Nebraska Law Review

Volume 102 | Issue 4 Article 2

2024

Zero Progress on Zero-Days: How the Last Ten Years Created the Modern Spyware Market

Mailyn Fidler
University of New Hampshire Franklin Pierce School of Law, Mailyn.Fidler@law.unh.edu

Mailyn Fidler*

Zero Progress on Zero-Days: How the Last Ten Years Created the Modern Spyware Market

ABSTRACT

Spyware makes surveillance simple. The last ten years have seen a global market emerge for ready-made software that lets governments surveil citizens and foreign adversaries alike and to do so more easily than when such work required tradecraft. The last ten years have also been marked by stark failures to control spyware and its precursors and components. This Article accounts for and critiques these failures, providing a socio-technical history since 2014, focusing on the conversation about trade in zero-day vulnerabilities and exploits and more recently spyware. This Article also applies lessons from these failures to guide regulatory efforts going forward. While recognizing that controlling this trade is difficult, I argue countries should focus on building and strengthening multilateral coalitions of the willing rather than on strong-arming existing multilateral institutions into working on the problem. Individually, countries should focus on entity- or use-based export controls and leverage broader sanctions that target specific bad actors rather than focusing on technology-specific controls. Last, I continue to call for transparency as a key part of oversight of domestic governments' use of spyware and related components.

* Assistant Professor, University of New Hampshire Franklin Pierce School of Law, and Faculty Affiliate, Berkman Klein Center for Internet & Society at Harvard University. Thank you to Katie Moussouris of Luta Security, Trey Herr of the Atlantic Council, Andrew Self of the State Department, and a senior security engineer with insight into the zero-day trade for enlightening conversations about developments in this field. Thank you to Trey Herr, Asaf Lubin, James Shires, and Randy Wheeler for comments, Matt Kristoffersen for research and revision assistance, and Susan Drisko Zago for research guidance. For a repository of primary documents on this topic referenced in this Article, please visit mailynfidler.com/primary-sources-zero-days. As responses to FOIA requests associated with this Article are received, they will be posted there

TABLE OF CONTENTS

I. INTRODUCTION

I began researching zero-day vulnerabilities and possibilities for regulating their use and sale ten years ago.[1] Zero-day vulnerabilities are flaws in computer code that are unknown to the maker of that code and the general public; they are known only to the discoverer and

1. This research culminated in publication of Mailyn Fidler, *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis*, 11 I/S: J.L. & POL'Y INFO. SOC'Y 405 (2015).

whomever they choose to tell. These "secret" flaws in code can be used to build software that enables digital surveillance campaigns—now often called "spyware"—and launch cyberattacks or cyber-subterfuge, making them desirable to governments and private actors alike, for more and less legitimate purposes. In essence, zero-days can be key components of the tools of cyberwar, cyberespionage, and cybercrime.

Like components of traditional weapons, attempting to restrict access to or otherwise regulate the use of zero-days might make sense. When, say, certain weapons are regulated as a whole, trade in components might continue, enabling the eventual assembly of full weapons. The same pattern might apply to zero-day vulnerabilities and cyber-surveillance and -subterfuge software.[2] So, regulators might wish to control both the full package (spyware) and components (zero-days).

In my 2015 article, *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis*, I investigated what options might exist to regulate the trade in zero-day vulnerabilities and exploits domestically and internationally.[3] Domestically, I concluded that the most feasible and desirable approach was executive branch oversight of the U.S. government's practices towards zero-day vulnerabilities and exploits.[4] Internationally, I argued that the most feasible and desirable approach was through voluntary collective action to harmonize export controls on zero-day exploits through a mechanism called the Wassenaar Arrangement.[5]

Since 2015, the domain of zero-days has been riddled with headline-making cyber incidents and substantial regulatory failure. This Article traces these regulatory efforts and ultimate failures, investigating why even the lightest-touch regulatory mechanisms have failed to launch.

My analysis shared in some of that failure: an overly specific focus on zero-days raised definitional problems and complicated implementations that scuttled otherwise promising mechanisms. While policymakers focused narrowly on zero-days or the ill-fated category of "intrusion software," a sophisticated trade in what is now called spyware—monitoring software that may or may not rely on zero-days—has flourished. The regulatory landscape for spyware is less robust as a result of the zero-day regulatory failures, resulting in some good regulatory options effectively becoming non-starters and calls for more extreme measures like moratoriums.[6]

---

2. *But see* MAX SMEETS, NO SHORTCUTS: WHY STATES STRUGGLE TO DEVELOP A MILITARY-CYBER FORCE (2022) (providing reasons to believe that transferring components of spyware operates differently than traditional weapons transfers, because operational knowledge must be transferred with it).
3. Fidler, *supra* note 1.
4. *Id.* at 453–54.
5. *Id.* at 480–81.
6. *Spyware Scandal: UN Experts Call for Moratorium on Sale of 'Life Threatening' Surveillance Tech*, OFF. OF THE HIGH COMM'R. FOR HUM. RTS. (Aug. 12, 2021), https://

Another main driver of this shift towards fewer regulatory possibilities has been the realities of national interest. Overall, countries whose national interests benefit from access to, or sale of zero-days and associated spyware have won out. In the U.S., the policy window to make substantial changes to the government's own use of these tools has narrowed despite promises not to use certain spyware.[7] Internationally, changing power dynamics have made full-scale international cooperation on trade in zero-days and related software essentially moot. Instead, countries are turning to unilateral and smaller-scale multilateral export controls, particularly to restrict commercial sales of the broader category of "spyware" software, which may be built on zero-days, to certain actors.[8] These controls are promising but more limited in scope than a wide-ranging multilateral mechanism.

This Article serves two purposes. First, it provides an account of regulatory and scholarly efforts at this particular intersection of law and technology over the last ten years. Most of the legal debate over this issue has taken place online and in policy circles, so this Article provides a needed written account. This account, which occupies Parts II and III, is necessarily detailed. The last subsection of each Part critically assesses the events of the last ten years and where each issue stands now. Part IV offers broader recommendations informed by the details of these more specific debates over the last ten years.

Part I gives a brief background on zero-days and related technologies themselves, their typical uses, and the broad kinds of applicable regulatory approaches. Part II explores how the market for zero-days and related software has changed over the last decade. Part III addresses the primary demand-side regulation pursued in the U.S., the Vulnerabilities Equities Process. Part III addresses multilateral export controls with respect to zero-days and related technologies. Each of these Parts uses a range of terminology, from zero-days to intrusion software and spyware, reflecting the varied focuses of and terminology used in policy discussions over the past ten years.

Going forward, I argue that countries should lean into unilateral export controls and broader, non-export-control sanctions that restrict or punish those providing a wide range of goods or services to an end "bad actor." This approach differs from the export control and sanctions approaches favored towards zero-days and spyware up to this point, which has usually focused on restricting the export of certain technologies rather than on stymying particular bad actors. Smaller-scale multilateral efforts to coordinate these export controls also seem wise and more achievable than broad multilateral cooperation. Lastly,

---

www.ohchr.org/en/pressreleases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening [https://perma.cc/FDR3-V8CJ].

7. Exec. Order No. 14093, 88 Fed. Reg. 18957 (Mar. 27, 2023).

8. *See infra* Part IV.C.

I recommend something that might seem out of place in a legal debate: fund investigative journalism and related multidisciplinary analysis. Among the most effective policy changes over the last ten years, almost all came in response to reporting about and analysis of abuses of these technologies. Supporting that proven trigger of regulatory action and government transparency seems wise in an atmosphere otherwise marked by inconsistent political will.

II. ZERO DAYS TO SPYWARE BACKGROUND

A. Terminology

Zero-day vulnerabilities are so named because a discoverer can exploit the identified vulnerability on the "zero-th" day (software programmers count from zero, rather than one). This exploitation can occur before the software creator knows about or can fix the vulnerability. What someone can do with a zero-day vulnerability ranges. Some uses are relatively benign, while others are so powerful that they are, as one zero-day discoverer described, "the closest thing we have to magic—enabling access, monitoring, data extraction, and damage."[9]

Zero-day vulnerabilities technically refer to the flaw in the code itself, while code written to take advantage of that flaw is a zero-day exploit.[10] Some coders emphasize this distinction: Zero-days are information, so reports about zero-days themselves are speech that should not be regulated, while exploits are closer to "tools" or "weapons."[11] The debate over this distinction and lack of precision in regulatory efforts has hampered efforts to regulate the market.[12]

Zero-day exploits can be used in a wide range of products, along with non-zero-day elements. As such, names for software that might use zero-days do not necessarily reflect their inclusion. Malware is perhaps the most general term, used to refer to "software that is intentionally included or inserted in a system for a harmful purpose."[13] Malware, as a category, is agnostic to the type of harmful purpose and the actor deploying it, as well as the method of incursion or harm.[14] Importantly,

9. I thank the senior security engineer who spoke with me for this project for this description.
10. *See* Trey Herr & Paul Rosenzweig, *Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model*, 8 J. NAT'L SEC. L. & POL'Y 301, 306 (2016).
11. *See* Fidler, *supra* note 1, at 408–09 (describing market participants' divergent views).
12. *See infra* Part IV.
13. *Glossary*, NAT'L INST. OF STANDARDS & TECH., https://csrc.nist.gov/glossary/term/malware [https://perma.cc/XE3H-RK6A] (last visited Nov. 22, 2023).
14. Ransomware, for instance, is a more specific category of malware that denies access to data in anticipation of a ransom being paid. Ransomware may also include zero-days. *See Stop Ransomware*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/stopransomware [https://perma.cc/CD59-JK6P] (last visited Nov. 22, 2023).

it may or may not include zero-days. As discussed more below, "intrusion software" was a popular, albeit confusing, term used particularly in policy circles.[15]

An increasingly favored term as of this writing is "spyware" or "commercial spyware."[16] These new terms emphasize two aspects: the espionage-related purposes for which the software is used and the non-governmental origin of that software. Again, not all commercial spyware incorporates zero-days, but they certainly can and do. This Article's analysis begins with the zero-day debates of ten years ago. But because spyware is an increasingly important and contested arena in which zero-days are used, and an area where so much recent regulatory efforts focus, this category appears frequently throughout this Article.

