Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry

George T. Papademetriou*

ABSTRACT

The rapid growth of the private surveillance technology industry over the past two decades poses a significant threat to journalists and activists at the forefront of human rights organizing. While cyber surveillance tools have traditionally been concentrated in the hands of a few governments due to their cost, the software licensing model exemplified by the Israel-based NSO Group has democratized access to sophisticated and invasive spyware. These tools have in turn granted governments unprecedented access to the lives and private communications of their citizens, and in several cases enabled autocrats to track, harass, imprison, and torture opposition leaders and journalists they viewed as threats.

This Note aims to document the rise of the spyware industry, identify the policy failures and gaps in existing legal regimes that contributed to its growth, and suggest several pathways for reform. Part II describes the underlying conditions that allowed the private surveillance software industry to flourish. Part III introduces the conceptual framework of market disruption and explains why it is suitable for evaluating the existing policy landscape. Part IV then assesses whether ongoing efforts to curtail the industry's abuses have been coherent and recommends changes to existing legal and policy frameworks that reinforce the right to privacy and limit the reach of digital surveillance.

The Note focuses on three bodies of law which are ripe for reform: international human rights instruments, export controls and criminal sanctions, and civil litigation remedies. On their own, each of these existing regimes have significant defects. Successfully curtailing the private surveillance software industry will require a comprehensive approach that deters future market entrants and limits incumbents' ability to re-invest profits by stigmatizing private surveillance firms, driving up the cost of capital and of key technological inputs, and limiting firms' ability to sell to customers with known track records of violating human rights.

* J.D. Harvard Law School '23. My thanks to Professor Tyler Giannini and the participants in the Spring 2022 Human Rights Writing Group, for which this Note was originally conceived, as well as to the participants in the 2023 Salzburg Cutler Fellows Program for their insights and thoughtful comments. Thanks also to my friend and mentor Bob Boorstin, without whom I would never have encountered the journalists and human rights activists whose everyday struggles inspired this article.

Introduction: The Pegasus Project

For investigative journalists and human rights activists working in repressive environments, operating in a digital world means engaging in a constant battle for privacy. These individuals play an essential role in the human rights ecosystem by calling attention to abuses carried out by governments and multinational corporations. In doing so, activists often make powerful enemies who would readily search through their personal and professional communications for any excuse to silence them. Many human rights advocates are aware of this risk[1] and take precautions—including taking advantage of significant advancements in the availability of encrypted communications technology.[2] Nevertheless, the emergence of a private sector surveillance industry which creates sophisticated and invasive spyware for clients with few concerns about the lawfulness of their targets appears to have tipped the scales decisively in the direction of governments.

Any illusions about the surveillance capabilities available to governments were ripped away in July of 2021. That month, a collaborative investigation by more than eighty journalists from seventeen media organizations published a dramatic new accounting of how governments have deployed spyware to "silence journalists, attack activists and crush dissent."[3] The investigation, which was titled the Pegasus Project and was coordinated by a Paris-based media nonprofit called Forbidden Stories, detailed how spyware developed by an Israeli surveillance technology company called NSO Group has become the "weapon of choice for repressive governments."[4] The evidence that the Pegasus Project presented was groundbreaking: investigative journalists examined leaked documents containing more than fifty thousand phone numbers that NSO Group clients had selected for surveillance and identified least 180 journalists in twenty countries as targets. The list included more than fifteen thousand numbers in Mexico and large clusters in the Middle East's Gulf States (Qatar, United Arab Emirates, Bahrain, and Yemen).[5]

Subsequent forensic analysis of a small subset of these phones by Amnesty International's Security Lab confirmed that NSO Group's military-

1. *Being the Target*, Privacy International, https://privacyinternational.org/campaigns/being-target [https://perma.cc/8ADV-X56B].

2. Namrata Maheshwari, *Four Strategies to Defend Encryption and our Human Rights*, AccessNow (Oct. 21, 2021), https://www.accessnow.org/how-to-defend-encryption/ [https://perma.cc/J9J3-YMB9].

3. Press Release, Amnesty International, Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally (July 18, 2021), https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/ [https://perma.cc/G2PE-Z29T].

4. The company's name, "NSO Group," reportedly refers to the names of its founders, Niv Carmi, Omri Lavie, and Shalev Hulio. Orr Hirschauge and Inbabl Orpaz, *U.S. Fund to Buy NSO and Its Smartphone-Snooping Software*, Haaretz (Feb. 17, 2017), https://www.haaretz.com/israel-news/business/u-s-fund-to-buy-snooping-software-1.5323394 [https://perma.cc/VBE4-TKBH].

5. Phineas Rueckert, *Pegasus: The New Global Weapon for Silencing Journalists*, Forbidden Stories, (July 18, 2021) [hereinafter Forbidden Stories], https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/ [https://perma.cc/RH8F-TCYB].

grade spyware, which it claims to license to governments for tracking terrorists and criminals, "was used in attempted and successful hacks of 37 smartphones belonging to journalists, human rights activists, business executives, and two women close to murdered Saudi journalist Jamal Khashoggi."[6] Finally, the University of Toronto's world-renowned Citizen Lab investigative team independently verified the presence of Pegasus spyware on these devices and conducted a peer review of Amnesty's methods, which concluded that they were sound.[7]

Though using digital tools to spy on journalists is not a new phenomenon, the sophistication of the technology uncovered in the Pegasus Project is unparalleled. Since organizations like Amnesty International began documenting attacks, "the complexity of performing these attacks has increased exponentially."[8] Rather than a target having to click on a link to install the spyware, for example, Pegasus employs so-called "zero-click" exploits that can penetrate a device remotely without any engagement on the part of the user.[9] Security researchers at Google's Project Zero, a team dedicated solely to finding unpatched software vulnerabilities, have called NSO Group's zero-click capability "one of the most technically sophisticated exploits we've ever seen."[10]

The stories that have emerged about the journalists affected are similarly jarring. Leading Azerbaijani investigative reporter Khadija Ismayilova, who has faced harassment and imprisonment for the past decade, discovered that Pegasus had hacked her smartphone repeatedly between March 2019 to May 2021.[11] Carmen Aristegui, a prominent investigative journalist in Mexico who faces routine threats for investigating corruption between politicians and drug cartels, has also been targeted—including through Pegasus links on her personal assistant's phone.[12] Mexican journalist Cecilio Pineda, who was shot and killed while investigating alleged collusion between police and the leader of a local drug cartel, also appeared on the NSO Group target list.[13]

---

6. Dana Priest, Craig Timberg, and Souad Mekhennet, *Private Israeli Spyware Used to Hack Cellphones o Journalists, Activists Worldwide*, Wash. Post (July 18, 2021) [hereinafter Washington Post, *Private Israeli Spyware*], https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/?itid=LK_inline_manual_3 [https://perma.cc/BXH5-PKWY].

7. Bill Marczak, John Scott-Railton, Siena Anstis, and Ron Deibert, *Independent Peer Review of Amnesty International's Forensic Methods for Identifying Pegasus Spyware*, CitizenLab (July 18, 2021), https://citizenlab.ca/2021/07/amnesty-peer-review/ [https://perma.cc/Z62B-EA4E].

8. Forbidden Stories, *supra* note 5 (quoting Claudio Guarnieri, Director of Amnesty International's Security Lab).

9. *Id*.

10. Ian Beer & Samuel Groβ, *A Deep Dive Into an NSO Zero-Click iMessage Exploit: Remote Code Execution*, (Dec. 15, 2021), https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html [https://perma.cc/5L8M-ZVJK].

11. Washington Post, *Private Israeli Spyware*, *supra* note 6.

12. *Id*.

13. Forbidden Stories, *supra* note 5.

These accounts are but the latest and most extreme in the critically important legal and policy landscape of surveillance, technology, and privacy. They speak to at least two types of human rights violations: (1) the violation that occurs when an individual's privacy is arbitrarily infringed;[14] and (2) the imprisonments, harassment, and torture that such a dramatic erosion of privacy rights enables.[15] These abuses in turn implicate other internationally recognized human rights—most notably free expression and freedom of the press.[16] This Note explores the conditions that produced the rapid growth of privately developed surveillance software, assesses whether ongoing efforts to curtail the industry's worst abuses have been coherent, and recommends changes to the existing legal and policy framework to push the balance between privacy and surveillance back towards individual rights.

While many human rights and digital privacy organizations had previously raised concerns about NSO Group's sale of surveillance software to authoritarian governments,[17] the pace of activity in response to the Pegasus Project was dizzying. In October 2021, the U.S. Department of Commerce issued a new rule tightening export controls for surveillance software technology and its components.[18] Several weeks later, the Department added NSO Group to its Entity List along with three hacking groups, effectively blacklisting them from doing business in the United States.[19] Countering authoritarian uses of technology also became a central theme in the United States' participation in the Summit for Democracy, culminating in the issuance of an Executive Order prohibiting the U.S. government from using any commercial spyware which poses "significant counterintelligence or security risks to the United States government or significant risks of improper use by a foreign government."[20]

The fallout from the Pegasus Project has also triggered litigation. WhatsApp and Apple both filed civil lawsuits against NSO Group for causes of action arising out of the Computer Fraud and Abuse Act, state computer

14. International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 17 [hereinafter ICCPR].

15. *See, e.g.*, ICCPR art. 7 ("No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment").

16. G.A. Res. 217 (III) A, *Universal Declaration of Human Rights*, art 19. (Dec. 10, 1948) [hereinafter UNDHR].

17. For a compilation of CitizenLab's commentary and forensic analyses of NSO spyware dating back to 2016, see *NSO Group*, CitizenLab, https://citizenlab.ca/tag/nso-group/ [https://perma.cc/XSK6-VFXR].

18. Press Release, U.S. Dep't of Com., Commerce Tightens Export Controls on Items Used in Surveillance of Private Citizens and other Malicious Cyber Activities, (Oct. 20, 2021), https://www.commerce.gov/news/press-releases/2021/10/commerce-tightens-export-controls-items-used-surveillance-private [https://perma.cc/GQB5-ZP7K].

19. Press Release, U.S. Dep't of Com., Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities (Nov. 3, 2021), https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list [https://perma.cc/6SG6-C3ZS].

