU control list should continue to be maintained through incorporating the control lists of international agreements, including the Wassenaar Arrangement." Id. at 410. What drove this legislative attitude was the understanding that "[t]he human rights-oriented recast of the export control regime would create stricter restrictions on cyber surveillance technology, and with such an approach, the EU might lose business competitiveness over other leading States—especially the US and China." Id.

[62] Information Security Controls: Cybersecurity Items, 86 Fed. Reg. 58,205, Oct. 21, 2021, https://perma.cc/3NDN-JA5E. The supplementary information to the rule clarifies that it is aimed at implementing the Wassenaar Arrangement negotiations. It goes on to describe the three biggest changes adopted in the amendments, which sought to address concerns of both over- and under-inclusion in the original definitional text: "There were three significant changes: First, using 'command and control' in the control language for both hardware and software addressed concerns from cybersecurity companies to more specifically control tools that can be used maliciously. Second, adding a note to the control entry for technology for the 'development' of 'intrusion software' that excludes from the entry 'technology' that is exchanged for "vulnerability disclosure" or "cyber incident response". Third, adding a note to the 'software' generation, command and control, or delivery entry that excludes from this entry products designed and limited to providing basic software updates and upgrades."

[63] See NDAA FY23, supra note 29, at 1127.

Controls and Human Rights Initiative.[64] The goal of this initiative is to develop "a written code of conduct intended to guide the application of human rights criteria to export licensing policy and practice"[65] and to "build[] policy alignment with likeminded partners that leads to common action, and concrete and practical outcomes."[66]

Most recently, in March 2023, following the second Summit for Democracy, the United States joined Albania, Australia, Bulgaria, Canada, Costa Rica, Croatia, Czechia, Denmark, Ecuador, Estonia, Finland, France, Germany, Japan, Kosovo, Latvia, the Netherlands, New Zealand, North Macedonia, Norway, the Republic of Korea, Slovakia, Spain, and the United Kingdom as part of an Export Controls and Human Rights Initiative.[67] Together, this consortium of states adopted a "Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights."[68] The code itself uses relatively vague terms and is quite aspirational.[69] But it is a first step toward a broader framework. In fact, the countries all agreed to "hold

---

[64] "Fact Sheet: Export Controls and Human Rights Initiative Launched at the Summit for Democracy," White House, Dec. 10, 2001, https://perma.cc/RQA2-8M49.

[65] Id.

[66] Id. at 1124. Similarly, the U.S.-EU Summit in June 2021 concluded with a set of commitments for further development of "shared principles and areas for export control cooperation." These commitments included "capacity building assistance to third countries to support multilateral export control regimes, prior consultations on current and upcoming legislative and regulatory developments and developing convergent control approaches on sensitive dual-use technologies." "Fact Sheet: U.S.-EU Establish Common Principles to Update the Rules for the 21st Century Economy at Inaugural Trade and Technology Council Meeting," White House, Sept. 29, 2021, https://perma.cc/8BCJ-5YRY.

[67] "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware," White House, March 30, 2023, https://perma.cc/T83M-J559; Department of State, Office of the Spokesperson, "Export Controls and Human Rights Initiative Code of Conduct Released at the Summit for Democracy," March 30, 2023, https://perma.cc/46EA-5P4Q.

[68] "Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights," State Department, March 30, 2023, https://perma.cc/RG5Z-DU9A.

[69] "The Code of Conduct calls for Subscribing States to: [1] Take human rights into account when reviewing potential exports of dual-use goods, software, or technologies that could be misused for the purposes of serious violations or abuses of human rights; [2] Consult with the private sector, academia, and civil society representatives on human rights concerns and effective implementation of export control measures; [3] Share information with each other on emerging threats and risks associated with the trade of goods, software, and technologies that pose human rights concerns; [4] Share best practices in developing and implementing export controls of dual-use goods and technologies that could be misused, reexported, or transferred in a manner that could result in serious violations or abuses of human rights; [5] Encourage their respective

ongoing meetings, either annually or as otherwise agreed" in order to "further develop the workings of the Code of Conduct" and to "[d]esignate a national point of contact" for inquiries about domestic export control procedures and implementation of the code of conduct.[70]

EXPLAINING THE LIMITS OF EXISTING PROPOSALS AND ACTIONS

This paper has so far described the wide array of policy responses that have been taken or recently proposed to address the risks from the trade in commercial spyware. Combined, these measures demonstrate a growing commitment by members of the international community to seriously respond to the threat of spyware. In fact, one scholar, Joseph Devanny, has recently suggested that we have entered a "transitional point in the relationship between states and commercial spyware."[71] What has triggered this transitional phase we find ourselves in? The cynic in me would suggest that recent revelations about the use of spyware against heads of state has at least something to do with it.[72] Regardless of the reason, this recent trend increases the likelihood that meaningful change could be achieved in the near future.

Nonetheless, I argue that, to date, none of the actions taken nor the proposals made is sufficient to curtail the harms of commercial spyware. In this section I discuss the pitfalls of each of the existing measures, setting up, in the next section, the case for the need for a new binding international instrument.

Industry Self-Regulation Is Not a Solution

We should be suspicious about the ability of spyware companies to self-regulate. As already discussed, international norms like the UNGPs and the OECD MNE Guidelines are soft law instruments whose

---

private sectors to conduct due diligence in line with national law and the UN Guiding Principles on Business and Human Rights or other complementing international instruments, while enabling non-subscribing states to do the same; [6] Aim to improve the capacity of States that have not subscribed to the Code of Conduct to do the same in accordance with national programs and procedures." Id.

[70] This position was similarly promoted by the PEGA Committee, which has called for "the EU-US Trade and Technology Council to hold wide and open consultations with civil society for the development of the joint EU-US strategy and standards, including the joint whitelist and/or blacklist" as well as "talks to be launched with other countries, in particular Israel, to establish a framework for spyware marketing and export licences, including rules on transparency, a list of eligible countries regarding human rights standards and due diligence arrangements." See PEGA Recommendations, supra note 17, at paras. 68–69.

[71] Joe Devanny, "Pegasus in Downing Street? Commercial Spyware and Espionage Competition," *The National Interest,* April 27, 2022.