B. Use Scenarios

The canonical attack involving zero-days is Stuxnet, the program that sabotaged Iranian uranium enrichment centrifuges. The Stuxnet attack, first launched in 2007, used four zero-day vulnerabilities, an unusually high number.[17] Each vulnerability played a role in the goal of the attack: to disrupt the centrifuges by affecting the industrial control software.[18] The U.S. developed the attack with the help of Israel as part of a broad strategic plan to counter the Iranian nuclear program.[19]

More recently, the zero-day attacks that have received the most attention and sparked calls for reform were those used in the Pegasus spyware, which was developed by NSO Group, an Israeli company.[20] The spyware is not static, but experts have documented its use of multiple zero-days over different versions.[21] Customers used this software to target journalists, the wife of murdered Saudi dissident Jamal

15. *See infra* Part IV.
16. *See infra* notes 188–199.
17. Ryan Naraine, *Stuxnet Attackers Used 4 Windows Zero-Day Exploits*, ZDNET (Sept. 14, 2010, 4:18 AM), https://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/ [https://perma.cc/L7SF-9Z2L].
18. *Id.*; Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon,* WIRED (Nov. 3, 2014, 6:30 AM), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [https://perma.cc/N7CC-JJ35].
19. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Attacks Against Iran*, N.Y. TIMES (June 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=1&hp [https://perma.cc/W7KS-F8DU].
20. David Pegg & Sam Cutler, *What is Pegasus Spyware and How Does It Hack Phones?*, THE GUARDIAN (July 18, 2021, 12:00 PM), https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones [https://perma.cc/X768-C4TH].
21. BILL MARCZAK ET AL., THE GREAT IPWN: JOURNALISTS HACKED WITH SUSPECTED NSO GROUP IMESSAGE 'ZERO-CLICK' EXPLOIT 9 (2020), https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/ [https://perma.cc/Y6C5-D6RS].

Khashoggi, human rights lawyers and activists, political opposition figures, mainstream politicians, and others.[22]

Stuxnet and Pegasus demonstrate how the use of zero-day exploits has evolved over the past ten years. Painting in very broad strokes, zero-days used to be more restricted to sophisticated actors and high politics, such as in Stuxnet. The "elite" nature of zero-day exploits was due in part to the fact that governments were one of the few—although, not only—entities with the personnel skilled enough to identify and exploit such vulnerabilities or the funds to acquire them.[23] Over the last ten plus years, the number of companies offering either zero-days or software incorporating zero-days has grown.[24] These companies sell to government actors, including those without "in house" capabilities, and to other private entities. The expanded availability of zero-days and software incorporating zero-days means that an increasingly wide range of customers can deploy these products in a similarly wide range of everyday politics.[25]

Much more is publicly known now about zero-days as a feature of the cybersecurity ecosystem than ten years ago. A key RAND study demonstrated that zero-days have a fairly long average life expectancy, which increases their value to users. Zero-days have on average a pre-discovery lifespan of 6.9 years. [26] For any given stockpile of zero-days, only about 5.7% had been publicly discovered after a year.[27] Researchers in a second study estimated a higher rediscovery rate, at 14.9%.[28] These features confirm one of the reasons for sustained demand for zero days: they (can) retain utility over time by virtue of their fairly long life expectancy. Certainly, the second study's rediscovery rate is

22. *See* Natalie Kitroeff & Ronen Bergman, *How Mexico Became the Biggest User of the World's Most Notorious Spy Tool*, N.Y. TIMES (Apr. 18, 2023), https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html [https://perma.cc/SXM3-MENB]; Philip Bennett, *Pegasus Spyware Placed on Phone of Jamal Khashoggi's Wife Before his Murder, Washington Post Reports*, PBS FRONTLINE (Dec. 21, 2021), https://www.pbs.org/wgbh/frontline/article/pegasus-spyware-jamal-khashoggi-wife-phone-washington-post/ [https://perma.cc/7KEK-HJ3J]; AMNESTY INT'L, *The Predator Files: Caught in the Net* 30, 32 (2023), https://www.amnesty.org/en/documents/act10/7245/2023/en/ [https://perma.cc/R7AB-BEUB].
23. Elite hackers, like those of the l0pht group, were another source of zero-day vulnerabilities; l0pht pioneered "responsible disclosure" practices that informed today's bug bounties. *See, e.g.*, Craig Timberg, *A Disaster Foretold—And Ignored*, WASH. POST (June 22, 2015), https://www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/ [https://perma.cc/8XS7-A6G6].
24. *See, e.g.*, James Sadowsky, *Zero Tolerance: More Zero-Days Exploited in 2021 Than Ever Before*, MANDIANT (Apr. 21, 2022), https://www.mandiant.com/resources/blog/zero-days-exploited-2021 [https://perma.cc/Y3X6-J4KU] (citing "the expansion of the exploit broker marketplace" as one driver of this growth.)
25. *Id.* (describing the increase in financially motivated zero-day exploitation).
26. LILLIAN ABLON & ANDY BOGART, ZERO DAYS, THOUSANDS OF NIGHTS 33, 43 (RAND Corp. ed., 2017).
27. *Id.*
28. TREY HERR ET AL., TAKING STOCK: ESTIMATING VULNERABILITY REDISCOVERY 15 (2017).

higher but still low as an absolute number. The authors also acknowledge that bugs valuable to the intelligence community may differ in nature and likelihood of rediscovery, further increasing their value.[29] For instance, a vulnerability reserve tailored to targeting consumer devices may require more frequent refreshing than one directed at niche systems, since consumer devices frequently change. For such vulnerabilities, the above rediscovery estimates, and the lessons for their usefulness over time, may be less relevant.[30]

C. Market Changes Overview

The zero-day market has undergone a shift in the last ten years. Ten years ago, independent zero-day sellers or small vendors were prominent.[31] Over the past decade, many of those vendors have exited the market and transitioned to more traditional cybersecurity consulting services.[32] Anecdotally, government contractors have picked up some of the work these smaller companies used to perform.

Full-service spyware companies—which develop software providing the full spectrum of needed services to take full advantage of a zero-day vulnerability—have become more central in the market as well.[33] By offering full-service software, these companies can sell to a broader

29. *See Id.* at 26.
30. I thank Ian Beer for this observation.
31. The Grugq being the canonical example. *See* Andy Greenberg, *Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits*, FORBES (Mar. 23, 2012, 9:43 AM), https://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/?sh=46b2654b2660 [https://perma.cc/VYF7-3QTM].
32. Companies including ReVuln, Arc4dia, Endgame, and Netragard—which were featured in this Author's earlier work—have transitioned to more traditional offerings, according to their public-facing descriptions. *See* Fidler, *supra* note 1, at 419–20 (featuring these companies which have since transitioned to more traditional offerings).
33. *See, e.g.*, Steve Feldstein & Brian Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses* 16 (March 2023) (working paper) (on file with the Carnegie Endowment for International Peace at https://carnegieendowment.org/files/Feldstein_Global_Spyware.pdf [https://perma.cc/CQ78-Z28Y]) (listing NSO Group, Candiru, Cytrox, Circles, and Candiru as examples of full-service spyware companies); D.J. Pangburn, *Inside the Shadowy World of Spyware Makers that Target Activists and Dissidents*, FAST CO. (June 26, 2019), https://www.fastcompany.com/90369108/inside-the-shadowy-world-of-spyware-makers-that-target-activists-and-dissidents [https://perma.cc/C5XV-ZPNY] (listing eSurv and Verint as examples of full-service spyware companies); Steve Feldstein & Brian Kot, *Mapping the Shadowy World of Spyware and Digital Forensics Sales*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Feb. 27, 2023), https://carnegieendowment.org/programs/democracy/commercialspyware [https://perma.cc/7NVC-55LK] (listing Quadream, Paragon, Mollitiam, DigiTask, DarkMatter, Dark Caracal, Cyberbit, and Black Cube as examples of full-service spyware companies).

range of less sophisticated clients.[34] Another key change is that companies are offering this full-service software as a service—clients sign up and receive use of (but not copies of) spyware, for instance, over cloud services.[35] This shift to software-as-a-service has substantial implications for regulating zero-days, discussed below.

Despite these market shifts, Max Smeets argues that some of the inherent dynamics of this market have actually limited the market's international reach.[36] In particular, Smeets argues that government buyers tend to buy from vendors they can trust—or possibly exert control over—and those vendors tend to be from their own geographic area.[37] Other factors increasing this need to work with trusted entities include the difficulty of pricing these tools that may hold their full value only for a short time and the need to purchase tools that meet secret intelligence goals without advertising those objectives.[38] And governments without existing cyber capacity need both the tools and the human capital to deploy it, again increasing incentives to work with trusted entities.