20. Exec. Order No. 14093, 88 Fed. Reg. 18957 (Mar. 30, 2023).

fraud statutes, and breach of contract claims. [21] More recently, a group of journalists affiliated with Salvadoran news organization El Faro relied on analysis from Amnesty and CitizenLab to file a lawsuit against NSO Group in the Northern District of California.[22]

Human rights groups have urged the European Union (EU) to undertake similar measures.[23] In March 2022, the European Parliament launched a formal inquiry into allegations that EU member states Poland and Hungary employed Pegasus spyware against opposition politicians.[24] The parliamentary hearings revealed that at least fourteen EU countries, including Poland, Hungary, Spain, Belgium, and the Netherlands purchased Pegasus[25] and produced committee report calling for a moratorium on spyware.[26] The European Data Protection Supervisor (EDPS), an independent authority which monitors privacy protections in EU institutions, went further in calling for an outright ban on Pegasus and similar spyware.[27] Even Israel, which in the past has lobbied heavily for the United States to lift its sanctions on NSO Group, moved quickly to remove sixty-five countries from its approved purchasers list, restricting NSO Group's client base by roughly two thirds.[28]

The coordinated media campaign around the Pegasus Project likely played an important role in generating momentum towards political reform where past efforts have failed. After a dramatic initial wave of articles in a wide array of leading global publications, a steady drumbeat of new stories over the past two years has maintained the public spotlight on NSO Group and created pressure for policymakers to act. The sophisticated and far-reaching nature of the surveillance, along with the fact that several high-profile targets have been affected, may have been a factor as well: phone numbers contained in NSO Group's target list included those of French

21. Nicole Perlroth, *Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones*, N.Y. Times (Dec. 6, 2021).

22. Tim Starks and Aaron Schaafer, *Here's a First: Journalists and a U.S. Citizen are Suing NSO Group*, Wash. Post (Dec. 1, 2022), https://www.washingtonpost.com/politics/2022/12/01/here-first-journalists-us-citizen-are-suing-nso-group/ [https://perma.cc/KMU2-GQR2]; *see also* Complaint, *Dada et al v. NSO Group Technologies Limited et al.*, No. 22-07513-JD (Nov. 30, 2022), ECF No. 1.

23. *Rights Groups Urge EU to Ban NSO Over Clients' Use of Pegasus Spyware*, The Guardian (Dec. 3, 2021), https://www.theguardian.com/law/2021/dec/03/rights-groups-urge-eu-to-ban-nso-over-clients-use-of-pegasus-spyware [https://perma.cc/25JT-3QMU].

24. Press Release, European Parliament, Three new committees on Pegasus spyware, foreign interference and COVID-19 (Mar. 10, 2022), https://www.europarl.europa.eu/news/en/press-room/20220304IPR24801/three-new-committees-on-pegasus-spyware-foreign-interference-and-covid-19 [https://perma.cc/28D5-D4CG].

25. Julie Fuchs, *Is the EU Protecting People from Pegasus Spyware?*, AccessNow (Jan. 17, 2023), https://www.accessnow.org/eu-pegasus-spyware/ [perma.cc/8F77-NYEB].

26. Press Release, Access Now, EU Calls for spyware moratorium, but no ban to protect human rights (Nov. 8, 2022), https://www.accessnow.org/eu-spyware-moratorium/ [perma.cc/E7XP-P3K2].

27. Preliminary Remarks on Modern Spyware, European Data Protection Supervisor, 1, 9 (2022).

28. *Israel Slashes List of Countries That Can Buy Cyber Tech*, Reuters (Nov. 25, 2021), https://www.reuters.com/markets/us/israel-slashes-list-countries-that-can-buy-cyber-tech-report-2021-11-25/ [perma.cc/PRS3-V8SH].

President Emanuel Macron, thirteen other heads of state, and at least one high-level European Union Official.[29]

The increased global scrutiny arising from the Pegasus Project has resulted in a sharp drop-off in sales and shaken investor confidence.[30] Reports in November 2021 that NSO Group was on the verge of defaulting on $500 million USD worth of debt stirred chatter of potential bankruptcy.[31] Though it appears to have secured the financing necessary to avoid default, NSO Group bonds continued to be traded at distressed debt levels well into 2022.[32] The firm is now spending heavily on new, less controversial assets (including drone-monitoring technology and a big data analytics platform), which executives are pitching to potential acquirers, but may be forced to shut down the Pegasus program in the event of an acquisition.[33] NSO Group's most promising acquisition option, the American defense contractor L3Harris, backed away from sale negotiations in June 2022 after the Biden White House signaled their frustration that a government contractor would even entertain such a purchase.[34]

The Pegasus Project's sharp focus on NSO Group's abuses and subsequent government responses to these disclosures have effectively disrupted one of the most prominent purveyors of private sector surveillance technology. Even if NSO Group disbands, however, the lucrative market for cyber exploits will entice similarly unscrupulous actors to take its place. Policymakers seeking to rein in the surveillance technology industry confront several complex and interrelated problems. First, while many legal tools are now available to regulate private surveillance firms, this Note identifies

29. *Emmanuel Macron Identified in Leaked Pegasus Project Data*, The Guardian (July 20, 2021), https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data [perma.cc/7HV8-5BEJ]; *Top EU Officials Hacked by Israeli Pegasus Spyware*, EuroNews (July 27, 2022), https://www.euronews.com/my-europe/2022/07/27/top-eu-officials-hacked-by-israeli-pegasus-spyware [perma.cc/U5PA-RLE9].

30. Court filings in a UK lawsuit between NSO Group's private equity backers revealed that the firm received no new bookings to use its Pegasus spyware since July 2021, when the Pegasus Project was released. Kaye Wiggins, *NSO Group Deemed 'Valueless' to Private Equity Backers*, Financial Times (Apr. 10, 2022), https://www.ft.com/content/24584247-0fd4-4826-bcac-f726ad17af58 [perma.cc/ZGB5-LMW8].

31. *Israeli Spyware Firm NSO 'At Risk of Defaulting' After U.S. Blacklisting*, Haaretz (Nov. 23, 2021), https://www.haaretz.com/israel-news/tech-news/israeli-spyware-firm-nso-at-risk-of-defaulting-after-u-s-blacklisting-1.10408897 [perma.cc/T3SJ-YSFF].

32. *Israeli Spyware Firm NSO Seen at Risk of Default as Sales Drop*, Bloomberg (Nov. 22, 2021), https://www.bloomberg.com/news/articles/2021-11-22/israeli-spyware-firm-nso-seen-at-risk-of-default-as-sales-drop [perma.cc/F7QW-6XRW]; *see also Fitch U.S. Leveraged Loan Default Insight*, Fitch Ratings (Oct. 26, 2022), https://www.fitchratings.com/research/corporate-finance/fitch-us-leveraged-loan-default-insight-market-concern-loan-total-soars-ytd-default-rate-reaches-1-4-26-10-2022 ("Neovia Logistics Services LLC, NSO Group and 24 Hour Fitness Worldwide Inc. are among the YE 2022 default candidates") [perma.cc/5VD5-UQF9].

33. *Pegasus Spyware Maker NSO Group Throws Cash at New Ventures to Survive*, Bloomberg (Dec. 21, 2021), https://www.bloomberg.com/news/articles/2021-12-21/nso-group-burned-up-most-of-its-cash-to-shift-away-from-pegasus [perma.cc/A956-ZTWE].

34. Mark Mazzetti Ronen Bergman, *Defense Firm Said U.S. Spies Backed Its Bid for Pegasus Spyware Maker*, N.Y. Times (Jul. 10, 2022), https://www.nytimes.com/2022/07/10/us/politics/defense-firm-said-us-spies-backed-its-bid-for-pegasus-spyware-maker.html [perma.cc/VN7V-AUHJ].

several gaps which persist—including a lack of enforcement resources and limited opportunities for victims to seek redress. Second, and more fundamental, is the challenge of striking the appropriate balance between privacy and security. This requires weighing legitimate purposes for which surveillance can be used, including criminal investigations, against the important role that privacy plays in a well-ordered society. The role governments play in upholding this balance is crucial but often circumspect: while governments have the singular ability to bring regulatory actions against abuses, there are countless examples in which the government's interest in promoting security and stability has won out against privacy rights.[35]

This Note offers an approach for evaluating these tradeoffs. It argues that where other authors have focused on the technical architecture of security or the role of multistakeholder networks in constraining the behavior of surveillance firms, the relationship between law and markets remains critically important. When considering how to adjust existing doctrinal rules or policy levers (e.g., the amount of resources devoted to enforcement) to achieve a smart policy mix, protecting individual users' privacy rights requires examining the effect these changes would have on the spyware industry through the lens of market disruption.

To do so, the Note adopts the analytical framework developed by Lawrence Lessig which asserts that law, norms, markets, and architecture each constrain the behavior of regulated actors. It then proceeds by applying this frame to three bodies of law—international human rights instruments, export controls and criminal sanctions, and civil litigation remedies—with a particular sensitivity to the relationship between law and markets. International legal instruments, which face challenges when it comes to national implementation, operate most powerfully through their ability to influence norms. Existing regulations, including export controls and other sanctions, can raise surveillance firms' cost of doing business but are often implemented on an ad-hoc basis, creating a perpetual whack-a-mole problem. Civil litigation remedies offer a more universal way of holding surveillance firms to account, but jurisdictional bars and practical challenges associated with litigating technical and fact-intensive disputes put this form of redress beyond the reach of most victims.

None of these approaches will be sufficient to solve the threat posed by private surveillance firms on their own. Instead, this Note argues that to reset the balance between surveillance and privacy, policymakers should adopt a combination of regulatory approaches aimed at extinguishing the market opportunity for private surveillance firms that carry out human rights abuses. By stigmatizing private surveillance firms, driving up the cost of capital and of key technological inputs, and limiting firms' ability to

35. *See, e.g.*, the Edward Snowden revelations. Ewen Macaskill and Gabriel Dance, *NSA Files: Decoded*, The Guardian (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 [perma.cc/4M4C-RZ6R].

sell to customers with known track records of violating human rights, lawmakers can disrupt the surveillance business model and deter firms considering entering this space. This will not solve the problem in its entirety. Some firms will decide the risk is worthwhile, and governments may step up efforts to develop capabilities internally. But perfect cannot be the enemy of the good. Taking affirmative steps to limit the scale on which existing firms like NSO Group operate, and which have enabled them to develop such sophisticated technologies, will have concrete benefits for the lives of human rights activists and is an undertaking well worth pursuing.