[72] See, e.g., "France's Macron Targeted in Project Pegasus Spyware Case - Le Monde," *Reuters*, July 21, 2021; Bethan McKernan, "Emmanuel Macron 'Pushes for Israeli Inquiry' Into NSO Spyware Concerns," *The Guardian,* July 25, 2021.

success depends on strong domestic implementation.[73] Without such legislation and supporting enforcement, any promise of corporate social responsibility in the spyware industry is aspirational at best.[74]

Take, for example, the State Department's Due Diligence Guidance. The guidance is purely voluntary.[75] Both the guidance and the UNGPs seek to implement a formal institutional structure that could be utilized to confirm corporate compliance with the commitments or to hold a spyware company to account whenever it fails to meet them. Moreover, the Due Diligence Guidance is not comprehensive enough. This is because the guidance is not meant to address commercial spyware per se but, rather, is intended to capture a broader category of companies, covering any "product or service with intended or unintended surveillance capabilities."[76] The guidance is clear about this, noting that the different measures that it introduces "will be more or less relevant depending on the industry sector and type of product or service."[77] So not only do we have nonbinding instruments, but even when we try to comply with the instruments, they are insufficiently tailored to address the full scope of human rights risks posed by the spyware industry.

---

[73] Anna Triponel, "When Soft Law Is Not So Soft: The Rapid Legalisation of Business and Human Rights," Triponel Consulting, Oct. 14, 2019, https://perma.cc/8DBN-54WD.

[74] "Direct approaches to the voluntary responsibility of corporations developing and selling the technology rely upon the UN Guiding Principles, which are affected by the absence of a binding enforcement arm, with the most sophisticated oversight regime (the OECD NCP system) rendered toothless through its inability to compel evidence or oblige engagement." United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, "Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach," April 2023, https://perma.cc/F6QJ-ZN8A, 84 para. 122 (hereinafter UN Special Rapporteur on Counterterrorism Position Paper on Spyware).

[75] Triponel, supra note 73.

[76] See Due Diligence Guidance, supra note 24, at 5 (For the purpose of this document, "product or service with intended or unintended surveillance capabilities" [also referred to as "product(s) or service(s)" in this document] is defined as a product or service marketed for or that can be used (with or without the authorization of the business) to detect, monitor, intercept, collect, exploit, preserve, protect, transmit, and/or retain sensitive data, identifying information, or communications concerning individuals or groups."). The guidance goes on to list a set of examples of relevant products and services, including sensors, biometric identification, data analytics, internet surveillance tools, non-cooperative location tracking, and recording devices. Id. at 6.

[77] Id. at 6. For example, the issue of vulnerabilities hoarding and trade, and the equities process associated with it—a topic of particular concern in commercial spyware regulation—is not mentioned in the guidance nor sufficiently addressed in the general commitments.

There is a broader problem, one that has to do with the lack of an incentive structure for the companies to comply with human rights norms. Due to the secrecy surrounding the practice, and the plausible deniability attached to such secrecy, a process of norm internalization and follow-on enforcement by the companies is hard to achieve in the context of spyware regulation. Take NSO Group, for example. The company publicly "committed to the authoritative international standards"[78] of the UNGPs and affirmed that it has implemented "policies towards complete alignment" with those guiding principles.[79] We now know that NSO Group did not in fact meet any of its commitments. While NSO Group has been the subject of significant enforcement action, how many more companies might be claiming human rights compliance as a marketing scheme while secretly violating the rules with impunity? The same is also true for NSO Group's June 2021 transparency and responsibility report.[80] That report was the first of its kind for the industry. But it was far from an accomplishment worth celebrating. Indeed, Amnesty International called the report "a sales brochure" and "yet another missed opportunity."[81]

There is now a large body of literature available to explain when, how, and why corporate self-regulation fails.[82] As Karen Yeung explains:

> Businesses cannot be relied on to regulate themselves (except in very limited circumstances). The reasons are simple: Firms lack sufficient incentives to set, comply with, police and punish violations of their own standards, and markets cannot ensure that firms will behave with integrity. The ability of markets to provide effective oversight relies on consumers having the information and capacity to evaluate the quality of goods and services. Yet businesses can utilize their technological prowess and superior knowledge to evade detection.[83]

All of these elements are especially visible in the spyware market, where acts of self-restraint are perceived as corporate self-sabotage. So long as there is at least one company operating from one

[78] "Transparency and Responsibility Report 2021," NSO Group, June 30, 2021, https://perma.cc/BJ5R-23RN, 8 (hereinafter NSO Group's Transparency Report).

[79] Id. at 5.

[80] Id.

[81] "NSO Group's New Transparency Report Is 'Another Missed Opportunity'," Amnesty International, July 1, 2021, https://perma.cc/KAG8-6S6T.

[82] See, e.g., Christopher D. Stone, *Where the Law Ends: The Social Control of Corporate Behavior* (Harper & Row, 1975); Ans Kolk & Rob van Tulder, "The Effectiveness of Self-Regulation: Corporate Codes of Conduct and Child Labour," *European Management Journal* 20 (2002): 260; Jodi L. Short & Michael W. Toffel, "Making Self-Regulation More Than Merely Symbolic: The Critical Role of the Legal Environment," *Administration Science Quarterly* 55 (2010): 389.

[83] Karen Yeung, "Very Few Businesses Can Be Trusted," *New York Times,* Nov. 10, 2015.

territory in which export control restrictions and due diligence obligations are lax, all other companies will race to the bottom, generating the lowest common denominator of standards. This is because the more human rights restrictions a company imposes on itself, the less likely it is to find buyers who would be willing to tolerate the additional precautions, since there is an equivalent product on the market without those restrictions.

Private Action, Ad Hoc Enforcement, and Sanctions Are Only a Partial Solution

There is no question that blacklisting and litigation by victims and administrative agencies are helpful tools in the broader enforcement toolbox against recalcitrant surveillance corporations. But these tools by their very nature are relevant only *after* the harm has been felt. They require information about abuses to first surface before meaningful action could be taken. Yet as the PEGA Committee explained:

> For most victims it is not possible to get any information about their case from the authorities. In many cases the authorities refer to national security grounds as justification for secrecy, in other cases they simply deny the existence of a file, or the files are destroyed. At the same time, prosecutors frequently refuse to investigate these cases, arguing that the victims do not have sufficient evidence. This is a vicious circle that leaves victims without recourse. Governments most often refuse to disclose whether they have bought spyware and what type. Spyware vendors equally refuse to disclose who their customers are. Governments often resort to middlemen, proxies or personal connections, to purchase commercial spyware or spyware-related services, so as to conceal their involvement. They circumvent procurement rules and budget procedures, so as to not leave any government fingerprints.[84]

But secrecy is only one concern. The effectiveness of ad hoc litigation and enforcement is routinely debated as well. Civil litigation depends on standing requirements and the codification in statute of particular torts, especially where the common law privacy torts and trespass to chattel fail to capture the harms suffered. Indeed, "domestic law doctrines of tort/delict form an inconsistent patchwork, with ample room for argument about degrees of responsibility along transnational production chains, how human rights harms equate to (or diverge from) traditional models of physical harm, and how relationships between private entities and foreign sovereign entities ought to be dealt with."[85] Relying on tort law as a means of enforcement and deterrence-generation also raises evidentiary challenges to litigants trying to prove the facts under a preponderance-of-the-evidence standard.