But others disagree with the conclusion that these needs effectively regionalize markets. For example, Moussouris argued that while Smeets' observations about purchasing are correct and that the "regional" limits may hold for some countries, elite countries tend to work with elite vendors, and these elite vendors are not necessarily within-region. Other non-elite countries may not have vendors, elite or otherwise, within their geography to turn to, either, and so may shop internationally even if, all things considered, they prefer to shop regionally. Therefore, a certain portion of the market will remain international. Similarly, Smeets' arguments about trust may be true for "component" vendors—those selling only exploits, perhaps—but might differ for companies offering full-service products.[39]

---

34. WINNONA DESOMBRE ET AL., COUNTERING CYBER PROLIFERATION: ZEROING IN ON ACCESS-AS-A-SERVICE (Mar. 1, 2021), https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/ [https://perma.cc/8LX4-E8ZD].
35. *See, e.g.*, Brian de Luna et al., *What Products are Available on the Malware Markets?*, NEW AM., https://www.newamerica.org/in-depth/malware-markets/what-products-are-available-malware-markets/ [https://perma.cc/6WYK-6V66] (last visited Oct. 16, 2023).
36. SMEETS, *supra* note 2; Max Smeets, *Cyber Arms Transfer: Meaning, Limits, and Implications*, 31 SEC. STUD. 65 (2022); Max Smeets, *Hack Global, Buy Local: The Inefficiencies of the Zero-Day Exploit Market,* LAWFARE (June 6, 2022), https://www.lawfaremedia.org/article/hack-global-buy-local-inefficiencies-zero-day-exploit-market [https://perma.cc/Z46A-4Y9T].
37. SMEETS, *supra* note 2, at 154–55, 157.
38. *Id.* at 155–56.
39. I thank Trey Herr for this observation. *See also* Katie Collins, *Hacking Team's Oppressive Regimes Customer List Revealed in Hack*, WIRED (June 7, 2015), https://www.wired.co.uk/article/hacking-team-spyware-company-hacked [https://perma.

Bug bounty programs, which offer payments for reports of vulnerabilities to a legitimate source, have also experienced a substantial shift over the last ten years.[40] Bug bounties "match" bug hunters with companies offering payouts for reports or demonstrations of particular vulnerabilities.[41] This Article uses the term "bug bounties" only to refer to transactions between bug hunters and legitimate buyers, meaning companies in whose software a bug originates or a central clearinghouse that ultimately works with such companies.

The structure of bug bounties varies. Some software companies run bug bounties themselves, paying only for vulnerabilities reported in their own software; other programs are independent and accept a range of vulnerability reports.[42] Bug bounties vary in their approach, but the standard model includes offering payouts for reports or demonstrations of particular vulnerabilities.

Ten years ago, policy efforts were directed at increasing bug bounties, a response to two concerns, one more realistic than the other. First, bug bounties provided a way to compensate security researchers for disclosure.[43] Second, they provided a way to divert at least a certain kind of hacker from less legitimate customers.[44] The efforts worked, at least measured by volume: Bug bounties now abound.[45] Even the Department of Defense launched a version.[46] HackerOne, a website that collects bug bounty opportunities, lists hundreds of such programs hosted by entities ranging from dating apps to the restaurant chain Kentucky Fried Chicken (KFC).[47] More than that, platforms like HackerOne's

---

cc/HSV9-XMKW] (demonstrating one well-known full-service company's customer list had an impressive international reach).

40. *See* INT'L ORG. FOR STANDARDIZATION & INT'L ELECTROTECHNICAL COMM'N, ISO/IEC Standard 29174:2018 (available at https://www.iso.org/obp/ui/#iso:std: iso-iec:29147:ed-2:v1:en [https://perma.cc/RB7A-PAJG]) (providing outlined guidelines for receiving and sending vulnerability reports).
41. *See* RYAN ELLIS & YUAN STEPHENS, BOUNTY EVERYTHING: HACKERS AND THE MAKING OF THE GLOBAL BUG MARKETPLACE 6 (2022), https://datasociety.net/library/bounty-everything-hackers-and-the-making-of-the-global-bug-marketplace/ [https://perma.cc/Y4V8-6KW8].
42. For an example of a clearinghouse program, *see, e.g.*, ZERO DAY INITIATIVE, https://www.zerodayinitiative.com/ [https://perma.cc/FDK3-8WYJ] (last visited Feb. 27. 2024); OPEN BUG BOUNTY, https://www.openbugbounty.org/about/ [https://perma.cc/4JEY-XLYB] (last visited Oct. 15, 2023).
43. ELLIS & STEPHENS, *supra* note 41, at 39–40 (see description of "no more free bugs" protest).
44. *Id.* at 40 ("Behind the protest stood a more worrisome reality: if companies weren't going to pay for bugs in their systems, someone else certainly would.").
45. ELLIS & STEPHENS, *supra* note 41, at 7, 14; 42–43.
46. *Vulnerability Disclosure Program (VDP) Overview*, DEP'T OF DEFENSE CYBER CRIME CTR., https://www.dc3.mil/Missions/Vulnerability-Disclosure/Vulnerability-Disclosure-Program-VDP/ [https://perma.cc/5CZB-JBV9] (last visited Oct. 15, 2023).
47. *See Bug Bounty Programs*, HACKERONE, https://hackerone.com/bug-bounty-programs [https://perma.cc/U775-NV32] (last visited Oct. 15, 2023).

help streamline the process so that various entities can establish bug bounties more easily, much like setting up an Etsy storefront.[48]

But this growth has not always resulted in increased security posture or in diverting key players from other markets for bugs. The bugs reported in these kinds of programs are not typically of the same caliber as those that interest nation states. Bug bounties also do not guarantee that the receiving companies will fix bugs that are reported.[49] Nor do bug bounties incentivize companies to improve their security at the design stage, in part because bug bounties can financially reward security engineers for bug discovery in finished products more than taking a salaried position in software development might.[50]

Bug bounties also have—very generally speaking—diverted lower-skilled bug hunters away from the broader market, while high-end hackers still find more lucrative opportunities with high-end clients.[51] Bugs that are interesting to high-end clients, such as intelligence services, are typically the ones that can inflict the most damage.[52] Given this dynamic, bug bounties seem to have curbed trade in the most severe vulnerabilities the least. That said, at least one study of the Russian market suggests pricing in "underground" markets is sometimes similar to and sometimes above bug-bounty pricing, providing some evidence that the gap between the two markets may not be as big as supposed.[53]

Some in the bug bounty community bemoan the small security gains that the successful growth in bug bounties has prompted and point to software liability—once anathema—as a possible solution.[54] Bug bounties do not translate into security success unless companies face

48. *See HackerOne Bounty*, HACKERONE, https://www.hackerone.com/product/bug-bounty-platform [https://perma.cc/J3D4-BEQT] (last visited Oct. 15, 2023); ELLIS & STEPHENS, *supra* note 41, at 13.

49. *See, e.g.*, Vlad Garbuz, *How to Stop Wasting Security Budget on Bug-Bounties*, LINKEDIN (June 26, 2018), https://www.linkedin.com/pulse/how-stop-wasting-security-budget-bug-bounties-vlad-garbuz [https://perma.cc/9ZYY-BE2Y]; Anders Reeves, *Pen Testing vs. Bug Bounties: Which is Best for Business?*, CYBER MAG. (July 22, 2023), https://cybermagazine.com/articles/pen-testing-vs-bug-bounties-which-is-best-for-business [https://perma.cc/H8HM-2DDS].

50. *See, e.g.*, Ryan Ellis et al., *Fixing a Hole: The Labor Market for Bugs*, *in* NEW SOLUTIONS FOR CYBERSECURITY 129–159 (Howard Shrobe, David L. Shrier, & Alex Pentland, eds., 2018).

51. I thank Katie Moussouris for this observation. *See* ELLIS & STEPHENS, *supra* note 41, at 5–7; *see also* Adversary Academy Research, *Confessions of a Top-Ranked Bug Bounty Hunter*, MEDIUM (Feb. 15, 2023), https://piffd0s.medium.com/confessions-of-a-top-ranked-bug-bounty-hunter-5f4d71d34598 [https://perma.cc/BW2M-ST4M] (providing an example account by a bug bounty participant making the same point).

52. *See supra* notes 17–19 and accompanying text (discussing Stuxnet).

53. Luca Allodi, *Economic Factors of Vulnerability Trade and Exploitation*, PROCEEDINGS OF THE 2017 AGS SIGSAC CONF. ON COMP. & COMM. SEC. 1483 (2017).

54. Signs of this shift are also evident in the Biden Administration's *National Cybersecurity Strategy*, WHITE HOUSE 20 (Mar. 1, 2023), https://www.whitehouse.gov/

consequences for failing to act on information provided to them. From a security stance, this argument makes some sense: adding liability in constrained circumstances, such as for failing to implement a security patch that a bug bounty participant started or provided, might be worth exploring.[55] Introducing liability when companies fail to respond or respond in a timely manner, fits into principles that have been introduced about software liability in general, including principles of failure to respond to notices of defects, duties to inspect, and duties to repair promptly.[56] Google's Project Zero 90-day deadline could be a model for what qualifies as a timely response.[57] However, adding liability might discourage companies from offering bug bounties for their own products, removing one tool in their security toolkit.

D. Regulatory Overview

Broadly speaking, two avenues to regulate either zero-days or associated software exist: regulating the market or regulating use. Each avenue can exist at the domestic or international level. Regulating the market can involve either seller-side or buyer-side regulations. Seller-side regulations place restrictions on those who discover and otherwise offer zero-days and associated software for sale. Buyer-side regulations place regulations on those who purchase zero-days and associated products, which can include government clients. Regulating use of zero-days and spyware involves placing restrictions on whether or how zero-days can be used; this kind of regulation also can encompass government actors as well.

As Table 1 sets out, the primary efforts to regulate the market over the last decade have been seller-side, with various attempts to implement export controls on zero-day-related technologies. Export controls come in a variety of forms, but most prohibit sellers within a particular jurisdiction from exporting certain products to certain buyers without approval from the government. More recently, the U.S. implemented restrictions on some government purchases of spyware and launched a multilateral export control code of conduct. Use regulation efforts over the last decade have been fewer and weaker. The primary use regulation in the U.S. has been a government process called the Vulnerabilities Equities Process, which details procedures for deciding whether

wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [https://perma.cc/X6LA-LVM2].