I. Background: The Evolving Relationship between Private Actors and the Surveillance State

The past decade has seen a dramatic increase in the frequency, sophistication, and severity of cyberattacks against civilian targets. High-profile incidents have jeopardized critical infrastructure,[36] taken municipal services offline,[37] undermined confidence in electoral outcomes,[38] and hampered hospitals and health care institutions' ability to combat the COVID-19 pandemic.[39]

In part, this trend reflects the fact that while the most technologically advanced governments have traditionally dominated the cyber domain, their lead is slipping: the proliferation of hacking groups and the evolution of a flourishing market for technical vulnerabilities mean that a much wider range of organizations can carry out attacks. As award-winning New York Times journalist Nicole Perlroth details in her book, *This is How They Tell Me the World Ends*, governments have played a crucial role in the development of a marketplace for software exploits. In seeking to stay ahead of their adversaries, many governments (including the United States' National Security Agency (NSA)) began to pay amateur hackers for software flaws that could be turned into weapons.[40] Cybersecurity professionals (who refer to the industry as "information security," or "infosec") have responded to this demand signal by pooling their talent through secretive firms which

36. Scott Neuman, *What We Know About the Ransomware Attack on a Critical U.S. Pipeline*, NPR (May 10, 2021), https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-ransomware-attack-on-a-critical-u-s-pipeline [perma.cc/W6QX-YCAB].

37. *Ransomware Attacks Are Testing Resolve of Cities Across America*, N.Y. Times (Apr. 27, 2021), https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html [perma.cc/DVA6-V8B7].

38. *See* Robert S. Mueller, III, U.S. Dep't Of Justice, Report On The Investigation Into Russian Interference In The 2016 Presidential Election (2019); *see also* Eric Auchard, *Macron Campaign Was Target of Cyber Attacks by Spy-Linked Group*, Reuters (Apr. 24, 2017), https://www.reuters.com/article/us-france-election-macron-cyber/macron-campaign-was-target-of-cyber-attacks-by-spy-linked-group-idUSKBN17Q200 [perma.cc/3FSX-RV9M].

39. Sophie Porter, *Cyberattack on Czech Hospital Forces Tech Shutdown During Coronavirus Outbreak*, Healthcare IT News (Mar. 19, 2020), https://www.healthcareitnews.com/news/emea/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak [perma.cc/RD53-EAZ6].

40. Nicole Perlroth, This is How they Tell Me the World Ends: The Cyber-Weapons Arms Race, 389–90 (2021).

essentially function as government contractors for cyberweapons. These companies scan software for vulnerabilities, develop malicious code to exploit them, then sell (or license) the resulting hacking tools to governments.[41]

Over the past decade, governments have increasingly come to rely on these kinds of contractors for intelligence collection. Two developments have accelerated this shift. First, the widespread adoption of mobile technology has made every cell phone a potential target, rich with information that governments might find useful in tracking perceived threats. Second, due in large part to a growing sense that there is a need to protect sensitive communications (especially in the aftermath of the Edward Snowden disclosures), technology companies now employ end-to-end encryption technologies which protect communications between individuals—making it far more difficult for law enforcement agencies to access communications via traditional wiretaps.[42] Surveillance companies including NSO Group offer governments a powerful workaround: rather than target encrypted data in transit, they provide unfettered access to the mobile device itself. As leading cryptologist Bruce Schneier has put it, "if someone is reading over your shoulder, it doesn't matter what kind of encryption was used."[43]

Though its origins remain murky, NSO Group appears to have been one of the first firms to recognize and exploit the commercial opportunity that governments' desire to circumvent cell phone encryption created. Founded in 2008 by former Israeli signals intelligence operatives, just at the onset of the smartphone boom, NSO Group initially marketed its surveillance technology as a way for telecommunications companies to troubleshoot cell phone issues remotely.[44] In the early 2010s, however, its founders shifted course and began advertising their remote access technology as a surveillance tool called "Pegasus."[45] The sophisticated technology gave clients complete control over targets' devices—including access to calls, messages, and location data—without a trace; it could even record sounds and video using the phone's microphone and video camera.[46]

NSO Group's rebranding proved highly lucrative. Investigative reporting dating back to 2016 suggests that NSO Group was able to charge governments double the rates of its competitors: the first ten iPhone targets would cost $650 thousand USD, plus a 'setup' fee of $500 thousand USD;

41. In the cyber context, the kinds of access on which hacking tools rely can be used for surveillance as well as more destructive attacks.

42. For years, law enforcement agencies expressed concern at the increasing adoption of encryption technology that threatened to cut off access to digital communications between suspects. *See, e.g.*, Brookings Institution, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*, YouTube (Oct. 16, 2014), https://www.youtube.com/watch?v=A8BSr3XqVwE&t=228s [perma.cc/7EQE-RTZ5].

43. Forbidden Stories, *supra* note 5.

44. Perlroth, *supra* note 40 at 178.

45. *Id.* at 179.

46. *Id.*

additional targets could be added at costs of $150 thousand USD (ten targets), $250 thousand USD (twenty targets), $500 thousand USD (fifty targets) and $800 thousand USD (one hundred targets).[47] Governments from Mexico, to Finland, to Saudi Arabia all sought access to this powerful technology.[48]

Spurred by demand, NSO Group grew rapidly. Outside investors took notice. In 2014, the founders sold their controlling stake to a San Francisco private equity firm for $120 million USD; a year later the new owners were in talks for another deal which would have appraised the company at 10 times the value.[49] In 2019, the firm's founders re-acquired the company at a $1 billion USD valuation (based on $250 million USD in annual revenue) even after extensive reporting on its ties to human rights abuses.[50] By January 2021, the company was reportedly considering a $2 billion USD Initial Public Offering (IPO).[51]

NSO Group's sophisticated spyware has realized incredible financial gains, but NSO Group is not alone in pursuing government surveillance contracts. Companies like Cellebrite, FinFisher, Blue Coat, Hacking Team, CyberPoint, L3 Technologies, and Verint—many of which are headquartered in democratic countries (including Germany, Italy, and the United States)—all compete for clients.[52] This market competition has driven down prices and radically democratized access to once unthinkable surveillance power. By one account, at least sixty-five governments worldwide, from Chile to Vietnam, employ commercial spyware tools.[53]

II. Conceptual Framework: Lawrence Lessig's 'Four Modalities' of Regulation

The public backlash against NSO Group in the aftermath of the July 2021 Pegasus Project revelations was swift, but most efforts to curtail surveillance technology have focused narrowly on NSO Group's abuses, rather than the industry writ large. Understanding how various policy choices will

47. *Id.* at 181; *see also* Nicole Perlroth, *Spy Tech Firms Let Governments See Everything on a Smartphone*, N.Y. Times (Sep. 2, 2016), https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html [perma.cc/2U65-ABPL].

48. Perlroth, *supra* note 40 at 181–82.

49. Perlroth, *Spy Tech Firms Let Governments See Everything*, *supra* note 47.

50. *NSO Group's Management Buys Firm From Francisco Partners*, Reuters (Feb. 2, 2019), https://www.reuters.com/article/nso-ma-francisco-partners/update-1-nso-groups-management-buys-firm-from-francisco-partners-idUSL5N209642 [https://perma.cc/8STC-8M75].

51. *Israeli Cyber Firm NSO Group Mulls Tel Aviv IPO at $2 Billion Value*, Reuters (Jan. 6, 2021), https://www.reuters.com/article/israel-cyber-nso-ipo-int-idUSKBN29B0WU [perma.cc/TVB9-X6MW].

52. Steven Feldstein, *Governments Are Using Spyware on Citizens. Can They Be Stopped?* Carnegie Endowment for International Peace (Jul. 21, 2021), https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019 [perma.cc/4HX9-2WNN].

53. *Id.*

affect the broader surveillance technology industry and deter potential market entrants from facilitating abuses requires a broader conceptual framework.

As a starting point, this Note adopts the EU's widely accepted definition for surveillance technologies, which comprises "information and communications technology (ICT) goods, services and technologies that are specifically designed, in whole or in part, for surveillance purposes."[54] Within this broad category, several distinctions are important. First, it is useful to clarify the line between mass surveillance and targeted surveillance. Mass surveillance involves the "indiscriminate and uses systems or technologies to collect, analyze, store, and/or generate data on indefinite or large numbers of people."[55] This type of large-scale, indiscriminate data collection received increased attention in the aftermath of the Snowden disclosures, and has alarming privacy implications (especially when considered alongside the exponential increase in data generated by digitally connected "Internet of Things" devices).[56] Targeted surveillance, on the other hand, typically directs monitoring resources toward specific individuals. This type of surveillance can be carried out overtly or covertly, and may include the direct interception of communications, analysis of communications metadata, and visual and geolocation surveillance.[57] These modes of surveillance can also be lawful or unlawful, depending on whether they comply with domestic legal frameworks or interpretations of international human rights treaties.[58]

Beyond these preliminary definitions, how should we think about the ways in which policy decisions affect the behavior of regulated actors? The approach Lawrence Lessig developed in his article, *The New Chicago School,* and later expounded in his treatise on the regulability of the internet, *Code 2.0*, provides a useful framework for analyzing regulation in cyberspace.[59]

---

54. European Commission, Data and information for EU dual-use export control policy review 149 (2015).

55. Surveillance Technologies Accountability Project (STAP), Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors 6 (March 2022); *see also Mass Surveillance*, Privacy International, https://privacyinternational.org/learn/mass-surveillance [perma.cc/VRN8-CKJA].

56. Though its definition is continually evolving, the "Internet of Things," or IoT, is typically understood to reference digitally connected devices which collect and share data with one another via private internet networks. *See* Matt Burgess, *What is the Internet of Things? Wired Explains*, Wired (Feb. 2, 2018), https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot [perma.cc/KK69-NUB6].

57. Surveillance Technologies Accountability Project, *supra* note 55 at 5.

58. In 2020, for example, the Ninth Circuit ruled that the U.S. government mass surveillance program which Edward Snowden exposed was unlawful and in violation of the Foreign Intelligence Surveillance Act. Devlin Barrett, *Surveillance Program That Gathered Americans' Phone Data was Illegal, Court Finds*. Wash. Post (Sep. 4, 2020), https://www.washingtonpost.com/national-security/phone-records-surveillance-edward-snowden/2020/09/02/97f26498-ed67-11ea-99a1-71343d03bc29_story.html [https://perma.cc/FHL6-64L8].