---

[84] PEGA Report, supra note 14, at 144.

[85] See UN Special Rapporteur on Counterterrorism Position Paper on Spyware, supra note 74, at 84, para. 123.

While the industry is plummeting headfirst into a bottomless pit, the European Parliament is set to adopt a set of recommendation that would replace voluntary self-regulation with mandatory regulation. Among other things, such regulation should compel spyware companies to "comply with strict due diligence requirements,"[86] adopt policies around disclosures to national supervisory authorities of the nature and scope of their exports,[87] and set a "cooling-off period, temporarily preventing former employees of governmental bodies or agencies from working for spyware companies."[88] For the time being, however, such regulations have not taken hold; and even if adopted by the European Parliament, it remains to be seen whether EU members will agree to import such regulation into their domestic systems.

Not only that, but even if robust regulation was there, enforcement through sanctions does not guarantee success in achieving efficient levels of deterrence. Indeed, the commercial spyware industry is booming, with an estimated global worth of $12 billion.[89] These companies are extremely resilient. When a company becomes insolvent or gets blacklisted, many others quickly step in to take its place,[90] while the sanctioned company in turn gets bought out, merges with another company, or rebrands. The fact that NSO Group is still standing today, despite the draconian sanctions imposed on it, is an example of this resiliency.

Moratoriums Are Not a Solution

There are some misconceptions about moratoriums. To be clear, no organization or expert that I am familiar with has ever called for a complete and total ban on the commercial spyware industry. In fact, all of the proposals for moratoriums made so far were conditional, at least formally. Their advocates envision a restoration of business once regulations have been put into place that could guarantee "compliance with international human rights standards."[91]

Nevertheless, none of these organizations and human rights experts has ever proposed what a human-rights-compliant design and use of spyware could even look like. There is something disingenuous about calling for a *temporary* moratorium—subject to an ultimate human-rights-protecting legal framework—

[86] PEGA Recommendations, supra 17, at para. 39.

[87] Id. at para. 40.

[88] Id. at para. 41.

[89] Mazzetti et al., supra note 49.

[90] Id. (Referring to the Biden administration's decision to blacklist NSO Group and noting that "the use of spyware continues to proliferate around the world, with new firms — which employ former Israeli cyberintelligence veterans, some of whom worked for NSO — stepping in to fill the void left by the blacklisting.")

[91] See, e.g., UN Proposed Moratorium, supra note 44.

when no one who calls for the moratorium is willing to commit to the work of developing that very framework. In fact, I would argue that those who call for a temporary moratorium secretly harbor the sense that no framework would ever be good enough. In other words, what is being proposed is for all intents and purposes a complete and indefinite ban, since no one assumes that a human-rights-compliant framework could be designed.[92]

A notable exception is the excellent work produced by the UN special rapporteur on counter-terrorism and human rights, Fionnuala Ní Aoláin. In a 2023 position paper, she began to scope "proposals for a human-rights complaint approach."[93] The document provides the most detailed account, to date, that I am familiar with that tries to imagine a pragmatic framework for the design and use of spyware.

---

[92] David Kaye, the former special rapporteur for freedom of expression and one of the staunchest advocates for a moratorium, has acknowledged that, in an ideal world, that is precisely what he would like to see: "[I]t's time to begin speaking of not merely a moratorium but a ban of such intrusive technology, whether provided by private or public actors. No government should have such a tool, and no private company should be able to sell such a tool to governments or others." At the same time, however, even he acknowledges that such a ban is very unlikely to materialize and that new creative and more nuanced solutions need to be considered. As he writes: "In the land of reality, however, a ban will not take place immediately. Even if a coalition of human rights-friendly governments could get such negotiations toward a ban off the ground, it will take time. Here is where bodies like the European Parliament and its PEGA Committee—and governments and parliamentarians around the world—can make an immediate difference. They should start to discuss a permanent ban while also entertaining other interim approaches: stricter global export controls to limit the spread of spyware technology; commitments by governments to ensure that their domestic law enables victims of spyware to bring suits against perpetrators, whether domestic or foreign; and broad agreement by third-party companies, such as device manufacturers, social media companies, security entities and others, to develop a process for notification of spyware breaches especially to users and to one another." See David Kaye, "Here's What World Leaders Must Do About Spyware," Committee to Protect Journalists, Oct. 13, 2022, https://perma.cc/DRU5-KNGJ.

[93] UN Special Rapporteur on Counterterrorism Position Paper on Spyware, supra note 74. The position paper establishes a set of mandatory and minimum features that must be incorporated into any human-rights-compliant spyware technology. The spyware must "(a) allow for users to specifically target certain data and metadata, rather than automatically monitor and record all data and metadata; (b) avoid automatically accessing data relating to contacts of targeted individuals, unless users specifically require that additional information for investigative purposes; (c) engineer mechanisms to prevent harmful use, such as flagging systems and 'kill switches' in cases of apparent misuse; and, in any event, (d) create an indelible, permanent, and uneditable auditable record of what actions have been taken by the user of the spyware, including any interferences/modifications of data/ metadata, when those occurred, and by whom they were effected so that the use of the tool can be verified, and its human rights compliance assessed after the fact by judicial authorities. Part of that indelible and uneditable record must be some form of identifier or watermark such that judicial authorities overseeing complaints may verify the producer of spyware alleged to have been used against a victim and the customer to which that spyware was originally supplied and, from such source, can

But until such a framework is adopted, endorsed, and embraced, the interim period entails a long-lasting moratorium. There are two primary reasons why a complete and near-permanent ban on the industry is unfeasible and impractical. First, commercial spyware offers a needed solution to law enforcement and intelligence agencies operating in an increasingly encrypted communications environment.[94] In this new environment, "encryption poses real challenges for public safety officials" as it hinders their ability to access timely evidence and "to effectively and efficiently protect society" from serious crime.[95] Regardless of whether law enforcement has completely "gone dark" in this new age,[96] it is clear that the negative impacts that encryption has had on investigations merit a technological and regulatory response.