55. I thank Peter Swire and Bryan Choi for developing this suggestion in conversation.

56. *See, e.g.,* Andrea Matwyshyn, *Hidden Engines of Destruction: The Reasonable Expectation of Code Safety and the Duty to Warn in Digital Products*, 62 FLA. L. REV. 109, 135–36 (2021); Bryant Walker Smith, *Proximity-Driven Liability*, 102 GEO. L.J. 1777, 1806–07 (2014).

57. *See Project Zero: Vulnerability Disclosure Policy*, PROJECT ZERO, https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-policy.html [https://perma.cc/ZZX5-6PFN] (last visited Feb. 27, 2023).

and how government actors should keep—and therefore remain able to use—or disclose vulnerabilities of which they know. More recently, the U.S. has added restrictions on government use of certain kinds of spyware, and various entities have called for regional or global moratoriums on use.

Table 1: Categories of Regulation for Zero-Days and Associated Technologies

Category of Regulation	**U.S. Domestic Effort**	**International Effort**
Market (seller- or buyer-side restrictions)	Export controls[58] (seller-side restrictions) Spyware Executive Order[59] (buyer side-restrictions) Visa restrictions on individuals associated with financial gain from misuse of commercial software[60] Proposed use of Magnitsky Act sanctions[61]	Wassenaar Arrangement[62] (seller-side restrictions) Multilateral export control code of conduct[63] Proposed global spyware moratorium (on sale/transfer)[64]

58. *See* Information Security Controls: Cybersecurity Items, 86 Fed. Reg. 58205 (Oct. 21, 2021); 15 C.F.R. § 774 Supp. 1 (2024) (providing a commerce control list, which includes 4A005, 4D004, 4E001.c, 4D001.a, 4E001.a).
59. *See, e.g.*, Exec. Order No. 14093, 88 Fed. Reg. 18957 (Mar. 27, 2023).
60. Press Release, Anthony Blinken, Dep't of State, Announcement of a Visa Restriction Policy to Promote Accountability for the Misuse of Commercial Spyware (Feb. 5, 2024), https://www.state.gov/announcement-of-a-visa-restriction-policy-to-promote-accountability-for-the-misuse-of-commercial-spyware/ [https://perma.cc/PH9N-JVUD].
61. Letter from Ron Wyden et al., to Janet Yellen, U.S. Sec'y of Treasury, & Anthony Blinken, U.S. Sec'y, of State (Dec. 15, 2021), https://www.wyden.senate.gov/imo/media/doc/Magnitsky%20Letter%20to%20Sec.%20Yellen%20&%20B linken.pdf [https://perma.cc/3NMT-ECCD].
62. WASSENAAR ARRANGEMENT SECRETARIAT, LIST OF DUAL-USE GOODS AND TECHNOLOGIES AND MUNITIONS LIST 80–81 (2022), https://www.wassenaar.org/control-lists/ [https://perma.cc/T26Y-6ZX2] (providing 4.D.4; 4.E.1.c as examples).
63. *Fact Sheet: Advancing Technology for Democracy*, WHITE HOUSE (Mar. 29, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/29/fact-sheet-advancing-technology-for-democracy-at-home-and-abroad/ [https://perma.cc/HL5M-T94R].
64. David Kaye, *UN Expert Calls for Immediate Moratorium on the Sale, Transfer, and Use of Surveillance Tools, United Nations Human Rights Office of the High Commissioner* (June 25, 2019), https://www.ohchr.org/en/press-releases/ 2019/06/

Use	Vulnerabilities Equities Process[65] Spyware Executive Order[66] (government use restrictions) Visa restrictions on individuals associated with misuse of commercial software[67]	Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware (government use portion)[68] Proposed European Union spyware restrictions[69] Proposed global spyware moratorium (on use)[70]

III. DOMESTIC REGULATION: VULNERABILITIES EQUITIES PROCESS

A. VEP Introduction

The use regulation that received the most traction in the U.S. over the last decade is the Vulnerabilities Equities Process (VEP), although it is only very narrowly a use regulation. The VEP is a U.S. government policy regulating government decision-making about keeping or disclosing zero-day vulnerabilities.[71] Keeping a vulnerability means it can be used for government purposes, from espionage to cyberattacks. Disclosing a zero-day means the relevant company has an opportunity to patch the vulnerability, and the government can no longer use the vulnerability. Other questions that inform the VEP include: What factors should the government consider when deciding whether to retain

---

un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance [https://perma.cc/E35G-XFBD].

65. *Vulnerabilities Equities Policy and Process for the United States Government*, WHITE HOUSE (Nov. 15, 2017), https://trumpwhitehouse.archives.gov/sites/ whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF [https://perma.cc/P8JD-SNHV].
66. *See, e.g.*, Exec. Order No. 14093, 88 Fed. Reg. 18957 (Mar. 27, 2023).
67. Blinken, *supra* note 60.
68. Press Release, Office of the Press Sec'y, Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware (Mar. 30, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/ [https://perma.cc/2DQH-B7RW].
69. Molly Killeen, *EU Parliament Calls for 'De Facto Moratorium' on Spyware*, EURACTIV (May 9, 2023), https://www.euractiv.com/section/digital/news/eu-parliament-adopts-calls-for-de-facto-moratorium-on-spyware/ [https://perma.cc/F8HF-XACL].
70. Kaye, *supra* note 64.
71. *Vulnerabilities Equities Policy and Process, supra* note 65.

or disclose a vulnerability? And how much should the government share with the public about the parameters of its decision-making processes and actual decisions to disclose a vulnerability? These questions largely relate only to retention, disclosure, and transparency aspects of government use of zero-days. The VEP does not regulate, for instance, particular ways that the U.S. government can use or operationally integrate vulnerabilities. In this way, the VEP is a narrow-use regulation.

Although it is primarily a use regulation, the VEP also has market effects. Whether and how long agencies may keep vulnerabilities affects what kinds of vulnerabilities and exploits they are willing to source, whether in-house or through outside vendors. A pro-disclosure policy on the part of U.S. agencies could dampen U.S. government market demand because vulnerabilities could not be kept for as long, perhaps lessening their utility.[72] Alternately, perhaps a pro-disclosure policy could increase demand, either by upping prices on highly valuable vulnerabilities, or by requiring government actors to purchase replacements for disclosed vulnerabilities. As explored more below, a wrinkle of the VEP has also had market effect; bugs known to contractors and incorporated into systems used by government agencies do not go through the VEP.[73] So, the VEP, as formed, also encourages reliance on full-service contractors rather than on in-house or direct vendor sourcing.

My 2015 article addressed domestic regulation and VEP regulation. More specifically, I called for expanded executive branch oversight of zero-day use and procurement.[74] At the time, this option appeared to be the most politically feasible and practically tractable. In particular, the article recommended increased interagency coordination through purchase price sharing, which could lower prices for government agencies while also bringing government prices closer to those paid out in bug bounties.[75]

The article also recommended strengthening the Vulnerabilities Equities Process (VEP).[76] I argued for increased transparency in the VEP, while noting that transparency is an initial step that only goes so far.[77] Increasing the VEP's transparency lacks enforceability measures unless those transparency measures are codified—a significant

72. *See, e.g.*, Brian Fung, *The NSA Hacks Other Countries by Buying Millions of Dollars' Worth of Computer Vulnerabilities,* WASH. POST (Aug. 31, 2013, 1:05 PM), https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/ [https://perma.cc/6P6S-BPY6] (confirming U.S. participation in the market, reporting on the NSA's expenditure of $25 million plus to procure vulnerabilities on the private market).
73. *See infra* note 124.
74. Fidler, *supra* note 1, at 451.
75. *Id.* at 452.
76. *Id.* at 453–54.
77. *Id.* at 445–52.

drawback. But, given the politics of government cyber operations, this light-touch approach seemed the most politically palatable option despite its limitations.

B. The Last Ten Years

In the last decade, U.S. policymakers interested in the zero-day issue focused much of their attention on the VEP. In particular, these efforts focused on increasing transparency and structuring decision-making about agencies' use of zero-days. This section focuses on the U.S.'s VEP, but it is worth noting that other countries publicly announced VEPs, at least in name, over the last ten years, including in the United Kingdom (2018), Canada (2017), and Australia (2019).[78]

To briefly recap the U.S. VEP's history, the VEP took its first formal form in 2010—although that fact was not known until years later, when the U.S. government declassified that version in response to efforts under the Freedom of Information Act (FOIA).[79] Edward Snowden's

78. *See, e.g.*, Charlotte G., *The UK's Vulnerability Equities Process and the Role of the National Cyber Security Centre* (Oct. 2018), *in* BUILDING COMMON APPROACHES FOR CYBERSECURITY AND PRIVACY IN A GLOBALIZED WORLD 5, 108–11 (Randal S. Milch et al. eds., 2020); *The Equities Process*, GCHQ (Nov. 29, 2018), https://www.gchq.gov.uk/information/equities-process [https://perma.cc/3UWA-MYPU]; Matthew Braga, W*hen Do Canadian Spies Disclose the Software Flaws They Find? There's a Policy, But Few Details*, CBC NEWS (Sept. 6, 2017, 5:00 AM), https://www.cbc.ca/news/science/canada-cse-spies-zero-day-software-vulnerabilities-1.4276007 [https://perma.cc/6EML-6H9N]; Kevin Townsend, *Australia's Intelligence Agency Publishes Its Vulnerability Disclosure Process*, SECURITYWEEK (Mar. 18, 2019), https://www.securityweek.com/australias-intelligence-agency-publishes-its-vulnerability-disclosure-process/ [https://perma.cc/8V3H-LFZV]; *Responsible Release Principles for Cyber Security Vulnerabilities*, AUSTRALIAN SIGNALS DIRECTORATE, https://www.asd.gov.au/sites/default/files/2022-03/Responsible-Release-Principles-for-Cyber-Security-Vulnerabilities.pdf [https://perma.cc/8MSG-XY9V] (last visited Oct. 15, 2023). The Netherlands and Germany are also sometimes included in this list. However, I was unable to find documents supporting their public disclosure of a vulnerability equities process for government actors, which is different from their announced coordinated vulnerability disclosure programs, which focus on private actors. *See, e.g.*, Sven Herpig & Ari Schwarz, *The Future of Vulnerabilities Equities Processes Around the World*, LAWFARE (Jan. 4, 2019, 12:30 PM), https://www.lawfaremedia.org/article/future-vulnerabilities-equities-processes-around-world [https://perma.cc/ZPQ4-LNB3].