59. Lawrence Lessig, *The New Chicago School*, 27 J. of Legal Stud. 661 (1998) [hereinafter Lessig, *New Chicago School*]; Lawrence Lessig, Code: And Other Laws of Cyberspace, Version 2.0 (2006) [hereinafter Lessig, Code 2.0].

At the outset, Lessig identifies four 'modalities' of regulation which constrain behavior in both real space and in cyberspace: law, norms, markets, and architecture.

Law, in its simplest form, "directs behavior in certain ways" and threatens ex post sanctions at the hands of the state if those orders are disobeyed.[60] This combination of state-backed rules and penalties is familiar in both the analog and digital contexts: if you break the speed limit, you may receive a ticket; if you infringe a copyright, you will be liable for civil and criminal penalties. These sanctions rely on the coercive power of the state to govern behavior.

Norms lack the state's centralized enforcement authority. Instead, they constrain behavior through internalization and community enforcement. Internalization operates as an ex ante deterrent, discouraging actions that may violate social custom, while community enforcement occurs after the fact (e.g., through naming and shaming). Tipping your waiter and complying with COVID-19 masking requirements rely on this mechanism. In Lessig's words, "a norm governs socially salient behavior, deviation from which makes you socially abnormal."[61]

Markets govern behavior through prices: supply and demand dictate the terms on which X goods may be exchanged for Y services.[62] Resource scarcity, the cost of labor, and overhead costs such as litigation risk[63] influence the price at which suppliers are willing to sell their products. On the other hand, purchasing power, preferences, and the price of comparable goods all impact willingness to pay by consumers. Market dynamics operate against the background of laws, which enforce contracts (among other things), and norms which influence consumer preferences.

The fourth modality, architecture, operates more subtly. Architecture refers to the physical or digital features which "restrict or enable in a way that directly affects behavior."[64] In the physical world, there are physical limits. Physical walls, for example, act as a barrier on law enforcement's ability to eavesdrop on private conversations.[65] The architecture of end-to-end encryption creates a parallel constraint on law enforcement in the digital realm. In both domains, increasingly sophisticated technology can circumvent these protections, but requires time and resources to develop.

60. Lessig, *New Chicago School*, *supra* note 59 at 662.

61. Lessig, Code 2.0, *supra* note 59 at 341.

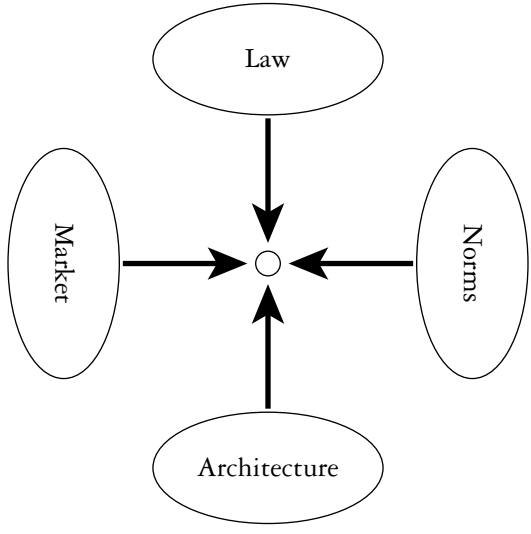
62. As Lessig notes, though markets are distinct from law and norms, they are deeply intertwined—markets rely on property and contract law to govern exchanges, and norms set limits on what types of transactions are socially permissible (e.g., you cannot "buy" a "friend"). Lessig, *New Chicago School*, *supra* note 59 at 663.

63. Jonathan Molot, *A Market in Litigation Risk*, 76 Univ. of Chi. L. Rev. 367 (2009).

64. Lessig, *New Chicago School*, *supra* note 59 at 663.

65. *Id.*

FIGURE 1



The net effect of "regulation" is the sum of these four constraints, as illustrated in Figure 1.[66] But while it can be analytically useful to distinguish each of these four modes of regulation, they are also mutually interdependent.[67] Law, for example, will often reflect broader social norms, but it also has the effect of legitimating or stigmatizing behavior. Legal choices affect markets (e.g., taxes drive up the cost of cigarettes) and can influence architecture (e.g., through building codes). On the other hand, markets will determine prices for building materials, and architecture can create its own norms (e.g., internet chat rooms); all four modalities operate together to shape what types of behavior are possible.[68]

Using this framework, Lessig's core argument (developed at length in *Code 2.0*) is that while architecture plays an important role in the physical world, in cyberspace its reach is pervasive. Structural choices about the physical infrastructure of the internet, as well as the code that flows across it, have profound and underappreciated effects on the types of online spaces users can access, the types of content they see, and the amount of data they surrender. Coding decisions affect every online interaction and are typically invisible to the average user, making them highly efficient mechanisms of control when compared to offline approaches.[69] In the privacy context, for example, real-space surveillance is generally self-authenticating: if a surveil-

66. *Id.* at 664.

67. LESSIG, CODE 2.0, *supra* note 59 at 123.

68. Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 511 (1999) [hereinafter Lessig, *Law of the Horse*].

69. LESSIG, CODE V. 2.0, *supra* note 59 at 4.

lance team tracked your every move, or ransacked your hotel room, you would likely notice. In cyberspace, however, the websites you visit may be designed to extract your data regardless of whether you have given permission, and users have little recourse because "nothing reveals whether you are being watched."[70]

In response, concepts like end-to-end encryption, privacy by design, and multi-factor authentication, all seek to embody "privacy" in architecture through coding decisions. Norms also play an important role, both in shaping everyday practice (e.g., refraining on clicking on links from unknown senders and other elements of cyber hygiene) and in establishing what types of data collection are deemed unacceptable—such as those so intrusive as to constitute human rights violations. These measures have clear market implications as well: they increase the sophistication of the tools needed to access data, which in turn raises the cost of spying.

As Lessig's framework suggests, the relationships between law, norms, markets, and architecture are dynamic and deeply intertwined. This Note focuses on interactions between law and market forces governing the surveillance industry for two reasons. First, though cataloguing and assessing possible developments across all four vectors may be possible in theory, a narrower analysis of a subset of relationships allows for more concrete and actionable insights. The relationship between law and market forces governing the surveillance tech industry, in particular, has been relatively underexamined and provides fruitful ground for inquiry. The evolution of this relationship, and the degree to which new legal measures incorporate human rights values, will have important implications for activists and journalists operating in repressive environments.

Second, while architecture—including physical telecommunications infrastructure, internet routing protocols,[71] and end-user devices like laptops and cell phones—plays a crucial role in the surveillance ecosystem, it is a mode of regulation that is both constantly evolving and difficult to modulate. Leading scholars have noted shifts in the architecture of the internet, including a proliferation of digitally connected devices known as the "Internet of Things"[72] and increasing reliance on a handful of cloud computing providers upon which much of the internet is hosted.[73] These developments are important for the future of privacy but offer more problems than solutions. Cybersecurity professionals can roll out sophisticated safeguards that protect data by default—and some firms like Apple have even realized that making privacy a part of their brand can help distinguish them from com-

70. Lessig, *Law of the Horse*, *supra* note 68 at 505.

71. Internet routing protocols are the rules and standards which routers use to direct traffic from one device or network to another.

72. Berkman Klein Center for Internet and Society, Don't Panic: Making Progress on the Going Dark Debate 3 (Feb. 1, 2016).

73. John Bowers and Jonathan Zittrain, *Internet Entropy*, Lawfare (June 21, 2021), https://www.lawfareblog.com/internet-entropy [perma.cc/6LQH-VAU2].

petitors—but hackers will continue to develop new ways to access sensitive information.[74] Because architecture is ultimately a product of this push and pull, this Note instead focuses on the relationships between law, norms, and markets—all of which shape both the design decisions software developers make and the ability of firms like NSO Group to emerge and thrive.

III. Responses

The remainder of this Note examines several legal and regulatory approaches which seek to curtail the ability of private sector surveillance companies to facilitate human rights abuses: (i) efforts to clarify how international human rights instruments apply to privacy; (ii) the creation of new tools for domestic enforcement through export control regimes and criminal sanctions; and (iii) the possible expansion of opportunities for domestic redress through civil litigation. This analysis reveals that while each of these tools is ostensibly 'legal,' they impact the cybersecurity environment in different ways.[75] Discussions about the obligations international human rights instruments create, for example, are unlikely to produce binding law in the near future but could result in norms that make it easier to condemn bad actors. Spyware firms will internalize this change as a reputational cost. Tighter criminal sanctions, on the other hand, can sever the linkages between spyware firms and both a) their clients and b) the platforms which provide them software inputs. These changes introduce uncertainty into the industry and will drive up cost of borrowing—which in turn limits the ability of spyware firms to reinvest profits into even more sophisticated tools. Because these policy levers tend to reinforce each other, an optimal policy mix will require a set of smart adjustments evaluated in light of their potential to limit the surveillance technology industry's ability to profit from human rights abuses.

A. International Human Rights Instruments

The past several years have seen important developments within the United Nations regarding the right to privacy in the digital age. At a basic level, it has long been agreed that international law enshrines a 'right to privacy' as a fundamental human right. Article 12 of the 1948 Universal Declaration of Human Rights states: "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to at-

74. Heather Kelly, *Apple iOS Privacy Settings to Change Now*, Wash. Post (Nov. 26, 2021), https://www.washingtonpost.com/technology/2021/11/26/ios-privacy-settings/ [perma.cc/S3ME-AGP5].

75. A fourth area of potential reform, the development of multistakeholder models for promoting human rights compliance among surveillance companies, has also garnered attention but is beyond the scope of this Note. David Kaye and others develop this idea. *See* David Kaye and Marietje Schaake, *Global Spyware Such as Pegasus is a Threat to Democracy. Here's how to Stop it.* Wash. Post (Jul. 19, 2021), https://www.washingtonpost.com/opinions/2021/07/19/pegasus-spyware-nso-group-threat-democracy-journalism/ [perma.cc/RR7K-9V7Y].

tacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[76] Article 17 of the 1966 International Covenant on Civil and Political Rights (ICCPR) echoes this language, and a wide range of subsequent of human rights instruments have repeatedly affirmed the right to privacy as fundamental.[77]

These core human rights instruments predated the Internet and did not anticipate the transformative effect that global and instantaneous communications would have on daily life. More recent efforts to update human rights law to account for these changes have made some progress in filling the gap, including highlighting the importance of the right to privacy within the digital technology ecosystem. In 2015, the Office of the High Commissioner for Human Rights established a Special Rapporteur on the Right to Privacy, which aims to "raise awareness concerning the importance of promoting and protecting the right to privacy, including with a view to particular challenges arising in the digital age."[78] Human Rights Council resolutions in 2017, 2018, and 2019 laid the foundation for a groundbreaking General Assembly Resolution on Privacy in the Digital Age in 2020.[79] This resolution identified several specific concerns about privacy in the digital context, including the need for states to maintain adequate oversight mechanisms ensuring accountability for state surveillance of communications, and to provide effective remedies when violations occur.[80] The General Assembly also emphasized the important role that businesses play in maintaining the right to privacy and called on businesses that collect data to meet their responsibility to respect privacy in accordance with the UN Guiding Principles on Business and Human Rights' "Protect, Respect and Remedy" Framework.