If spyware was not available to them, law enforcement would have imposed the requirements that backdoors be designed by software vendors and would further compel the assistance of those vendors. But such measures introduce too great a risk to cybersecurity and innovation.[97] So we would be right to call on law enforcement to give up their calls to vendors to adopt such exceptional access-by-design. But we can't simultaneously tie the hands of law enforcement in this way and then also forbid them from seeking the use of spyware as an alternative solution. "Lawful hacking" must be part and parcel of the investigative arsenal of contemporary law enforcement,[98] for how else can we expect them to fight against serious crime and bring perpetrators to justice?

---

compel disclosure of the auditable record such that the legality of any use complained of can be adequately reviewed." Id. at 86, para. 126.

[94] See, e.g., Susan Landau and Asaf Lubin, "Examining the Anomalies, Explaining the Value: Should the USA FREEDOM Act's Metadata Program Be Extended?" *Harvard National Security Journal* 11 (2020): 308, 340–342 (discussing how evolving methods of terrorist communications, including through the use of end-to-end encrypted and self-destructing IP-based applications, has impacted investigative efforts of law enforcement and the intelligence community).

[95] Jim Baker, "Rethinking Encryption," *Lawfare,* Oct. 22, 2019.

[96] See supra note 3 and accompanying text.

[97] Harold Abelson et al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity* 1, no. 1 (2015): 69, 70 (suggesting that designing communications systems for exceptional access (through mandatory backdoors) "would pose far more grave security risks, imperil innovation, and raise thorny issues for human rights and international relations").

[98] See Hennessey, supra note 3 ("Lawful hacking is a necessary, though possibly not sufficient, element of a workable solution without mandated exceptional access. Therefore, lawful hacking should be viewed as the central element of a comprehensive alternative strategy, which includes investments in using metadata and the emerging Internet of Things to offset the losses to communication content that make up the going dark problem."). See also Rozenshtein, supra note 1, at 1210 ("[L]awful hacking will remain indispensable to investigations into criminal activity on the 'dark web.' It will also be an important tool where suspects use

Equally problematic is the increasing role that authoritarian governments are playing in exporting surveillance technologies. A moratorium on surveillance tech by advanced democracies will not end the trade in spyware. Instead, it will open new opportunities and markets for authoritarian governments, which obviously will not sign on to the regime, further promising even less regulation or oversight. China, for example, relies on the spyware trade to increase its diplomatic hold over countries in the Global South, particularly in African countries such as Uganda and Zambia.[99] Such trade helps China's global strategy, both by exporting its model of authoritarian surveillance and by intensifying the major powers competition.[100] For countries such as Russia and Iran, the spyware trade is conducted, in part, in order to resist and defy international sanctions regimes.[101] A ban on trade in spyware by democratic countries could thus only further increase human rights abuses rather than decrease it.

So we need to accept that spyware is here to stay, and as Alan Rozenshtein has noted, the "best we can often do is to put forward partial proposals and focus on minimizing their flaws, in the hope that, flaws and all, they will nevertheless represent an incremental improvement over where things stand today."[102] This kind of pragmatism and abandonment of purism was also embraced by Ní Aoláin in her role as special rapporteur and is the only way forward.[103] As explained by Devanny:

> [W]hilst the fates of a single company like NSO Group can rise and fall, it is very difficult to see the wider industry enjoying anything other than continued success. States are not going to stop wanting to spy on each other, or on other, non-state targets. The market that has grown to cater to this perennial state practice is too valuable, too globally

---

products or services that are outside the scope of any exceptional-access mandates (for example, one of the many internationally produced secure messaging services).").

[99] See, e.g., Joe Parkinso, Nicholas Bariyo, & Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal,* Aug. 15, 2019.

[100] See, e.g., Khwezi Nkwanyana, "China's AI Deployment in Africa Poses Risks to Security and Sovereignty," Australian Strategic Policy Institute, May 5, 2021, https://perma.cc/W533-FU6W.

[101] See, e.g., Alena Popova, "Russia Exports Digital Surveillance, Despite Sanctions," Center for European Policy Analysis, Aug. 26, 2022, https://perma.cc/XM84-THGW; Karen Freifeld, "U.S. Accuses Huawei of Stealing Trade Secrets, Assisting Iran," *Reuters*, Feb. 13, 2020.

[102] See Rozenshtein, supra note 1, at 1210.

[103] See UN Special Rapporteur on Counterterrorism Position Paper on Spyware, supra note 74, at 86, para. 129 (Where she notes her proposals for a new regulatory framework "should neither be considered an endorsement of the trade in, or use of, spyware, nor a non-endorsement of the calls by various civil society voices and human rights experts for an outright ban on the use of spyware. While the Special Rapporteur notes the force of those calls, the reality is that while such measures are debated and considered, the use of, and trade in, spyware technology continues, and the existing patchwork of controls discussed in this paper fail adequately to prevent the widespread violations of human rights which result.").

> dispersed, and likely also too covert to be readily amenable to collective, verifiable efforts to curb it. And, in the absence of effective constraints, commercial spyware will continue to level the playing field between state actors in the competition for intelligence gains. This will create both opportunities to be exploited and challenges that must be overcome—an ever-present feature of intelligence competition between states throughout history.[104]

Existing International Cooperation Frameworks Are Not Enough

Moratoriums, self-regulation, and ad hoc litigation and sanctions are not meaningful solutions in the regulation of spyware. The only meaningful solution can come from international collaboration and cooperation. If the industry suffers from a weak-link problem, as I have suggested—whereby the quality of the overall industry depends on how good the worst corporate actor within it behaves—then international standardization is the only way forward.

So far, that standardization has been limited to the amendment process of the WA. Yet the WA "has been the subject of increasing criticism from academics and policymakers who argue that it is ineffective at addressing the proliferation of dual-use technology."[105] First, because the WA is a nonbinding arrangement, "non-compliance by a participating State does not constitute a breach of an international obligation."[106] Second, several key players in the commercial spyware space, including China, Israel, Cyprus, the United Arab Emirates, and Belarus, are not parties to the WA.[107] Their non-participation opens a potential export control loophole.[108] Third, the WA does not prohibit the purchase

---

[104] See Devanny, supra note 71.

[105] Jamil Jaffer, "Strengthening the Wassenaar Export Control Regime," *Chicago Journal of International Law* 3, no. 2 (2002): 520. See also Mailyn Fidler, "Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis," *I/S: A Journal of Law and Policy for the Information Society*, 11 (2015): 466 ("The WA has been criticized for weakness and ineffectiveness and critiqued by developing countries as a way for developed nations to maintain a high technology monopoly.").

[106] Roland Klein, Scenario 26: Export Licensing of Intrusion Tools, Cyber Law Toolkit, https://perma.cc/B5SY-ZD4S.