79. For a helpful account of the VEP's history up until 2016, see Ari Schwartz & Robert Knacke, *Government's Role in Vulnerability Disclosure*, BELFER CTR. (June 2017); *see also Vulnerabilities Equities Policy and Process (VEP)*, ELEC. FRONTIER FOUND. (Jan. 2016) https://www.eff.org/document/vulnerabilities-equities-process-january-2016 [https://perma.cc/5CEA-KE82] (providing a policy document released by the National Security Agency (NSA) in response to a Freedom of Information Act (FOIA) lawsuit brought by the Electronic Frontier Foundation); Electronic Frontier Foundation v. National Security Agency, No. 14-cv-03010-RS, 2016 WL 1059389 (N.D. Cal., Mar. 17, 2016); *see also EFF v. NSA, ODNI—Vulnerabilities FOIA*, ELEC. FRONTIER FOUND., https://www.eff.org/cases/eff-v-nsa-odni-vulnerabilities-foia [https://perma.cc/2UPD-GL6N] (last visited Oct. 16, 2023) (describing

2013 disclosures provided the first major source of information about the VEP, including about the National Security Agency's (NSA) use and purchase of vulnerabilities.[80] On the heels of these disclosures, the dramatic 2014 Heartbleed vulnerability in a key internet security protocol spurred interest in whether and how the NSA and other government agencies were keeping or disclosing vulnerabilities.[81] In the wake of Heartbleed, the Obama Administration's Cybersecurity Coordinator Michael Daniel publicly discussed the Administration's commitment to "reinvigorating" the government's vulnerability disclosure policy.[82] This language raised obvious questions: why did this policy need reinvigorating? And what counted as reinvigoration?

That was the context in which I wrote my original article. The process has since remained opaque, despite Daniel's blogpost signaling an interest in transparency. The Electronic Frontier Foundation's (EFF) FOIA efforts, which began in 2014, did not reveal what the Obama Administration's call for "reinvigoration" of the VEP after the Heartbleed incident meant. The FOIA request also did not seek any data about VEP disclosure decisions.[83] Other than that FOIA release, the government did not release additional information about the VEP until 2017.

In 2017, another disclosure, the Shadow Brokers leak, released information about several zero-days kept by the NSA. Over eight months, the group released over a gigabyte of software exploits allegedly attributable to the NSA.[84] Significantly, some of these vulnerabilities existed in Microsoft Windows systems and the SWIFT banking

---

EFF's efforts to gain access to the government's Vulnerability Equities Process policy via a FOIA lawsuit).

80. *See, e.g.*, Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. TIMES (July 13, 2013), https://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html [https://perma.cc/3N45-AWMX].

81. *See The Heartbleed Bug*, SYNOPSYS, INC. (June 3, 2020, 4:39 PM), https://heartbleed.com [https://perma.cc/TH2Y-HK3W].

82. Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, OBAMA WHITE HOUSE ARCHIVES: BLOG (Apr. 28, 2014, 3:00 PM), https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities [https://perma.cc/8B7U-LJ4W].

83. *See* Comp. for Injunct. Relief for Violation of the Freedom of Information Act, Electronic Frontier Foundation v. National Security Agency, No. 3:14-cv-03010-JCS (N.D. Cal., Mar. 17, 2016), 2014 WL 3058315.

84. Matt Burgess, *Hacking the Hackers: How Everything You Need to Know About Shadow Brokers Hack on the NSA*, WIRED (Oct. 4, 2017, 10:22 AM), https://www.wired.co.uk/article/nsa-hacking-tools-stolen-hackers [https://perma.cc/42CZ-8RTF].

system.[85] Microsoft openly criticized the NSA for "stockpiling" vulnerabilities after Shadow Brokers.[86]

This leak reignited interest in the VEP. Notably, Congress started paying attention. In 2017, two bills were introduced in Congress to codify the VEP and institute transparency requirements.[87] The first bipartisan bill, the Protecting Our Ability to Counter Hacking (PATCH) Act, was sponsored in the Senate by Senators Brian Schatz of Hawai'i, Ron Johnson of Wisconsin, and Cory Gardner of Colorado—all members of the Senate Committee on Commerce, Science, and Transportation.[88] Representatives Ted Lieu of California and Blake Farenthold of Texas sponsored the bill in the House.[89] The PATCH Act would have required much of what was ultimately formalized in the 2017 VEP Charter, including a review board for vulnerabilities and transparency requirements.[90] The second bill, the Cyber Vulnerability Disclosure Reporting Act (CVDRA), was narrower in scope, and would have required the Department of Homeland Security to issue policies for government agency disclosure of vulnerabilities and reports on instances where disclosures occurred and led to mitigation.[91] Both bills were ultimately unsuccessful, although the CVDRA's sponsor reintroduced the bill in early 2023.[92]

85. Clare Baldwin, *Hackers Release Files Indicating NSA Monitored Global Bank Transfers*, REUTERS (Apr. 14, 2017, 2:40 PM), https://www.reuters.com/article/us-usa-cyber-swift-idUSKBN17G1HC?il=0 [https://perma.cc/P2MB-MC96].

86. Brad Smith, *The Need for Urgent Collective Action to Keep People Safe Online: Lessons From Last Week's Cyberattack*, MICROSOFT: MICROSOFT ON THE ISSUES (May 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.001c8i11317l0f3vs2f1cm2qoliu3 [https://perma.cc/65NC-6C79].

87. Mailyn Fidler & Trey Herr, *PATCH: Debating Codification of the VEP*, LAWFARE (May 17, 2017, 5:46 PM), https://www.lawfaremedia.org/article/patch-debating-codification-vep [https://perma.cc/8KAD-75HV].

88. Press Release, Sen. Brian Schatz, Bipartisan, Bicameral Lawmakers Introduce Bill to Enhance Cybersecurity, Promote Transparency (May 17, 2017), https://www.schatz.senate.gov/news/press-releases/bipartisan-bicameral-lawmakers-introduce-bill-to-enhance-cybersecurity-promote-transparency [https://perma.cc/CZ5H-PCMN].

89. *Id.*

90. Protecting Our Ability to Counter Hacking Act, S. 1157, 115th Cong. (2017).

91. Nate Cardozo & Andrew Crocker, *A Step in the Right Direction: House Passes Cyber Vulnerability Disclosure Reporting Act*, ELEC. FRONTIER FOUND. (Jan. 12, 2018), https://www.eff.org/deeplinks/2018/01/step-right-direction-house-passes-cyber-vulnerability-disclosure-reporting-act [https://perma.cc/PN55-9L9V].

92. Cyber Vulnerability Disclosure Reporting Act, H.R. 280, 118th Cong. (as referred to H. Subcomm. on Cybersecurity and Infrastructure Prot., Feb. 8, 2023).

Table 2: VEP Timeline

Date	Event
2008	Bush NSPD 54[93]
2010	First form of current VEP[94]
2013	Snowden disclosures
2014	Heartbleed blog post[95] EFF FOIA suit filed
2016	EFF FOIA response
2017	Shadow Broker leak PATCH Act and Cyber Vulnerability Disclosure Reporting Act introduced Revised VEP Charter[96]
2019	50 U.S. Code Section 3316 passed, requiring annual reports to Congress
2022	Amendment to 50 U.S. Code Section 3316 passed, requiring public disclosures of certain information.

Potentially to forestall such legislative action, the Trump Administration released the full VEP Charter to the public in November 2017.[97] Indeed, the VEP Charter looked remarkably similar to the requirements of the PATCH Act.

The key differences between the 2017 VEP and the 2010 VEP largely involve transparency and formalization. The 2017 VEP provides that an annual report to be shared with participating agencies will be produced with "an executive summary written at an unclassified level" and "annual reporting *may* be provided to the Congress."[98] This language does not specifically require that the unclassified executive summary be shared with the public, nor does it require Congressional reports; rather, the VEP uses the discretionary word "may."

93. The White House, National Security Presidential Directive/NSPD–54 & Homeland Security Presidential Directive/HSPD–23 (Jan. 8, 2008), https://irp.fas.org/offdocs/nspd/nspd-54.pdf [https://perma.cc/PC3N-YSAC].
94. *Vulnerable Equities Process (VEP)*, *supra* note 79.
95. Daniel, *supra* note 82.
96. *Vulnerabilities Equities Policy and Process for the United States Government*, *supra* note 65.
97. *See* Andi Wilson Thompson, *Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter*, Lawfare (Jan. 13, 2021), https://www.lawfaremedia.org/article/assessing-vulnerabilities-equities-process-three-years-after-vep-charter [https://perma.cc/R7AL-39EF].
98. *Vulnerabilities Equities Policy and Process for the United States Government*, *supra* note 65, at 5.