These instruments operate against the backdrop of other general principles of public international law and state responsibility, including limitations on when certain political rights may be infringed by governments.[81] The 2020 General Assembly resolution recalls, for example, that "states should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality."[82] This language parallels the ICCPR's test for when restrictions on free expression

76. UNDHR, art. 12

77. ICCPR, art. 17. For a partial list of international instruments affirming the right to privacy, see *International Privacy Standards*, Electronic Frontier Foundation (Accessed Apr. 17, 2020), https://www.eff.org/issues/international-privacy-standards [perma.cc/TW7P-V33N].

78. *Mandate: Special Rapporteur on the right to privacy*, UN Off. High Comm. Hum. Rts. (last visited Apr. 23, 2023), https://www.ohchr.org/en/special-procedures/sr-privacy/mandate [perma.cc/DQ49-WLH5].

79. G.A. Res. 75/176, The right to privacy in the digital age, Dec. 28, 2020, U.N. Doc. A/RES/75/176.

80. *Id.*

81. *See, e.g.,* Handbook for Parliamentarians No. 26, UN Off. High Comm. Hum. Rts. 48 (2016).

82. *Id.*

may be permissible under Article 19, which was extended to derogations of other rights guaranteed by the ICCPR in the Siracusa Principles and has been affirmed repeatedly in Human Rights Council documents.[83]

Nevertheless, many significant questions remain unresolved, and states continue to disagree about what obligations the right to privacy creates in cyberspace. External groups have provided views on what the responsibility to respect privacy entails for businesses,[84] but to date the UN's Working Group on Business and Human Rights has not addressed the issue.[85] Similarly, the Human Rights Council's guidance on how states should interpret "arbitrary" and "unlawful" allows for a wide range of concerning behavior.[86] One reason is that the guidance was last updated in 1988, when General Comment No. 16: Article 17 (Right to Privacy) was published, and the drafters did not contemplate the types of invasive and broad-reaching surveillance practices that are now common. The Human Rights Council's recommendations for how states should interpret other areas of law have occasionally touched on issues involving privacy,[87] but no ongoing efforts appear to address unique concerns relating to the development, transfer, use, or sale of surveillance technology.

The development of international legal protections faces another challenge: implementation into domestic law. While some documents, including Special Rapporteur for Free Expression David Kaye's 2019 Report on Surveillance and Human Rights, have asserted that governments deploying surveillance tools have an obligation to ensure that they do so in accordance with a "domestic legal framework that meets the standards required by international human rights law,"[88] nations have adopted a wide range of interpretations regarding what adequate domestic legal frameworks entail. Moreover, even if formally reflected in domestic law, the impact that inter-

83. Economic and Social Council Res. 1985/4, Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights (Sept. 28, 1984). The 'legality, necessity, and proportionality' limitation was supported by a group of privacy-oriented civil society organizations, such as Electronic Frontier Foundation and Article 19, which issued a joint white-paper in May 2014 advocating for these safeguards in the privacy context. Necessary and Proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance, Electronic Frontier Foundation and Article 19 (May 2014).

84. Business and Human Rights Resource Center, *Navigating the Surveillance Technology Ecosystem: A Human Rights Due Diligence Guide for Investors* (Mar. 2022).

85. For an overview of the UN Working Group's activities, see *Working Group on Business and Human Rights*, UN Off. High Comm. Hum. Rts. (accessed Apr. 17, 2023), https://www.ohchr.org/en/special-procedures/wg-business [https://perma.cc/B6R2-R73L].

86. Human Rights Committee, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, available at: https://www.refworld.org/docid/453883f922.html [https://perma.cc/SY6D-YWAX].

87. *See, e.g.,* Human Rights Council, CCPR General Comment No. 37: Article 21 (Right to Peaceful Assembly), Jul. 27, 2020.

88. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Surveillance and Human Rights*, U.N. Doc. A/HRC/41/35 at B.1 (May 28, 2019); *see also*, U.N. High Commissioner for Human Right, *The Right to Privacy in the Digital Age,* U.N. Doc. A/HRC/27/37 (June 30, 2014).

national human rights obligations have on individuals will depend on the strength of rule of law and judicial independence, which varies by country. Given that intelligence agencies tend to operate in the shadows and with limited oversight, even in open, democratic societies, generating international consensus around how governments should balance privacy with security faces serious obstacles.

Filling these existing legal gaps should be a priority for the international human rights community for two reasons. First, while the internationally recognized right to privacy creates certain legal obligations for states, these obligations are currently loose and provide substantial room for variation in state practice. A tighter set of authoritative interpretations (by updating the General Comment 16 on the right to privacy, for example) would provide the international community an essential tool for identifying and condemning governments and companies that violate the right to privacy.[89]

Second, even if these efforts do not succeed in creating new internationally binding legal instruments, the articulation and contestation of the right to privacy and its accompanying obligations in international forums has an important normative effect. The transnational legal process theory maintains that international human rights law, though underenforced, shapes state behavior in three phases: state-to-state *interaction* in which global norms are debated, *interpretation* of relevant legal principles, and *internalization* by domestic legal systems.[90] Kaye and others engaged in international debates about how states may comply with their privacy obligations are participating in an important normative conversation. Venues like the Human Rights Council or the UN's Group of Governmental Experts for Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE) can provide a space for governments to work through thorny issues and come to consensus about the alarming role of surveillance tech firms in facilitating human rights abuses. These conversations may in turn evolve into state practice, including through authoritative interpretive statements by governments. While limited somewhat by states willingness to violate norms when national security issues are at stake, the practical effect would nonetheless be significant.

Stronger norms and new international human rights law governing privacy in the digital age will undoubtedly impact the market for surveillance technology. One mechanism through which it will do so is the UN Guiding Principles on Business and Human Rights (UNGPs), which require that businesses implement policies and processes to mitigate adverse effects of their operations on human rights and enable remediation of any bad

89. Human Rights Council, CCPR General Comment No. 16: Article 17 (Right to Privacy), Apr. 8, 1988.

90. Harold Hongju Koh, *How is International Human Rights Law Enforced?* 74 IND. L. J. 1397, 1399 (1999).

human rights outcomes that they cause.[91] Advocacy groups have articulated how surveillance technology firms and prospective investors can meet these commitments with respect to privacy, but an authoritative statement from an international human rights body would lend greater credibility to their assessments. Failure to comply with the UNGPs carries a strong reputational effect, and firms that do not adequately implement policies to respect, protect, or remedy privacy violations would run the risk of being singled out as human rights violators. Because investors are increasingly conscious about reputational risks, a clearer, authoritative statement of which behaviors are and are not permissible by surveillance technology firms could deter investments in surveillance firms known to facilitate the abuse of human rights.

B. Export Control Regimes and Criminal Sanctions

Domestic export controls and criminal sanctions provide another set of mechanisms for reining in bad actors and driving up the cost of developing intrusive spyware. These tools are available to most (if not all) governments, but this Note chooses to focus on the United States because its market size and control over financial services infrastructure puts it in a position to exert tremendous influence as a global regulator. Furthermore, recent developments signal a fundamental shift in how U.S. policymakers view surveillance technology; expanded regulatory authorities now make it far easier to deploy sanctions against human rights violators. To date, however, this determination has often been a political one. This dynamic is problematic because it suggests that political concerns, rather than a principled commitment to human rights, will inform enforcement. To be truly praiseworthy, the U.S. export control framework should adopt policies that require determinations to conform with international human rights principles rather than target companies based on the latest political headwinds.

Export controls in the United States generally refer to the system of "laws, regulations and policies governing the export and reexport of commodities, software, and technology" (including sensitive military or dual-use technologies) in order to promote "continued U.S. strategic technology leadership."[92] Regulatory authority over commercial and dual-use technology flows from the recent Export Controls Act of 2018 (ECA), which gives the Department of Commerce's Bureau of Industry and Security permanent authority to develop and update the Export Administration Regulations (EAR) governing commercial, dual-use, and less sensitive mili-

91. UN Office of the High Commissioner, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* 16 (2011), https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf [https://perma.cc/Y2TZ-B4WX].

92. U.S. Export Controls, Int'l Trade Admin., https://www.trade.gov/us-export-controls (last accessed Feb. 25, 2023).

tary items.[93] The ECA aims primarily to advance the national security and foreign policy interests of the United States, but also notes that this policy should be considered to include the "protection of human rights and the promotion of democracy."[94]

The key mechanism implementing this framework is known as the "Entity List," codified as 15 C.F.R. § 744.11, which grants the U.S. government the authority to list an entity for which there is "reasonable cause to believe . . . that the entity has been involved . . . in activities that are contrary to the national security or foreign policy interests of the United States."[95] Designating companies to the Entity List can be commercially devastating because it "empowers the U.S. government to restrict parties from accessing U.S.-origin products or technology."[96] Companies on the Entity List cannot purchase any item subject to Export Administration Regulations (e.g., telecommunications equipment) without a government license —which can be summarily denied, forcing them to find alternative suppliers or opt for worse quality substitutes.[97] In Lessig's framework, these designations can be seen as having both a legal effect, because they proscribe behavior and declare penalties, as well as a market effect, because they signal that the United States views individual companies as pariahs. For these economic outcasts, ordinary market transactions are more costly and incur more risk than a sanctioned entity's counterparties may tolerate, making sanctions an effective way of putting pressure on violators.