[107] A number of these countries, such as Israel, China, and Singapore, "have domestic legislation that partially incorporates the list of goods and technologies identified by the arrangement." See Kim, supra note 53, at 387.

[108] For example, in the context of China, the Standing Committee of China's legislature, the National People's Congress, passed the Export Control Law, which went into effect on Dec. 1, 2020. For a summary of this law, see Karen M. Sutter, "China Issues New Export Control Law and Related Policies," Congressional Research Service, Oct. 26, 2020, https://perma.cc/5NLL-QJ4G. As Kim writes, while China "seemed to perceive that global standard setting and cooperation to restrict controlled items under the

of surveillance technology from a nonparticipating state. For example, the import of Pegasus spyware from a nonparticipating country, like Israel, into the EU is permitted under the WA and demonstrates one of its weaknesses.

For all of these reasons, the PEGA Committee has recently called for the WA "to become a binding agreement on all its participants, with the aim of making it an international treaty."[109] The committee further called on key players in the spyware trade, namely Israel and Cyprus, "to become participating states of the Wassenaar Arrangement."[110] Finally, the PEGA Committee stressed the need to introduce into the WA a "human rights framework that embeds the licensing of spyware technologies [and] assesses and reviews the compliance of companies producing spyware technologies." The PEGA Committee also argued that "participants should prohibit the purchase of surveillance technologies from states that are not part of the arrangement."[111]

I see value in these proposals, and yet it is extremely unlikely that all WA members states will agree to such a dramatic reorientation of this instrument. For one thing, the WA is a framework that deals with all dual-use technologies and is not limited to spyware. Even member states that might have an interest in regulating spyware would be worried about endangering a long-standing framework that served far broader functions for the international community. In the final section of this paper I therefore begin to sketch the contours of a new international framework tailored for the spyware industry that may offer an innovative alternative for enhancing standardization across the marketplace.

THE CASE FOR A MULTISTAKEHOLDER STANDARDIZATION AND ACCREDITATION MODEL

Ní Aoláin, in her role as special rapporteur, has concluded that the way forward for spyware regulation is the development of a novel international framework that "avoids the gaps in the existing patchwork of purported oversight and accountability methods."[112] Little scholarship has sought to promote such a framework. Here and in forthcoming work,[113] I try to do just that.

---

auspices of Wassenaar were essential to (or at least not contrary to) its national security interests," the adopted law "is flimsy" in its implementation of the Wassenaar Arrangement. See Kim, id. at 413.

[109] See PEGA Recommendations, supra note 17, para. 54.

[110] Id. at para. 55.

[111] Id. at para. 56.

[112] See UN Special Rapporteur on Counterterrorism Position Paper on Spyware, supra note 74, at 85, para. 125.

[113] See Asaf Lubin, *Selling Surveillance,* Indiana Legal Studies Research Paper No. 495 (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323985.

The insights gleaned from the first two sections of this paper can now serve as the foundation for the development of this new framework. First, the framework must be legally binding on both participating governments and companies, given that voluntary frameworks such as the UNGPs, the State Department Due Diligence Guidance, and the Wassenaar Arrangement will not work.

Second, the framework must include a mechanism through which violating companies and countries could address grievances and where greater accountability can be reached. Such a mechanism will need to take into account the inherent secrecy built into the practice of spyware. It will need to respect the proprietary rights of the industry and the national security concerns of the state parties while prioritizing accountability. The framework will thus strike a balance between preserving some degree of confidentiality and welcoming members of the civil society who can ensure a check on the governments and the companies involved.

What makes my proposal unique is that it also emphasizes the need to ban the privatization of zero-day hoarding. To understand this point, we need to take a step back and understand the benefits and risks associated with zero-day hoarding.

The Case for Banning the Privatization of Zero-Day Hoarding

Governments want to keep zero-days, because they are the most effective tool for engaging in lawful hacking. Governments want to disclose zero-days to companies, because malicious actors could equally use these vulnerabilities to target the government. Disclosure would mean fixing in the form of a patch that could be installed automatically through a software push.

The decision whether to hoard and use, or disclose and fix, is one vested with the government. It requires a complex balancing act that takes into account nuanced and complex issues of public policy. Even when a particular vulnerability is hoarded, the number of times it should be used is also a question of public policy. We want to hoard exploits and use them only when national security is truly on the line. This is because the more they are used, the more likely they are to be discovered and then either be patched (and thereby lose effectiveness) or, worse, be misused by one of our adversaries against us.

To accommodate the process of balancing the equities, some countries have developed public vulnerabilities equities processes (or VEPs).[114] The VEP "outlines the procedure through which the government weighs various considerations in determining when to disclose software vulnerabilities and when to exploit them for law enforcement or foreign intelligence purposes. Disclosure enables the involved company or entity to patch for that vulnerability and protect users' cybersecurity."[115] But

[114] See "Vulnerabilities Equities Policy and Process for the United States Government," White House, Nov. 15, 2017, https://perma.cc/6WLA-N686; "The Equities Process," U.K. Government Communications Headquarters, Dec. 12, 2022, https://perma.cc/GXM5-U245.

[115] Andi Wilson Thompson, "Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter," *Lawfare,* Jan. 13, 2021.

disclosure also entails that the vulnerability will be denied from use by the government for national security purposes. Here is where the "equities" lie, as different agencies within the government would have different motivations for retaining or disclosing a particular vulnerability.

Here lies a crucial finding. If you support the right of spyware companies to hoard vulnerabilities, you are essentially bypassing the entire VEP. What is the point of having an equities process if a country can simply sidestep it by buying commercial spyware from a foreign vendor? Unlike the government, commercial spyware companies, which enter the zero-day market, are not required to engage in any bureaucratic process before they decide whether to hoard or disclose a particular vulnerability. Government procurement of an off-the-shelf product is equally not subject to the VEP. Therefore, the more we allow commercial actors to possess these tools and profit from zero-days, the more we corrupt and degenerate the VEP. Instead of the equities being debated by government officials, elected to their posts and accountable to the public, they are decided in boardrooms by business moguls who care only about shareholder interests and their own bottom lines.

My suggestion isn't therefore that we put a moratorium on the trade in zero-day vulnerabilities like the European PEGA Committee has supported.[116] Rather, all we need is to restrict the privatization of that decision-making process. Specifically, through licensing schemes in the development phase of the spyware, the government should compel military-grade spyware companies to either participate in the VEP process or share with VEP representatives early information about the vulnerabilities found.