In addition to transparency, the new VEP Charter formalizes aspects of the VEP that were either slightly less structured or (presumably) redacted in the 2010 VEP. The Charter establishes an "Equities Review Board" composed of representatives from about a dozen government agencies, designating the NSA as the logistical head of the process.[99] The Charter also includes core principles to guide the Board's decisions about release or stockpiling, including considering the "overall best interests of USG missions" along with factors including "prevalence, reliance, and severity."[100]

Pursuant to the VEP, the U.S. government has publicly acknowledged only one disclosure of a vulnerability to a company.[101] In 2020, the NSA shared a "catastrophic" vulnerability in Microsoft's operating system with the company so that it could be fixed; the NSA also acknowledged this exchange publicly.[102]

The Trump Administration's decision to release a public VEP Charter did not totally dissuade Congress from action. In 2019, Congress returned to the issue of VEP codification in a new way, in a move that went almost unnoticed by the VEP-interested policy community.[103] In the Intelligence Authorization Act for 2018–2020, Congress codified Congressional transparency requirements for the VEP.[104] Senator Angus King of Maine appears to be the author of this language, which passed through the Senate Intelligence Committee.[105]

The language requires, among other things, annual reports to Congress that include the total number of vulnerabilities that went through the process (classified),[106] the number of those vulnerabilities disclosed (classified),[107] the aggregate number of vulnerabilities

99. *Id.* at 3–4.
100. *Id.* at 7.
101. Ellen Nakashima, *The Cybersecurity 202: Here's Why the NSA Rushed to Expose a Dangerous Computer Bug*, WASH. POST (Feb. 6, 2020), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/02/06/the-cybersecurity-202-here-s-why-nsa-rushed-to-expose-a-dangerous-computer-bug/5e3b0f41602ff15f8279a52e/ [https://perma.cc/3KQJ-8DKC].
102. *Id.*
103. 50 U.S.C. § 3316a.
104. Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020, S. 1589, 116th Cong. (2019).
105. Press Release, Sen. Angus King, Senate Intel Committee Unanimously Passes Intelligence Authorization Act with Key Collins, King Provisions Included (May 15, 2019), https://www.king.senate.gov/newsroom/press-releases/senate-intel-committee-unanimously-passes-intelligence-authorization-act-with-key-collins-king-provisions-included [https://perma.cc/R8NR-DHK6]; Press Release, Sen. Susan Collins, Senate Intel Committee Unanimously Passes Intelligence Authorization Act with Key Collins, King Provisions Included (May 15, 2019), https://www.collins.senate.gov/newsroom/senate-intel-committee-unanimously-passes-intelligence-authorization-act-key-collins-king [https://perma.cc/5EUM-99UC].
106. § 3316a(c)(1)(A).
107. § 3316a(c)(1)(B).

disclosed (unclassified),[108] and the number of disclosed vulnerabilities subsequently patched (unclassified).[109] This move appears to have been the brainchild of the Senate Select Committee on Intelligence, but debate and details about its more specific origins are absent from the legislative history, as is typical of bills originating in that Committee.[110]

In 2021, Senator Ron Wyden, another member of the Senate Intelligence Committee, introduced an amendment to the Intelligence Authorization Act.[111] This amendment requires public disclosure of the unclassified portions of the VEP reports sent to Congress.[112] Congress subsequently adopted this amendment in 2022, requiring public disclosure of the unclassified elements.[113]

C. Current State

Has the VEP moved the ball at all on U.S. government zero-day practices? Substantial debate exists over the VEP's effectiveness. Indeed, the VEP seems to have few unconflicted friends. Its critics largely fall into two camps: those who criticize procedural aspects and those who criticize substantive aspects of the process.

Transparency and enforceability are the primary procedural criticisms.[114] No information about the VEP's membership or procedures has been shared publicly since 2017. Perhaps the information reflected in the 2017 charter is outdated, including the VEP's membership and

108. §3316a(c)(2)(A).
109. §3316a(c)(2)(B).
110. *See* S. Rep. No. 116-47, at 19–20 (2019).
111. Press Release, Sen. Ron Wyden, Wyden Secures Key Provisions to Protect Whistleblowers, Defend Democracy and Strengthen Oversight in Intelligence Bill (July 28, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-secures-key-provisions-to-protect-whistleblowers-defend-democracy-and-strengthen-oversight-in-intelligence-bill [https://perma.cc/2ACC-9A65].
112. Intelligence Authorization Act for Fiscal Year 2022, S. 2610, 117th Cong. (2021).
113. Consolidated Appropriations Act for Fiscal Year 2022, Public Law 117-103, 136 Stat. 963 (incorporating and adopting the Intelligence Authorization Act for Fiscal Year 2022).
114. *See, e.g.*, Michelle Richardson, *Locking in Transparency on the Vulnerabilities Equities Process*, JUST SECURITY (July 27, 2018), https://www.justsecurity.org/59795/locking-transparency-vulnerabilities-equities-process/ [https://perma.cc/C68F-AWRQ]; Susan Hennessey, *Vulnerabilities Equities Reform that Makes Everyone (And No One) Happy*, Lawfare (July 8, 2016), https://www.lawfaremedia.org/article/vulnerabilities-equities-reform-makes-everyone-and-no-one-happy [https://perma.cc/GBC6-RC6X] (critiquing some transparency provisions); Lindsey Polley, *To Disclose or Not to Disclose, That is The Question: A Methods-Based Approach for Examining & Improving the US Government's Vulnerabilities Equities Process*, RAND CORP 57–58 (2022), https://www.rand.org/pubs/rgs_dissertations/RGSDA1954-1.html [https://perma.cc/BAK8-48TJ].

participation, which would affect the substantive critiques described below.[115]

Despite attempts at increased transparency, no further VEP information has been made public. The public has only received information during the one-off 2020 disclosure to Microsoft. We have yet to see if Congress's 2022 codification of that requirement will change that. Government officials believe Congress is receiving classified reports, but whether that is in response to the VEP itself or to Congressional codification is not clear.[116]

Because the VEP remains an executive-branch policy, enforceability of its provisions remains a key concern.[117] Neither watchdogs nor the public have means to force disclosures about its processes; nor does the process include obvious penalties for agencies that fail to comply with its substantive provisions. Some critics continue to call for legislative codification of the substantive portions of the VEP, while others prefer an executive order or national security memorandum, which would keep the VEP within the executive branch but formalize it to a greater degree.[118]

Substantively, criticisms of the VEP are manifold. Some criticize the process for being too biased towards retention and offense, citing key examples of vulnerabilities we know were exploited and not patched over recent years.[119] This potential bias towards retention is why knowing which agencies, and which parts of agencies, participate in the process is important. Depending on how closely the participants still match the list in the official VEP charter, the balance of equities could be much different from what the public believes it to be.

Others criticize the VEP as too subjective, lacking rigor in its assessments of different vulnerabilities.[120] And still others argue that the process does not adequately consider consumer perspectives.[121] Vocal VEP critics Dave Aitel and Matt Tait took issue—though before the

115. The Author is submitting FOIA requests on this and related information. Any responses will be posted on the Author's personal website.

116. Polley, *supra* note 114, at 58 (discussing interviewees' views on enforceability).

117. *Id.* at 58–59.

118. *See, e.g.*, Thompson, *supra* note 97; Polley, *supra* note 114, at 58–59 (finding that a majority of subject matter expert interviewees preferred branch formalization over codification).

119. *See, e.g.*, Thompson, *supra* note 97 (citing Mozilla's experience with the FBI exploiting a vulnerability in Firefox); Nicholas Weaver, *The NSA's Hubris and the Shadow Brokers 0-day*, LAWFARE (Sept. 23, 2016), https://www.lawfaremedia.org/article/nsas-hubris-and-shadow-brokers-0-day [https://perma.cc/P3GZ-6VDW].

120. Sasha Romanosky, *Developing an Objective, Repeatable Scoring System for a Vulnerability Equities Process*, LAWFARE (Feb. 4, 2019), https://www.lawfaremedia.org/article/developing-objective-repeatable-scoring-system-vulnerability-equities-process [https://perma.cc/2SAG-FG9E].

121. Polley, *supra* note 114, at 64 (discussing interviewees' views on consumer protection); *The Vulnerability Equities Process: What We Know and What We'd Like to See*, MOZILLA (May 2017), https://blog.mozilla.org/press/files/2017/05/

2017 Charter—with multiple aspects. Aitel and Tait contend that the VEP is unsuitable for making difficult calls when intelligence stakes are high or unclear.[122] They also argue that "the concrete benefit of a zero-day disclosed one-at-a-time," as the VEP seems to operate, "is extremely limited" because it "has little effect in practice" on the overall availability of bugs.[123]

The VEP also does not govern vulnerabilities in the hands of non-government entities.[124] If a government contractor acquires or discovers a vulnerability and incorporates it into products or services supplied to the U.S. government, that vulnerability does not enter the VEP.[125] As reliance on military contractors for such services grows, fewer bugs enter the VEP.

Taken together, what does all of this mean for the VEP? It is hard to know without more information about how it is functioning. This lack of information and the resulting lack of accurate assessment makes Congress's move to require public disclosure of some VEP information important. Without this kind of disclosure, the public relies on select government disclosures and leaked information, which presents less than a full picture of the VEP. Increased transparency would help in assessing the VEP.[126] Congress should build on its strengths in recent Intelligence Authorization Acts and require public disclosure of more information, including the average price of acquisition.[127] Congress should also require more disclosure of "denominator" information: what kinds of bugs enter the VEP and which do not. For instance, releasing information about how many intelligence products rely on bugs acquired by contractors versus those acquired or discovered by intelligence agencies themselves would help increase understanding of the scope of the VEP.

VEP-WhatWeKnow.pdf [https://perma.cc/7W7L-7MG6] (calling for better representation of civilian consumer security and protection agencies in the VEP).