Though the Entity List has traditionally served as an instrument to penalize parties suspected of violating export control, proliferation, or sanction authorities,[98] executive branch officials have recently broadened its use.[99] Both the Biden administration and the Trump administration, for example, have added Chinese firms to the list because of their alleged in-

93. *See* Export Controls Act of 2018, (H.R. 5040, codified as 50 U.S.C. 4801–4852) at §104, (requiring the Secretary of Commerce to "establish and maintain a list" of controlled items). Previously, regulatory authority for commercial and dual-use technology relied on executive orders and the International Emergency Economic Powers Act (IEEPA). Testimony of Kevin Wolf before the House Committee on Foreign Affairs (Mar. 14, 2018), https://docs.house.gov/meetings/FA/FA00/20180314/107997/HHRG-115-FA00-Wstate-WolfK-20180314.pdf [https://perma.cc/Q9T9-6JAT].

94. ECA § 102 (1)(d) (2022).

95. 15 C.F.R. § 744.11 (2022).

96. 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), https://www.lawfareblog.com/recent-additions-entity-list-part-broader-us-effort-targeting-spyware [https://perma.cc/H5YW-MJSX].

97. 15 C.F.R. § 744.11 (a)(1) (2022).

98. Capito, Van Grack, Wren, *Recent Additions to Entity List Part of Broader U.S. Effort Targeting Spyware*, Lawfare (Nov. 29, 2021), https://www.lawfareblog.com/recent-additions-entity-list-part-broader-us-effort-targeting-spyware [https://perma.cc/B8P9-L2AA].

99. *See*, *e.g.*, Brian Egan, *New US Semiconductor Export Controls Signify Dramatic Shift in Tech Relations With China*, Just Security (Oct. 24, 2022), https://www.justsecurity.org/83744/new-us-semiconductor-export-controls-signify-dramatic-shift-in-tech-relations-with-china/ [https://perma.cc/Q8CQ-DX2W].

volvement in enabling the repression of the Uighur population in Xinjiang, China.[100]

Likewise, policymakers have increasingly turned to export controls as a mechanism to weaken surveillance firms like NSO Group. In October 2021, the U.S. Department of Commerce issued a new rule tightening export controls on a range of cybersecurity items, including hardware and software components.[101] Weeks later, the department added NSO Group to its Entity List along with three other hacking groups.[102] The announcement of a new multilateral Export Controls and Human Rights Initiative at the Biden administration's Summit for Democracy in December 2021 attempted to internationalize this approach. The initiative identifies several joint measures to "stem the tide of authoritarian government misuse of technology," including the development of voluntary codes of conduct to guide the application of human rights criteria to licensing policy.[103] Building on this achievement, the United States and nine partners announced that they will work together to prevent the proliferation of commercial spyware at the second iteration of the Summit in March 2023.[104] Though it remains to be seen whether future export controls will embody human rights values in practice (as opposed to other American interests, such as technological supremacy), these measures signal a clear concern about the threat that private surveillance companies pose to human rights and provide a partial framework to address them.

U.S. government officials also have a series of criminal statutes available to pursue spyware developers they believe have violated the law. Often, prosecutors will turn to the computer fraud and access device fraud statutes,[105] which create criminal liability for obtaining unauthorized access to computers (or devices) and their underlying personal data. Prosecutors may

100. Press Release, U.S. Department of Commerce, Commerce Department Adds 34 Entities to the Entity List to Target Enablers of China's Human Rights Abuses and Military Modernization, and Unauthorized Iranian and Russian Procurement (Jul. 9, 2021), https://www.commerce.gov/news/press-releases/2021/07/commerce-department-adds-34-entities-entity-list-target-enablers-chinas [https://perma.cc/7UN3-2B3U]. Note that references to human rights in the context of the U.S.-China relationship are difficult to disentangle from other elements of the bilateral relationship and should be assessed with caution.

101. Press Release, U.S. Department of Commerce, Commerce Tightens Export Controls on Items Used in Surveillance of Private Citizens and other Malicious Cyber Activities (Oct. 20, 2021), https://www.commerce.gov/news/press-releases/2021/10/commerce-tightens-export-controls-items-used-surveillance-private [https://perma.cc/V68R-GBEK]; *see also* 15 C.F.R. 740, 772, 774 (2022).

102. Press Release, U.S. Department of Commerce, Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities (Nov. 3, 2021), https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list [https://perma.cc/BLM8-U7ZR].

103. *Fact Sheet: Export Controls and Human Rights Initiative Launched at the Summit for Democracy*, The White House, (Dec. 10, 2021).

104. *Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware*, The White House, (Mar. 30, 2023).

105. 18 U.S.C. § 1029 (2022) (Access Device Fraud); 18 U.S.C. § 1030 (2022) (Fraud and Related Activity in Connection with Computers).

also choose to pursue enforcement under the Arms Export Control Act[106] or the International Traffic in Arms Regulations (ITAR),[107] both of which focus on the export of military technologies (and thus require that at least one of the hacking weapons that defendants developed qualify as a "defense article"). The Department of Justice's resolution of criminal charges against three former military and intelligence officers for cyber espionage operations as part of a United Arab Emirates-backed initiative known as Project Raven marks the first time ITAR provisions criminalizing hacking were used and signals a new level of attention to criminal enforcement.[108] Since then, restrictions on post-service employment have gotten stricter: through the 2022 and 2023 Intelligence Authorization Acts, Congress has implemented new restrictions and reporting requirements for intelligence officials who served in covered positions, which the Director of National Intelligence has subsequently implemented as binding guidance.[109]

Given the size of the U.S. market and the scale of federal enforcement power, a policy leveraging export controls and criminal sanctions against surveillance firms known to violate human rights could have a sharp effect. Though coding specialists like NSO Group are less reliant on U.S. technological inputs than many hardware companies (which often rely on U.S. semiconductors), designating spyware firms to the Entity List will force them to re-establish supplier relationships outside the United States, which is undoubtedly disruptive. More significantly, however, the export controls can serve as powerful signals to potential investors, which would raise the cost of financing and limit firms' ability to reinvest profits into more sophisticated weapons. Export controls can have a similar effect on demand: though some customers will probably not be deterred, many governments which proclaim democratic values or have strong trade relationships with the United States (including many in Europe) may be reluctant to purchase spyware from firms that have been visibly sanctioned for human rights violations.

Export controls and sanction designations impact spyware companies' profitability more directly than international human rights instruments. Nevertheless, several factors limit the transformative potential of this approach. First, because the U.S. export control regime relies upon unilateral determinations by the Bureau of Industry and Security, export control decisions have the potential to reflect political concerns, rather than a principled commitment to human rights. Some export controls are not subject to

106. 22 U.S.C. § 2778 (2022).

107. 22 C.F.R. §§ 120–30 (2022).

108. Brandon L. Van Grack, Joseph Folio, *Prosecuting Project Raven: A New Frontier for Export Control Enforcement*, Lawfare (Oct. 20, 2021), https://www.lawfareblog.com/prosecuting-project-raven-new-frontier-export-control-enforcement [https://perma.cc/AUF5-RE98].

109. Press Release, Office of the Director of National Intelligence, Issuance of Intelligence Community Directive 712: Requirements for Certain Employment Activities by Former Intelligence Community Employees (Mar. 23, 2023).

the procedural safeguards of the Administrative Procedure Act, giving political actors more room to maneuver.[110] Moreover, experience has shown that political considerations are increasingly dictating U.S. export control policy—especially in the context of China.[111] Even where new legislation or designations to the Entity List do explicitly reference human rights (or surveillance software, as in the case of Xinjiang), undertones of U.S. nationalism undermine their credibility.[112]

Economic sanctions reveal a similar trend. Over the past two decades, the United States has relied on economic sanctions to address a wide variety of behavior by foreign adversaries which it seeks to punish but which falls below the threshold of armed conflict.[113] While these sanctions sometimes target regimes with dismal human rights track records, they have been deployed to advance a much wider range of policy goals.[114] This has raised concerns about the long-term efficacy of such approaches (which rely on American control of the global financial system), but also prompted criticisms of the United States' heavy-handed use of its economic weapon.[115] Ironically, while the United States is able to dramatically impact international markets because of its dominant financial position, American unilateralism can also be seen as undermining the legitimacy (and signaling effect) of sanctions directed against surveillance firms.

To mitigate these criticisms, the United States should commit to aligning its decisions to designate surveillance technology companies to the Entity List with well-accepted principles of international human rights law.[116]

---

110. In contrast to other areas of public law, where the Administrative Procedure Act serves as a safeguard (though often weak) against overly politicized agency decision-making, the 2018 Export Control Reform Act explicitly precludes APA-style review. 50 U.S.C. § 4821(a) (2022). Other standards of review, such as *ultra vires*, may remain available. *See* Fed. Express Corp. v. U.S. Dep't of Com., 486 F. Supp. 3d 69 (D.D.C. 2020).

111. *See, e.g.*, Jon Bateman, *The Fevered Anti-China Attitude in Washington is Going to Backfire*, Politico (Dec. 15, 2022), https://www.politico.com/news/magazine/2022/12/15/china-tech-decoupling-sanctions-00071723 [https://perma.cc/KTZ3-4FQT].

112. *See* Edward Wong and Ana Swanson, *U.S. Aims to Expand Export Bans on China Over Security and Human Rights*, N.Y. Times (Jul. 5, 2022), https://www.nytimes.com/2022/07/05/us/politics/us-china-export-controls.html [https://perma.cc/79QU-P9JD].

113. Jacob J. Lew, U.S. Treasury Secretary, Speech on the Evolution of Sanctions and Lessons for the Future (Mar. 30, 2016), https://carnegieendowment.org/2016/03/30/u.s.-treasury-secretary-jacob-j.-lew-on-evolution-of-sanctions-and-lessons-for-future/ivpl [https://perma.cc/ZZ26-275L].

114. Elizabeth Rosenberg, Peter Harrell, Paula J. Dobriansky, and Adam Szubin, Ctr for New Am. Sec., America's Use of Coercive Economic Statecraft (2020), https://www.cnas.org/publications/reports/americas-use-of-coercive-economic-statecraft (noting sanctions have been used to address the "proliferation of weapons of mass destruction (WMD); military aggression by adversaries; terrorism; narcotics trafficking; and mass atrocities, repression, and other serious violations of human rights") [https://perma.cc/48G2-PNZ4].

115. *See, e.g.*, Press Release, Office of the UN High Commissioner for Human Rights, Iran sanctions are unjust and harmful, says UN expert warning against generalised economic war (Aug. 22, 2018), https://www.ohchr.org/en/press-releases/2018/08/iran-sanctions-are-unjust-and-harmful-says-un-expert-warning-against [https://perma.cc/QS9K-QNMY].