The CSAS Model: Institutional Structure

Since a significant focus of the CSAS model is a ban on the decision-making process concerning the privatization of zero-day hoarding, the model draws much of its inspiration from a parallel instrument. In the 1990s and early 2000s, the international community saw a different challenge relating to the privatization of national security activity: private military and security companies (PMSCs). These PMSCs were involved in indiscriminate shooting of civilians, property damage, sex trafficking, and cruel and inhuman treatment, with limited accountability.[117] Similar to the spyware case, one of the core reasons for the lack of accountability was "the absence of a clear legal framework to govern the conduct of multinational [PMSCs]."[118] In fact, spyware companies and PMSCs also share secrecy in common. That secrecy made PMSCs "more likely to commit transgressions."[119]

---

[116] See supra note 47 and accompanying text.

[117] See Evgeni Moyakine, *The Privatized Art of War: Private Military and Security Companies and State Responsibility for Their Unlawful Conduct in Conflict Areas* (Intersentia, 2015), 10–32.

[118] Reema Shah, "Comment: Beating Blackwater: Using Domestic Legislation to Enforce the International Code of Conduct for Private Military Companies," *Yale Law Journal* 123 (2014): 2562.

[119] Id. at fn. 15.

Following years of negotiations and diplomatic efforts, an international framework was adopted, known as the International Code of Conduct for Private Security Service Providers (ICoC). The ICoC is "now regarded as the most comprehensive initiative setting standards for the industry."[120] This initiative, originally launched by the government of Switzerland, aims "to raise private security industry standards and practices that respect human rights and international humanitarian law and to engage with key stakeholders to achieve widespread adherence to its Code globally."[121] To support the ICoC, in September 2013 an association (the ICoCA) was launched as an oversight mechanism for the code:[122]

> [The ICoCA] is led by a Board of Directors empowered to monitor and certify the compliance of signatory companies. The Board is chosen by the vote of all members and consists of twelve individuals, with four members coming from [PMSCs], four from civil society organizations, and four from states. ICoCA's charter calls for in-field assessments of company practices and consultation between the Board and companies whose practices are found to violate the Code. It also establishes a complaint procedure through which allegations of misconduct can be reported.[123]

With the U.S. State Department, the United Kingdom, and the United Nations all making "government contract awards contingent on company membership in ICoCA[,]"[124] the regime has been lauded by "States and human rights organizations … as a groundbreaking step in regulating the industry."[125] The regime is far from perfect, however. The ICoCA's "effectiveness is limited because it lacks a viable enforcement mechanism."[126] The ICoCA does not possess "a judicial body or forum where [PMSCs] can be held accountable if they persist in violating norms," and this "makes adherence to the Code largely voluntary."[127] Moreover, the regime has seen a significant decline in the number of participating states and companies.[128] For its 2019–2023 strategic plan, the ICoCA sought to "diversify and expand

---

[120] See Moyakine, supra note 117, at 141.

[121] "About Us," International Code of Conduct Association, https://perma.cc/97PH-KFCA.

[122] See Shah, supra note 118, at 2654.

[123] Id.

[124] Id. at 2565.

[125] Id. at 2564.

[126] Id. at 2563.

[127] Id. at 2564.

[128] Christopher Kinsey & Christopher Mayer, "A Step Too Far: How the ICoCA Actions Could Unintentionally Help to Privatise War (Part One)," Defense in Depth, Jan. 31, 2022 ("[P]articipation in the ICoC has been less successful than the initial enthusiasm for the Code might have suggested. At its height, only 115 Private Security Companies were members and, as of December 2021, membership stood at just 66

ICoCA's Membership among companies, governments and civil society." That has not yet happened in any meaningful way.

The international accreditation and certification model that I am proposing thus builds on the ICoCA experience and improves it. The Commercial Spyware Accreditation System would be a multistakeholder framework that brings together governments, spyware companies, and civil society (acting as observers). The CSAS would be built around an international agreement that would be open to signature by both governments and companies. Parties to the agreement would take upon themselves a set of legally binding obligations, which would differ between governments and companies.

The CSAS would be run by a board of directors, chosen by the vote of all members, with some members coming from the spyware companies, some from civil society organizations, and some from the member states. The board would have two primary functions. First, it would review requests by new companies to either join the CSAS or renew their membership. As part of this review, the board would assess whether the company is in compliance with its obligations under the agreement. Second, the board would serve as an appeals instance to decisions made as part of the CSAS grievance mechanism.[129]

The CSAS grievance mechanism would consist of national contact points (NCPs) in each of the member states. This grievance mechanism is based on the NCP model adopted under the OECD MNE Guidelines.[130] All NCPs should have security clearance and likely prior work experience in the intelligence community of the member state. These NCPs would operate with the goal of furthering the effectiveness of the CSAS model. This entails a primary responsibility to advise participating companies and collaborate with civil society. The NCPs will further serve as a grievance mechanism. Any entity—an individual, an organization, a community, or a government—with an interest in the matter may report issues related to CSAS implementation to a national NCP. NCPs may collaborate with other NCPs, where such are involved, and proceed where appropriate to facilitate dialogue, either conciliation or mediation between the relevant parties in closed doors and subject to rules of confidentiality. Finally, NCPs could propose model language for standard contracts that may be incorporated by participating

---

PSCs …. Government participation has also failed to meet expectations. Only seven of the 58 governments that participate in the Montreux Document and its Forum are members of the ICoCA. Of those seven members, none are developing nations which are typically most at risk from non-state armed groups.").

[129] I leave unresolved the question of whether the board and/or the NCPs will have the power to impose sanctions on either governments or companies, or merely make recommendations.

[130] Today there are NCPs in 49 countries who work to provide "good offices" for the implementation of the OECD Human Rights Guidelines for Multinational Enterprises. The NCPs are nonjudicial in character and promote informal dialogue and professional mediation between victims of human rights abuses and the companies that are allegedly responsible for the abuse. The NCPs often rely on recommendations to be implemented by the corporation moving forward in a way that aligns itself better with the OECD guidelines. For further reading, see "National Contact Points for Responsible Business Behavior: Providing Access to Remedy 20 Years and the Road Ahead," OECD, https://perma.cc/MP26-EHE3.

companies.[131] This will ensure greater consistency in interpretation (which in turn can guarantee better enforceability).