122. Dave Aitel & Matt Tait, *Everything You Know About the Vulnerability Equities Process is Wrong*, LAWFARE (Aug. 18, 2016), https://www.lawfaremedia.org/article/everything-you-know-about-vulnerability-equities-process-wrong [https://perma.cc/W7LU-GXZP]; *but see* Mailyn Fidler, *A Response to "The Tech:" Continuing the Vulnerability Equities Process Debate*, JUST SECURITY (Sept. 13, 2016), https://www.justsecurity.org/32883/response-the-tech-continuing-vulnerability-equities-process-debate/ [https://perma.cc/UT53-JU3R] (responding to Aitel and Tait).

123. Aitel & Tait, *supra* note 122.

124. *Vulnerabilities Equities Policy and Process for the United States Government*, *supra* note 65 (describing that the VEP applies when the "USG obtains knowledge of newly discovered and not publicly known vulnerabilities." The VEP is not triggered when a private entity retains that knowledge, but the U.S. government receives operational benefits from its use.)

125. *Id.*

126. *See, e.g.*, Siena Anstis, Niamh Leonard & Jonathan W. Penney, *Moving From Secrecy to Transparency in the Offensive Cyber Capabilities Sector: The Case of Dual-Use Technologies Exports*, 48 COMPUT. L. & SEC. REV. (2023).

127. *See* Fidler, *supra* note 1, at 451–52.

Policymaking in this area seems to have largely been driven by public outcry. Reforms after leaks are common. The remainder of reforms have come from informed congresspeople, including members of the Senate Intelligence Committee, which has certain members who are particularly educated on, dedicated to, or staffed up on these issues, as well as congresspeople influenced by the Cyber Solarium Project.[128] Senator Angus King, for instance, a member of the Intelligence Committee who the Cyber Solarium Project influenced, was responsible for introducing the VEP codification language. Senator Ron Wyden, who introduced the 2022 transparency language, is a regular champion of tech law issues.

But the fact that change has been driven by a small, elite group of policymakers or in response to spikes in public outrage means the appetite for broader and sustained reform is low. The legislative efforts, spearheaded by actors with laudable but idiosyncratic appreciation for these issues, is not movement politics. The policy window for doing much else beyond limited transparency measures seems limited, especially as time passes without further leaks or disclosures to renew public interest. Transparency is about as good as we are going to get from a formal legal stance, much as I argued ten years ago, although its limits remain substantial.[129]

The U.S. made its first foray into buyer-side regulation in 2023, with the Biden Administration's Executive Order on "Commercial Spyware that Poses Risks to National Security."[130] The Order prohibits government agencies from making "operational use of commercial spyware that poses significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or foreign person."[131] As a consequence, U.S. government agencies would not use or procure spyware like NSO Group's Pegasus, given its links to "improper use by a foreign government" or other spyware posing national security risks to the U.S.[132] This policy is very different in nature from the VEP. It is essentially a procurement policy, not an internal oversight policy. Those two categories are extremely different in the specificity required, the enforcement mechanisms available, and the incentives for adherence. This buyer-side regulation will have market effects—removing the U.S. government as a potential buyer for a particular class of spyware—but those market effects might have limited punitive effect on sellers of this spyware, given their broad international customer base. The relative newness of the policy also makes assessing its outcomes difficult at this point.

128. *See* Angus King & Mike Gallagher, *Final Report*, Cyberspace Solarium Comm'n (Mar. 2020).
129. Fidler, *supra* note 1, at 451–52.
130. *See* Exec. Order No. 14093, 88 Fed. Reg. 18957 (Mar. 27, 2023).
131. *Id.*
132. *Id.*

Nonetheless, this Order is significant as the first national buyer-side regulation pursued in the U.S.

IV. REGULATING CROSS-BORDER SALE

A. Export Control Introduction

The primary mode of market regulation over the last ten years has been export controls. Export controls are seller-side restrictions, placing restrictions on the conditions under which an entity within a country can sell to an entity outside that country. These restrictions can vary from requiring a license from the home government prior to export to more stringent options.

There are broadly three types of export controls: item-based, user-based, and use-based.[133] Item-based export controls place restrictions on types of exports, say, a kind of software.[134] This approach has been the primary focus of export controls for zero-day-related software over the past ten years. For example, certain "cybersecurity items," a term of art, are listed on the Commerce Control List.[135] The second type, user-based controls, designates certain end-users to whom exports are restricted. As an example of a relevant user-based control, the spyware software company NSO Group was recently added to the Entity List.[136] The third type, use-based controls, indicates that exports to be used for certain purposes are restricted. The Export Control Act of 2018, discussed later in the Article, is an example of a use-based control.[137] However, export control regulations, as implemented, are often a blend of these categories. Indeed, even the examples in this paragraph are actually blends. The item-based Commerce Control List interacts with the user-oriented Commerce Country chart, for example.[138] The end-user focused Entity List interacts with the item-based Commerce Control

133. Destination controls, or controls over items being sent to a particular country or jurisdiction, also play an important role. These categories are based on similar ones put forward in Kevin Wolf et al., *BIS Has New Authorities to Impose Controls over Activities of US Persons in Support of Foreign Military, Security, or Intelligence Services*, AKIN (Jan. 5, 2023), https://www.akingump.com/en/insights/alerts/bis-has-new-authorities-to-impose-controls-over-activities-of-us-persons-in-support-of-foreign-military-security-or-intelligence-services [https://perma.cc/6RZH-NQST].

134. Export control professionals use the term "list-based" to describe these controls, but I have substituted "item-based" for ease of understanding. *See* Wolf et al., *supra* note 133; *Commerce Control List Index*, BUREAU OF INDUS. & SEC., DEP'T OF COM, https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl [https://perma.cc/2WN3-BR6Z] (last visited Dec. 1, 2023).

135. *See infra* notes 160–172; Information Security Controls: Cybersecurity Items, Category 4, *supra* note 58.

136. 15 C.F.R. § 744, Supp. No. 4 (providing a list of entities subject to license requirements).

137. *See infra* notes 208–219.

138. 15 C.F.R. § 738.3.

List and other item-based regulations.[139] And use-based controls intersect with various country-based, user-oriented categories, too.[140]

Export controls are implemented domestically and through international cooperation. The foremost international mechanism applicable to the topic at hand is the Wassenaar Arrangement, a primarily item-based mechanism. The Arrangement is a voluntary international mechanism through which states pledge to harmonize export controls on both conventional military and dual-use technologies.[141] Dual-use technologies can be used either for civilian or military purposes.[142] The Wassenaar Arrangement has been used to address a wide range of dual-use technologies, from certain kinds of lasers[143] to submersible vehicles,[144] and, most recently, types of software closely intertwined with zero-day vulnerabilities.[145]

The Wassenaar Arrangement has forty-two member states and was formed in the wake of the Cold War. The Arrangement—now problematically—includes Russia.[146] India joined in 2017, an important addition.[147] Israel, a key exporter of spyware, is not a formal member, although it nominally coordinates its export controls with the Arrangement.[148] The Arrangement serves as a forum through which states coordinate export controls. However, each state is responsible for separately implementing domestic laws to implement the agreed export controls.[149] States do not always complete this domestic implementation step, or they make slight adjustments to what was agreed at the Arrangement.[150]

---

139. See the column, "License Requirements" for differences in variation. 15 C.F.R. § 744, Supp. No. 4.
140. *See infra* notes 208–219.
141. *Introduction*, WASSENAAR ARRANGEMENT (Dec. 1, 2022), https://www.wassenaar.org [https://perma.cc/4NK8-TPAL].
142. *See, e.g.*, *Exporting Dual-Use Items*, EUROPEAN COMM'N, https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en [https://perma.cc/ZH4E-P9AD] (last visited Dec. 1, 2023).
143. WASSENAAR ARRANGEMENT SECRETARIAT, *supra* note 62, at 101–02.
144. *Id.* at 150–56.
145. *Id.* at 80.
146. *About Us*, WASSENAAR ARRANGEMENT, https://www.wassenaar.org/about-us/ [https://perma.cc/5ZFM-UZX4] (last visited Dec. 1, 2023) (listing Russian Federation as a member).
147. *Id.*; *India Joins Wassenaar Arrangement, and Other Trade Updates from New Dehli*, DELOITTE (Jan. 23, 2018), https://www2.deloitte.com/uk/en/blog/global-export/2018/india-joins-the-wassenaar-arrangement.html [https://perma.cc/M6G2-3K6Z].
148.. *Israel Export Control Information*, BUREAU OF INDUS. & SEC., DEP'T OF COM. (2020), https://www.bis.doc.gov/index.php/licensing/220-eco-country-pages/1147-israel-export-control-information [https://perma.cc/KMC6-R3KN].
149. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Scope, July 12, 1996, § III.3.
150. *See infra* Part III.B (discussing the 2013 implementation).

In my 2015 article, I argued in favor of using the Wassenaar Arrangement to place export controls on some sales of zero-day exploits (the "weaponized" form of vulnerabilities) because the Arrangement was designed, as an institution, to address problems similar in structure to the international trade in zero-day exploits.[151] It was also the only existing international institution that could address zero-days without significant institutional change.[152] Last, the Arrangement also had the benefit of substantial flexibility, important when dealing with the nuances of zero-days and associated technologies.

The downsides of this approach, however, included challenges precisely defining zero-day exploits (the flip side of flexibility), the challenge of national implementation, and the lack of hard enforcement power.[153] All of these came to pass.

B. The Last Ten Years

The last ten years of the Wassenaar Arrangement essentially played out this list of downsides. The member states of the Wassenaar Arrangement tried to place restrictions on software closely related to zero-days, but definitional challenges, both at the level of the Arrangement and domestically, other national implementation challenges, and member-state hesitation to enforce pockmarked this attempt.