116. The relationship between sanctions policy and human rights raises serious questions about the legality of unilateral and coercive sanctions imposed by governments. Because these concerns typically arise in the context of indiscriminate sanctions targeting broad sectors of a sovereign country, they are

Because sanctions are perceived as being more legitimate when implemented by a broad-based coalition and also tend to be more effective when enforced, the United States should also, as a matter of policy, seek to coordinate with other like-minded states to identify and select targets wherever possible.[117] These decisions should likewise consider the effects designations will have on third parties, with particular concern for individuals who are economically vulnerable.

Second, relying solely on the United States to serve as an enforcer is problematic because bureaucratic and institutional considerations make it unlikely that the United States will sanction actors with which it has existing relationships. Federal oversight mechanisms are more robust than they were prior to the Snowden revelations, but U.S. law enforcement agencies have strong incentives to preserve relationships with private contractors.[118] Reports indicating the Federal Bureau of Investigation has flirted with NSO Group products and that the Central Intelligence Agency continues to conduct surveillance on U.S. soil are important reminders that these law enforcement agencies will often opt for less privacy in the name of national security.[119]

These difficulties reflect deep tensions in the relationship between privacy and security and reveal that a reliance on any single state to serve as a global enforcer will not be a lasting solution. A related, more practical concern is the resourcing challenge that enforcement poses. Maintaining a strict regulatory regime depends on having the capacity available to investigate, assess, and prosecute spyware firms that have violated human rights, which in turn depends on political allocation of funding. While the Pegasus Project captivated many policymakers, and the United States has declared its intention to put human rights at the center of its export control policy, it is unclear how long the current momentum will last.

The United States maintains a dominant hold over the global financial system, which gives it a unique ability to make the business models which underpin the surveillance technology industry financially unsustainable. Ec-

---

beyond the scope of this Note. *See, e.g.*, *Bachelet Calls for Major Re-Think Over Impact of Sanctions on Human Rights*, UN News (Sept. 16, 2021), https://news.un.org/en/story/2021/09/1100142 [https://perma.cc/44EE-QS98].

117. Both legitimacy and effectiveness are complicated metrics to evaluate, and no two sanctions regimes are exactly alike. However, multilateral sanctions are broadly considered more legitimate in the eyes of the international community, especially when they have the backing of a UN Security Council Resolution.

118. David Fidler, *Is the Privacy and Civil Liberties Oversight Board Back in Business?* Council on Foreign Relations (Sept. 11, 2017), https://www.cfr.org/blog/privacy-and-civil-liberties-oversight-board-back-business [https://perma.cc/2YJT-D6HW]; *see generally* Perlroth, *supra* note 40 (suggesting that U.S. intelligence agencies continue to purchase technical vulnerabilities from a shadowy marketplace of outside contractors).

119. David Meyer, *The CIA has Been Conducting Mass Surveillance in the U.S. with Minimal Oversight—and the Program's Uncovering is Bad News for Big Tech*, Fortune (Feb. 11, 2022), https://fortune.com/2022/02/11/cia-mass-surveillance-wyden-privacy-shield-meta/ [https://perma.cc/U2Y3-CVL9].

onomically weaker states, on the other hand, will be unable to impose meaningful economic costs using export controls or sanctions. This concentration of power in the hands of a few strong states reflects the current structure of the international system, but it opens export controls to the criticism that they seek to advance U.S. political interests rather than address human rights concerns. Reaching multilateral agreements on law and norms governing spyware in forums like the United Nations and the Export Controls and Human Rights Initiative will be essential for addressing this challenge.

C. Opportunities for Redress Through Civil Litigation

A third potential reform pathway is to expand opportunities for victims of privacy violations to pursue redress through civil litigation in domestic courts.[120] Like victims of other grave abuses, victims of privacy intrusions deserve an opportunity to seek justice. The threat of potential lawsuits arising from human rights violations can also raise the litigation risk that spyware companies face and either a) encourage them to only work with customers with a track record of respecting human rights or b) limit their ability to reinvest profits into more powerful hacking products. Current legal regimes, however, provide only narrow opportunities to bring legal claims for such violations. In particular, jurisdictional challenges and statutory bars pose unique challenges to plaintiffs who may suspect their devices have been infected with malware but have no way of determining who put it there. This Section examines the legal frameworks available in the United States for victims to bring causes of action against spyware companies for privacy violations and suggests areas in which liability may be expanded to make redress available to these unique claimants.

As a starting point, it is worth noting that the "litigation landscape for actions concerning the legal responsibilities of business for human rights harm is constantly changing."[121] Today, there are many more litigation pathways available globally than there were two decades ago.[122]

This Note focuses on the challenges around litigating human rights violations arising from privacy intrusions, where the overall picture is less optimistic. The Alien Tort Statute (ATS), which allows non-citizens to bring tort claims against corporate defendants, has been a primary vehicle for

120. While the International Criminal Court may in theory be a suitable venue for claims involving human rights violations, this Note focuses on domestic courts because they are far more likely mechanisms in which plaintiffs will find themselves litigating (and offer a better chance at financial recovery).

121. Robert McCorquodale, *The Litigation Landscape of Business and Human Rights*, *in* HUMAN RIGHTS LITIGATION AGAINST MULTINATIONALS IN PRACTICE, 1, 1 (Richard Meeran ed., 2021).

122. *Id.*

litigating human rights violations in U.S. courts.[123] This long ignored section of the United States Code dates back to the Judiciary Act of 1789 but gained prominence in the aftermath of *Filártiga v. Peña-Irala*, a Second Circuit decision in which plaintiffs successfully used the statute to bring a claim for wrongful death and torture in U.S. federal court.[124] Since then, the Supreme Court has narrowed its scope dramatically.[125] In *Kiobel v. Royal Dutch Petroleum, Co.,* the Supreme Court determined that a presumption against extraterritorial application applied to federal common law claims recognized under the ATS, barring most cases where all relevant conduct occurred abroad.[126] There is also an open question as to whether the ATS will continue to apply to corporate defendants, which the Court has thus far opted not to resolve.[127] Other statutes, such as the Torture Victims Protection Act (TVPA), face similar challenges, including the exclusion of corporations from liability (though the Court has noted that the TVPA nonetheless "contemplates liability against officers who do not personally execute the torture or extrajudicial killing").[128]

Beyond these general claims, plaintiffs who suspect their devices have been compromised may rely upon several statutory causes of action specific to cyber intrusions. Though primarily a criminal statute, the Computer Fraud and Abuse Act (18 U.S.C. § 1030) also creates a civil cause of action: "any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."[129] Similarly, the Wiretap Act provides: " . . . any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate."[130] In addition to these federal statutory causes of action, plaintiffs can often bring claims based on state law (e.g., the California

123. 28 U.S.C. § 1350 (2022) ("The district courts shall have original jurisdiction of any civil action by an alien for a tort only, committed in violation of the law of nations or a treaty of the United States.")

124. Filártiga v. Peña-Irala, 630 F. 2d 876 (2d Cir. 1980).

125. Paul Hoffman, *International Human Rights Litigation in the United States*, *in* Human Rights Litigation against Multinationals in Practice 168, 168 (Richard Meeran ed., 2021).

126. *Id.* at 173.

127. William S. Dodge, *The Surprisingly Broad Implications of Nestlé USA, Inc. v. Doe for Human Rights Litigation and Extraterritoriality,* Just Security (June 18, 2021), https://www.justsecurity.org/77012/the-surprisingly-broad-implications-of-nestle-usa-inc-v-doe-for-human-rights-litigation-and-extraterritoriality/ [https://perma.cc/4PC5-22M7].

128. *Mohamad v. Palestinian Auth.*, 566 U.S. 449, 458 (2012). *See also* Hoffman, *supra* note 125 at 176 (suggesting that this language "raises the possibility of TVPA actions against corporate officers and managers").

129. 18 U.S.C. § 1030(g) (2022). The statute contains a two-year statute of limitations and bars claims which allege "negligent design."

130. 18 U.S.C. § 2520(a) (2022). The Wiretap Act is a part of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §2510 (2022).

Comprehensive Computer Data Access and Fraud Act) or common law (e.g., breach of contract or trespass to chattel).

Unlike the Alien Tort Statute, the Supreme Court has not ruled decisively on whether the Computer Fraud and Abuse Act (CFAA) applies extraterritorially, though lower court rulings and the text of the statute itself provide strong indications that it does. Key subsections of the statute guard against damage and unauthorized access to a "protected computer," which the CFAA defines as a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[131] District courts in the Ninth Circuit have taken the statute to be "as clear an indication as possible [that the law applies extraterritorially] short of saying 'this law applies abroad.'"[132] Because the statute's language plainly rebuts any presumption against extraterritoriality, other circuits should adopt the view that Congress intended extraterritorial application.

Even so, victims may face jurisdictional challenges and statutory bars. Claims against entities domiciled within the United States, like the California-based internet monitoring firm Blue Coat, will easily meet personal jurisdiction requirements. Personal jurisdiction over companies located outside of the United States is more difficult to establish—though the theories of personal jurisdiction over NSO Group that the court accepted in *WhatsApp v. NSO Group* seem to cast a wide net. In that case, WhatsApp asserted that NSO Group was subject to personal jurisdiction "because they obtained financing from California and directed and targeted their actions at California and its residents, WhatsApp and Facebook" and because defendants agreed to WhatsApp terms of service (including provisions requiring Defendants to submit to personal jurisdiction) by accessing and using WhatsApp.[133] The *Apple v. NSO Group* litigation asserted personal jurisdiction based on a similar theory.[134]

Victims who believe a sovereign government was involved in the violation must also contend with the Foreign Sovereign Immunity Act (FSIA), which withdraws subject matter jurisdiction for suits against nation-state actors in federal court, including suits arising under the Wiretap Act.[135] While the FSIA has some narrow exceptions (claims arising from acts of

131. 18 U.S.C. §1030(e)(2) (2022).

132. In re Apple Inc. Device Performance Litig., 347 F. Supp. 3d 434, 448 (N.D. Cal. 2018) (quoting Ryanair DAC v. Expedia Inc., No. 17-CV-01789-RSL, 2018 WL 3727599, at *2 (W.D. Wash. Aug. 6, 2018)).