The CSAS Model: Substantive Obligations

Government Obligations

Under the CSAS, the use of commercial spyware by governments and government actors is not prohibited *ipso facto* under international human rights law. Rather, the CSAS would establish a restrictive and tailored human rights protective framework for the way spyware can be employed by a member state using the following principles:

- **Principle of Legality**: Member states will need to prescribe the use of spyware per se in primary legislation that is both "publicly accessible, clear, precise, comprehensive, and [has] non-discriminatory" rules.[132]
- **Principle of Necessity**: Member states will need to establish a limited set of legitimate aims for the use of spyware and ensure that every deployment of spyware tools is done in furtherance of one of the aims. Under the principle of necessity, "both the general program for intelligence collection must be necessary for safeguarding democratic institutions, and the specific intelligence gathering operation in dispute must be additionally necessary to achieve those aims."[133] Possible aims include "protecting national security, preventing disorder and crime, and protecting the rights and freedoms of others."[134]
- **Principle of Proportionality**: Spyware should not be employed in an automatic fashion, and the member state will need to target particular information that it reasonably believes will further the

[131] For excerpts of certain contract provisions from NSO Group's standard contracts, see NSO Group's Transparency Report, supra note 78, at 31–32.

[132] See *Ivashchenko v. Russia*, App. No. 61064/10, Eur. Ct. H.R. Grand Chamber, paras. 72–73 (Feb. 13, 2018).

[133] See Asaf Lubin, "The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law," in *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives*, ed. Robert Kolb, Gloria Gaggioli, & Pavle Kilibarda (Edward Elgar, 2022), 463, 469; See also *Szabó and Vissy v. Hungary*, App. No. 37138/14, Eur. Ct. H.R., para. 73 (Jan. 12, 2016); "PI's Guide to International Law and Surveillance," Privacy International (version 3.0), December 2021, https://perma.cc/9347-F73U; and Eliza Watt, *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law* (Edward Elgar, 2021).

[134] *Big Brother Watch v. UK*, App. No. 58170/13, Eur. Ct. H.R. Grand Chamber, para. 365 (May 25, 2021).

aims sought. If the member state is able to acquire the same evidence without reliance on spyware, it must be required to do so.

- **Principle of Adequate Safeguards**. In the 2021 case *Big Brother Watch v. United Kingdom,* the European Court of Human Rights Grand Chamber introduced a set of eight criteria "to be considered both in the abstract and in the specific application of each [surveillance] program, as part of a 'global assessment' of those programs' internal checks and balances."[135] These eight factors cover "(1) the grounds on which [] interception may be authorised; (2) the circumstances in which an individual's communications may be intercepted; (3) the procedure to be followed for granting authorization; (4) the procedures to be followed for selecting, examining and using intercept material; (5) the precautions to be taken when communicating the material to other parties; (6) the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed; (7) the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance; (8) the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance."[136] The member state will need to develop a secondary regulation that addresses each of these points in the deployment of spyware technologies.

- **Principles of Access to Remedy and Transparency:** This obligation would "often involve providing affected persons, where reasonable, with notice (that either a general surveillance regime or specific surveillance measures are in place) and standing (to challenge such measures). Moreover, such a requirement would entail 'prompt, thorough, and impartial investigation of alleged violations' by an oversight body with full unhindered access to all relevant information and the capacity to issue binding orders."[137] In addition, the member state will commit to establishing annual disclosure protocols, to be shared with other members, of aggregate total uses of spyware as well as best practices and substantive incidents.

Beyond adopting a human rights framework for the use of spyware into their domestic legislation, each member state should commit to procuring spyware only from vetted and accredited CSAS companies. Since the spyware industry centers around government contracts, this would allow member states to leverage their own procurement power to nudge more spyware companies to join the CSAS.

[135] Asaf Lubin, "Introductory Note to Big Brother Watch v. UK (Eur. Ct. H.R. Grand Chamber)," *International Legal Materials* 61, no. 4 (2022): 605–606.

[136] Id. See also *Big Brother Watch v. UK*, supra note 134, at paras. 360–361.

[137] See Lubin, supra note 133, at 470.

Each member state will appoint an NCP who, as noted above, will serve as the primary grievance mechanism for the CSAS. Finally, each member state should establish a VEP process[138] and coordinate with the spyware companies within its jurisdiction to ensure that the decision to hoard, and develop spyware around, a particular zero-day vulnerability has been approved with advice and consent from relevant government agencies through the VEP or a VEP-like process.

Spyware Companies' Obligations

Every country that joins the CSAS will require, as part of its licensing, that each company that is headquartered in its territory will join the CSAS. But the CSAS will equally be open to companies that operate from the territory of non–member states. Each company that joins the CSAS commits to a review by the CSAS board of directors. As part of this review, the company will be required to release information about its product lines, contracts, and client base, as will be developed by the board of directors. Companies will also be subject to the following requirements:

- **Spyware Development:** Companies will be required to "integrate safety, privacy by design, and security by design features appropriate to the risks and technical capabilities of the covered product or service such as: (1) mechanisms for individuals to report misuse of the product or service; (2) strip certain capabilities from the product or service prior to sale; (3) limit use to authorized purpose; (4) limit upgrades, software updates, and direct support that enhance or provide new surveillance features; and (5) provide data minimization."[139]
- **VEP Process:** In the development of new software solutions that involve zero-day vulnerabilities, participating companies will be required to notify the NCP and when asked may be required to collaborate with the licensing government on an equities review relating to the particular vulnerability.
- **Spyware Marketing and Sales:** Participating companies will be required to engage in a human rights impact assessment when marketing to and contracting with new clients, including a review of the human rights record of particular end users and foreign governments. The NCPs will be available to advise participating companies that need further information about particular government clients.

---

[138] Note that the PEGA Committee recommends that every member state "develop … vulnerability equity processes, prescribed by law, which determine that, by default, vulnerabilities must be disclosed and not exploited, and that any decision to deviate from this must be an exception and assessed under the requirements for necessity and proportionality, including the consideration as to whether the infrastructure affected by the vulnerability is used by a large share of the population, and be subject to strict oversight by an independent supervising body, as well as to transparent procedures and decisions." See PEGA Recommendations, supra note 17, at para. 79.

[139] See Due Diligence Guidance, supra note 24, at 10–11.

- **Spyware Client Management and Termination:** Participating companies will be required to apply the following protocols:
    - Participating companies will incorporate "human rights safeguards language in contracts. The language should be specific to human rights risks identified and/or associated with the product or service."[140] Participating companies will further require end user license agreements (EULAs) that include end user limitations such as restrictions on who can use the product or service and how the product or service can be used to collect, store, or share data, further reserving the company's right to deny software updates, trainings, upgrades, or customer support in the event of a contractual breach (as part of a preset "preventative framework").[141] The EULA should establish the exact scope of the company's right to investigate allegations of abuse by its clients, including through remote access to end users' networks.
    - Participating companies will adopt "access and distribution mechanisms and contractual provisions that authorize seller to maintain full control and custody of the product and terminate access if necessary to minimize risk of diversion where practicable (e.g. cloud-based access rather than on-premises installations; license keys requiring periodic renewal rather than permanent activation)[.]"[142]
    - Participating companies will reassess "human rights due diligence considerations prior to [EULA] renewal; new activities, provision of services to, or relationships with the customer; major changes in the business relationships; and social and political changes that could result in misuse of products or services in the country where the customer resides."[143] Participating companies will further establish an internal grievance mechanism so that "both internal and external actors" could "report misuse of products or services."[144] Such mechanism should allow "secure and confidential reporting."[145] Each complaint of misuse should be "thoroughly investigate[d]" and where a "credible and significant complaint" is established the company

[140] Id. at 11.

[141] Id.

[142] Id.

[143] Id. at 12. This also includes the commitment to "[s]tay aware of news developments and shifts in a customer's home country in order to stay abreast of how the product or service could be used by the government to restrict civic space and/or target journalists, vulnerable groups, or minority groups."

[144] Id. at 11.

[145] Id.

should temporarily "disable the product or service" until the investigation is completed.[146] Finally, the company should "provide remedy where possible."[147]

- Participating companies shall "create an indelible, permanent, and uneditable auditable record of what actions have been taken by the user of the spyware, including any interferences/modifications of data/metadata, when those occurred, and by whom they were affected so that the use of the tool can be verified, and its human rights compliance assessed after the fact by judicial authorities. Part of that indelible and uneditable record must be some form of identifier or watermark such that judicial authorities overseeing complaints may verify the producer of spyware alleged to have been used against a victim and the customer to which that spyware was originally supplied and, from such source, can compel disclosure of the auditable record such that the legality of any use complained of can be adequately reviewed."[148]
- Procedurally, each company should establish and strictly adhere to a set of predefined whistleblower protections. Each participating company will adhere to annual reviews by the board of directors as part of its membership renewal process. Finally, each participating company will agree to comply with the recommendations of the NCP as part of its review of specific instances.

Why Would Countries Join This Framework, and How Will It Be Implemented?

As already noted, in March 2023 the United States and two dozen other countries adopted a code of conduct for the regulation of spyware.[149] That code itself is quite vague and aspirational, but the state parties to this consortium made it clear that they are committed to a new multilateral approach to the

[146] Id. at 12.

[147] Id. For a detailed discussion of the grievance mechanism and investigation protocols employed by NSO Group, see NSO Group's Transparency Report, supra note 78, at 25–28.

[148] This requirement and others might differ in the specific context of spyware-as-a-service. In this model, the spyware company is not providing spyware as a product to their foreign client. Rather, the spyware company keeps the tool in its possession and only provides the client remote access to the tool. For further reading, see PEGA Recommendations, supra note 17, at para. AR ("[T]here are cases where spyware companies, in particular Intellexa, have not only sold the interception and extraction technology itself, but also the entire service, also referred to as 'hacking as a service' or 'active cyberintelligence', offering a package of surveillance and interception technology methods, as well as training for staff and technical, operational and methodological support …. [T]his service could allow the company to be in control of the entire surveillance operation and aggregate the surveillance data.").

[149] See supra notes 67–70 and accompanying text.

regulation of spyware and will work together to develop a future framework.[150] This already demonstrates buy-in from states. What is motivating this recent buy-in? It's likely a combination of things.

On the one hand, world leaders have now themselves been targeted by spyware, and that has raised awareness to the foreign policy risks posed by the industry. Recall that it was the Edward Snowden revelations about the National Security Agency's spying on Angela Merkel and Dilma Vana Rousseff that brought Germany and Brazil together to champion new UN-based instruments for curtailing foreign surveillance. On the other hand, the ongoing cyber rivalry against Russia and China is pushing a need for democratic countries to develop an alternative narrative about cyberspace. When the Biden administration is caught purchasing the very same spyware it is warning against, that calls into question the sincerity of that narrative. If democratic leaders want to keep a moral leg to stand on in the spyware debate, when fighting against nations that use cyber oppression as a regular tool, they need to promote a lawful market for spyware that is under their tight control.

My CSAS proposal is but one idea that should be put on the table and negotiated between the parties. I do not assume that it will immediately be picked up, nor do I think it necessary that it be adopted in its entirety. Rather, I see my proposal as a modular solution, to pick and choose from as the parties to the code continue to debate a final framework in the years to come. Many questions remain unanswered, such as: What would be the funding scheme for this new international organization? How will the board of directors measure compliance? And how will sanctions be assigned in the case of abuse? I don't look to resolve these questions now.

The core principles, however, are simple. The only path forward to the spyware dilemma is through a legitimate market for vulnerabilities subject to explicit and strict constraints. The countries that joined the United States in its consortium are some of the most affluent countries in the world. Since the primary clients for spyware are government actors, these countries could and should leverage their procurement power to set new standards for the market. I imagine, therefore, only a club of countries initially developing and joining this framework. But since the marketplace for commercial spyware is relatively small (in terms of both supply and demand), a handful of powerful countries joining with their large budgets as an incentive might be enough to bend the arc of this industry toward justice.

Having a legitimate market will be good for the participating countries too. These countries not only will get a seat at the table in designing the future of spyware regulation (and thereby have an edge in the broader cyber and intelligence competition)—but they will also finally have the ability to go after those countries that abuse spyware to violate human rights and those companies that enable it.

[150] Id.

CONCLUSION

The past few years have seen a massive shift in the way countries are approaching spyware regulations. These developments make the findings in this paper particularly timely and increase the likelihood that meaningful change could be achieved in the near future.

The core understanding is this: Spyware companies are here to stay. In the age of end-to-end encryption and new types of cyber-enabled crimes, the need for lawful hacking tools by law enforcement is evident and widely undisputed. At the same time, these tools produce significant harms to those most at risk in our society: journalists, human rights defenders, and members of marginalized groups.

There is thus an urgent need for regulatory intervention. We should reject the old narratives that have constrained us and adopt a broader and holistic understanding of the problem of spyware to imagine new innovative solutions. One such solution is proposed in this paper, a comprehensive multistakeholder framework that could help standardize and harmonize global responses to the vulnerabilities trade. My hope is only that my proposal helps highlight the strategic points of contention and thereby further move the discourse in more creative directions.

The Digital Social Contract paper series is supported by funding from the John S. and James L. Knight Foundation and Meta, which played no role in the selection of the specific topics or authors and which played no editorial role in the individual papers.