133. Complaint, WhatsApp v. NSO Group, No. 3:19-cv-07123-JSC, 2019 WL 5571028, at *3.

134. Complaint, Apple v. NSO Group, No. 3:21-cv-09078-JD, 2021 WL 5490649 (N.D. Cal. Nov. 23, 2021) at *6.

135. Foreign Sovereign Immunities Act (FSIA), 28 U.S.C. §§1602–11 (2022). In *Kidane v. Federal Democratic Republic of Ethiopia*, a case involving the Wiretap Act, the D.C. Circuit affirmed that FSIA bars any suit in federal court against a foreign sovereign. Kidane v. Fed. Dem. Rep. of Eth., 851 F.3d 7, 9 (D.C. Cir. 2017).

terrorism including torture are not barred), legislators fear limiting foreign sovereign immunity any further will invite other governments to take reciprocal actions.

Foreign sovereign immunity does not extend, however, to private-sector actors like NSO Group. In *WhatsApp v. NSO Group*,[136] the Ninth Circuit rejected NSO Group's claim that it is entitled to derivative sovereign immunity because it "enables sovereign governments to investigate and combat terrorism, child exploitation, and other heinous crimes."[137] The panel held that the "Foreign Sovereign Immunity Act . . . occupies the field of foreign sovereign immunity as applied to *entities* and categorically forecloses extending immunity" to any entity that falls outside the definition of a foreign state.[138] When NSO Group sought to appeal the issue, the Supreme Court denied its cert petition.[139] As a result, victims should be able to bring lawsuits against hacking groups directly, following the approach Apple and WhatsApp have taken.[140] The Salvadoran journalists who brought suit in *Dada v. NSO Group* will be the first to test this theory, but the case remains in its preliminary phases.[141]

A final challenge victims face will be asserting standing to bring a claim. Most plaintiffs seeking damages from spyware companies will meet the injury in fact and redressability elements of standing but may face challenges asserting causation or meeting *Ashcroft v. Iqbal*'s pleading requirements.[142] The steepest limitation may be a practical one: while organizations like Apple and WhatsApp have the capacity (and financial incentive) to conduct security investigations in the event their software or devices are compromised, individual journalists or activists frequently lack investigative resources. Even asserting standing may require reams of data and sophisticated digital investigations, and victims must often rely on academic research institutions like CitizenLab, or non-profit subdivisions of corporate actors, like Google's Project Zero, to conduct forensic analysis.

These shortfalls in the current civil litigation regime have led civil causes of action to be relatively underused. If these litigation mechanisms were used to their full potential, they could serve as a powerful tool to curtail the use of spyware against human rights activists. Within Lessig's framework, civil causes of action are legal constraints (i.e., damages awards are penalties that must be paid on threat of contempt) but have strong market effects. Taxes on cigarettes regulate their supply in the market by increasing the

136. WhatsApp Inc. v. NSO Grp. Techs. Ltd., 17 F.4th 930 (9th Cir. 2021).

137. Motion to Dismiss, WhatsApp v. NSO Grp., No. 4:19-cv-07123-PJH, 2020 WL 4282549 (Apr. 2, 2020).

138. WhatsApp v. NSO Grp., 17 F.4th 930, 933 (9th Cir. 2021).

139. NSO Grp. Techs. Ltd. v. WhatsApp Inc., 143 S. Ct. 562 (2023).

140. *See* Perlroth, *supra* note 21. Nothing in the language of the statute precludes individual victims from bringing claims based on these actions.

141. Dada v. NSO Group, The Knight First Amendment Institute (Mar. 15, 2023), https://knightcolumbia.org/cases/dada-v-nso-group [https://perma.cc/4LXE-3GAM].

142. Ashcroft v. Iqbal, 556 U.S. 662 (2009).

marginal cost of production felt by cigarette manufacturers, causing them to produce less and leading to an overall decrease in consumption.[143] Litigation remedies operate similarly as they limit spyware firms' ability to facilitate human rights abuses on a large scale because doing so would expose firms to significant litigation risk, which suppliers will factor into cost per unit they need to recoup before making a profit. As in tort law, this deterrent effect does not negate civil litigations' potential to serve as a vehicle for corrective justice.[144] Instead, it serves as another tool policymakers can use to raise the overall cost of developing and commercializing spyware and force surveillance firm stakeholders to ask hard questions about whether to withdraw their investments.

As noted above, however, the current civil litigation landscape contains some gaps. Though the Computer Fraud and Abuse Act likely allows a broader set of claims to proceed than have been brought in the past, unresolved legal questions about extraterritoriality and jurisdiction cast some uncertainty on the longer-term future of CFAA's availability as a cause of action. Courts should resolve these questions in favor of broadening access to U.S. courtrooms, even if doing so would also result in some unforeseen litigation against U.S. tech giants. Practical barriers to standing present a separate set of issues. Looser causation chains or lower *Ashcroft v. Iqbal* pleading requirements would help individuals whose claims are currently barred, but these changes are unlikely given prevailing jurisprudence. Instead, policymakers should think seriously about investing in tools which help individuals who suspect they have been victims to identify and attribute hacking intrusions so that they may bring lawsuits in the future.

IV. Conclusion

The Pegasus Project's shocking revelations last year unleashed a flurry of regulatory activity directed at the surveillance technology industry. Nearly a year later, new stories of high-profile individuals targeted by NSO Group continue to make headlines. In May 2022, the Spanish government revealed that NSO Group's malware infected the phones of prime minister Pedro Sanchez and defense minister Margarita Robles.[145] For each incident in which NSO Group has targeted high-profile political leaders, however, many more human rights activists have had their lives thrown into upheaval. As the evidence of NSO Group's wrongdoing mounts, individuals like Human Rights Watch Beirut director Lama Fakih and Bahraini lawyer

143. *Cf. Law of the Horse*, *supra* note 69 at 501.

144. *See* Gary T. Schwartz, *Mixed Theories of Tort Law: Affirming Both Deterrence and Corrective Justice*, 75 Tex. L. Rev. 1801, 1802 (1997).

145. Sam Jones, *Spanish Prime Minister's Phone 'Targeted with Pegasus Spyware'*, The Guardian (May 2, 2022), https://www.theguardian.com/world/2022/may/02/spain-prime-minister-pedro-sanchez-phone-pegasus-spyware [https://perma.cc/UJA9-2RE2].

Mohammed al-Tajer are increasingly willing to tell their stories.[146] And yet, NSO Group continues to operate, while paying expensive lawyers and public relations professionals to divert attention from the harms they have perpetrated.

The measures policymakers have enacted to limit NSO Group's reach, while encouraging, are unlikely to quell the broader market for privately developed surveillance exploits. Fresh ideas for how to regulate an industry that has brazenly violated the right to privacy and facilitated the abuse of other internationally recognized human rights, like the right to free expression, are urgently needed.

This Note suggests a potential framework for evaluating the existing policy landscape and offers a glimpse of where those ideas might lie. Applying Lawrence Lessig's ideas about law, norms, markets, and architecture to three categories of legal instruments available to policymakers (with a specific eye toward the relationships between law and markets) this analysis suggests that a smart policy mix will be one that (1) clarifies international human rights obligations that arise from the right to privacy, (2) bases export control regimes on multilateral consensus and recognized principles of human rights law, and (3) expands opportunities for civil litigation in domestic courts.

International human rights instruments have important legal and normative effects. In the privacy context, however, there remains significant uncertainty about what the internationally recognized right to privacy means in the digital age. Policymakers would do well to strengthen international human rights law by clarifying what obligations the right to privacy creates both for states and for businesses under the UNGP. Even if ongoing discussions fall short of establishing hard law, the process of articulation, contestation, and internalization is likely to produce norms which will enable governments and human rights groups to call out bad actors. This will help isolate them and signal that there is significant reputational risk that comes from working with surveillance firms that license their exploits to human rights abusers.

Export controls and criminal sanctions, on the other hand, are an effective tool for curbing spyware firms' profitability because they possess a clear enforcement mechanism—which human rights law lacks. However, these tools occasionally lack legitimacy, especially when wielded unilaterally by the United States. American policymakers should recognize this challenge and incorporate global human rights standards into the United States' export control and sanctions decision-making framework, including adopting

146. *Interview: Phone of HRW Director Attacked Using Pegasus Spyware*, Human Rights Watch (Jan. 26, 2022), https://www.hrw.org/news/2022/01/26/interview-phone-hrw-director-attacked-using-pegasus-spyware [https://perma.cc/8A44-QGMW]; Stephanie Kirchgaessner, '*Most Harmful Thing*'—*How Spyware is Stifling Human Rights in Bahrain*, The Guardian (Feb. 18, 2022), https://www.theguardian.com/news/2022/feb/18/how-spyware-erodes-human-rights-in-bahrain-nso-group-pegasus-project [https://perma.cc/QXT5-KKNQ].

measures for targeting entities that routinely infringe the right to privacy. The United States should also, as a matter of policy, coordinate with other states to identify and select targets wherever possible.

Civil litigation, and particularly civil causes of action under the Computer Fraud and Abuse Act, create more opportunities for holding spyware firms accountable than is typically recognized. Several outstanding questions about extraterritoriality and jurisdiction threaten to undermine CFAA's long-term availability as a cause of action; resolving open questions in favor of broader access to U.S. courtrooms would provide individual victims with an opportunity for redress, while also increasing the financial strain on hacking firms which work with clients that carry out grave human rights abuses. Policymakers should also keep in mind the fact that existing standing and pleading doctrines create practical challenges for many victims who do not have the resources to identify their hackers with specificity; either lowering these doctrinal thresholds or providing additional attribution resources to victims would have a transformative effect on the civil litigation landscape.

These suggestions are only a starting point, and there will be plenty of avenues for future research, including understanding the role of multistakeholder frameworks in curtailing the reach of the spyware industry and assessing the impact the ever-changing architecture of the internet will have on human rights activists. The wide range of policy options available, however, underscores policymakers' lack of attention to the spyware industry's grievous human rights abuses and the urgency with which they must act. It has now been nearly two years since the Pegasus Project, and more than five years since NSO Group's abuses were first documented. In the meantime, as more spyware companies continue to emerge, and countless journalists, opposition politicians, and activists have been harassed or silenced because sophisticated surveillance technologies have given governments the ability to track their every move. Not only do these companies facilitate grave abuses of human rights, but they make a handsome profit from doing so. Policymakers must act immediately to curtail the surveillance industry's global reach.