In 2013, spurred by the United Kingdom and France, the Wassenaar Arrangement added controls on "[s]ystems, equipment, and components therefor, specially designed or modified for the generation, command and control, or delivery of" a new category of item termed "intrusion software."[154] These are all opaque terms of art. To better understand what this language controlled, think of a Russian stacking doll. At the center is a zero-day vulnerability, or the knowledge of a flaw in code. At the second level is a zero-day exploit, a program written to take advantage, or exploit, that underlying vulnerability. At the third level is "intrusion software." [155] The technical definition of intrusion software is provided in the footnotes, but in plainer language, intrusion

151. Fidler, *supra* note 1, at 471–72.
152. *Id.* at 472.
153. *Id.* at 472–74.
154. WASSENAAR ARRANGEMENT SECRETARIAT, *supra* note 62, at 80; *see also* Heejin Kim, *Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue*, 70 INT'L & COMPUT. L. Q. 379 (2021) (indicating that other changes were made to the list at the same time, including to network surveillance technologies, but intrusion software received the most debate).
155. Intrusion software is defined as:

> "Software" specifically designed or modified to avoid detection by "monitoring tools," or to defeat "protective countermeasures," of a computer or network capable device, and performing any of the following:
>
> a. The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or

software is a program that must be (a) designed to avoid detection and either (b) extract or modify data or (c) run an outside program.[156] Zero-day exploits could be used to complete steps a, b, or c. The fourth level refers to "systems, equipment, and components therefore, specially designed or modified for the generation, command and control, or delivery of" the third layer.[157] The fourth level is what is controlled. The drafters had in mind, perhaps, a full-service, dashboard-like software package that, once engaged, could deploy sub-modules to target particular targets based on need—and intended only to control the dashboard-like software.[158] This would leave all of the sub-modules, down to the zero-days, uncontrolled.

This move was probably an attempt to target the worst applications of zero-days while leaving scope for continued cross-border trade in zero-day vulnerabilities, which can happen in benign forms such as vulnerability disclosure programs and security research. That said, the language was convoluted, and that very nature raised fears about chilling effects on the inner portions of the Russian stacking doll.

Despite these likely intended limitations on scope, the U.S. essentially brought these fears to life through its attempt to implement these controls domestically. The Department of Commerce's Bureau of Industry and Security (BIS), responsible for the implementation, introduced language that read to many critics, myself included, as overbroad.[159]

The original BIS definition of "intrusion technology" included "proprietary research on vulnerabilities and exploitation of computers and network-capable devices" and further clarified that the U.S. would have a "policy of presumptive denial [for export] for items that have or support . . . zero-day exploit capabilities."[160] With this definition, BIS went beyond the carveout the Wassenaar Arrangement had tried to implement. This move prompted concerns that BIS was trying

---

b. The modification of the standard execution path of a "program" or process in order to allow the execution of externally provided instructions.

WASSENAAR ARRANGEMENT SECRETARIAT, *supra* note 62, at 226.

156. *See id.*

157. WASSENAAR ARRANGEMENT SECRETARIAT, *supra* note 62, at 80. Jennifer Stisa Granick & Mailyn Fidler, *Update: Changes to Export Control Arrangement Intended to Apply to Surveillance Technology, Not Exploits, but Confusion and Ambiguity Remain*, JUST SEC. (Feb. 19, 2014), https://www.justsecurity.org/7276/update-export-control-arrangement-intended-apply-surveillance-technology-exploits-confusion-ambiguity-remain/ [https://perma.cc/AX6V-NS9M].

158. The software obviously need not be configured as a dashboard; exploit kits are another common term. I use the example of a dashboard for explanatory purposes only.

159. Mailyn Fidler, *Proposed U.S. Export Controls: Implications for Zero-Day Vulnerabilities and Exploits*, LAWFARE (June 10, 2015, 9:00 AM), https://www.lawfaremedia.org/article/proposed-us-export-controls-implications-zero-day-vulnerabilities-and-exploits [https://perma.cc/3N72-D3VA].

160. *Id.* (citing 80 Fed. Reg. 28854, 28855 (May 20, 2015)).

to chill research, reigniting the debate about encryption software export controls from the 1990s.[161] Security professionals and others had issues with the underlying Wassenaar language, too, critiquing it as overbroad and risking the ability of security researchers to conduct beneficial work across borders.[162]

The broad-based criticism was effective. The Commerce Department (laudably) withdrew its proposal.[163] House oversight committees called the Department to task.[164] In a remarkable turnaround, the Department of Commerce indicated it would seek to renegotiate the Wassenaar Arrangement controls to remove the intrusion control software restrictions in 2016.[165] The first attempt at doing so, however, failed.[166] Bipartisan support for another attempt continued.[167] In 2017, the U.S. successfully negotiated alterations and clarifications to the Wassenaar language that addressed many of the critics' concerns.[168] Two changes were made to the language. First, a clarifying note was added to the

161. Karen Gullo, *EFF to Commerce Department: We Must Revise Overbroad Export Controls*, ELEC. FRONTIER FOUND. (July 21, 2015), https://www.eff.org/deeplinks/2015/07/eff-commerce-department-we-must-revise-overbroad-export-control-proposal [https://perma.cc/2VFT-6PX2].

162. *See, e.g.*, Allen Householder & Art Manion, *CERT Coordination Center Comments on Bureau of Industry and Security Proposed Rule*, CARNEGIE MELLON (2015), https://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_442291.pdf [https://perma.cc/D8HL-5R6V]; Sergey Bratus et al., *Why Wassenaar Arrangement's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense at Risk–And How to Fix It*, DARTMOUTH (2014), https://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf [https://perma.cc/AG4B-A8FY].

163. Garrett Hinck, *Wassenaar Export Controls on Surveillance Tools: New Exemptions for Security Research*, LAWFARE (Jan. 5, 2018, 9:30 AM), https://www.lawfaremedia.org/article/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research [https://perma.cc/V4PU-GXQN].

164. *Wassenaar: Cybersecurity and Export Control Before the Comm. on Oversight & Government Reform*, 114th Cong. (Jan. 12, 2016) (transcript available at https://oversight.house.gov/wp-content/uploads/2016/01/2016-01-12-Jt-OGR-IT-CHS-CIPST-Wassenaar.GO012251.pdf [https://perma.cc/48Z2-ELHU]. *See id.* at 14–16, 67, 74, 76–77, 85.

165. Letter from Penny Pritzker, U.S. Sec'y of Commerce, to Various Associations (Mar. 1, 2016) (available at https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/1434-letter-from-secretary-pritzker-to-several-associations-on-the-implementation-of-the-wassenaar-arrang/file [https://perma.cc/Y93W-XGEJ]).

166. Tami Abdollah, *US Fails to Renegotiate Arms Control Rule for Hacking*, ASSOC. PRESS (Dec. 19, 2016), https://apnews.com/article/c0e437b2e24c4b68bb7063f03ce892b5 [https://perma.cc/WBG5-7TQF].

167. *BSA Applauds Bipartisan House Letter Urging Trump Admin to Renegotiate the Wassenaar Arrangement*, BSA (Feb. 10, 2017), https://www.bsa.org/news-events/news/bsa-applauds-bipartisan-house-letter-urging-trump-admin-to-renegotiate-the-wassenaar-arrangement [https://perma.cc/H3VL-FKEH].

168. *See, e.g.*, Katie Moussouris, *Serious progress made on the Wassenaar Arrangement for global cybersecurity*, THE HILL (Dec. 17, 2017), https://thehill.com/opinion/cybersecurity/365352-serious-progress-made-on-the-wassenaar-arrangement-for-global/ [https://perma.cc/E9QL-8WMS].

definition of "technology for the development of intrusion software" to indicate that technology shared for vulnerability disclosure or incident response purposes was not covered.[169] Second, a clarifying note was added to make clear that standard, remote security updates are not controlled.[170] Domestically, BIS implemented these modified controls, using the new, and not particularly descriptive, term "cybersecurity items."[171]

The drama of the sloppy U.S. execution distracted from more serious concerns about the Wassenaar Arrangement's effectiveness during this time. Serious failures of political will resulted in the ineffectiveness of whatever controls were agreed on through Wassenaar.

First, and perhaps most blatantly, Wassenaar member governments—most notably Greece, Spain, Hungary, and Poland—started using spyware on domestic political opposition groups.[172] Officials from some of these countries have been openly contemptuous towards the European Union (EU) efforts to investigate and curtail these uses; after a visit by an EU investigating committee called

169. *See Deemed Exports FAQs: What Changes Were Made to the Wassenaar Arrangement List in 2017 for Intrusion Software and Why Were They Made?* BUREAU OF INDUS. & SEC., DEP'T OF COMM. https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports/deemed-exports-faqs/faq/62-1-what-changes-were-made-to-the-wassenaar-arrangement-list-in-2017-for-intrusion-software-and-why-were-they-made [https://perma.cc/J3E3-PBKQ] (last visited Dec. 1, 2023).

170. *See Deemed Exports FAQs: What Changes Were Made to the Wassenaar Arrangement List in 2017 for Intrusion Software and Why Were They Made?*, *supra* note 169; WASSENAAR ARRANGEMENT SECRETARIAT, *supra* note 62, at 80.

171. Information Security Controls: Cybersecurity Items, *supra* note 58; *see also* Kevin Wolf et al., *U.S. Department of Commerce Implements New Export Controls to Combat Malicious Cyber Activities*, AKIN (Mar. 17, 2022), https://www.akingump.com/en/insights/alerts/us-department-of-commerce-implements-new-export-controls-to-combat-malicious-cyber-activities [https://perma.cc/E92H-VXHD] (providing that this phrase is broad and complex).

172. Antoaneta Roussi, *How Europe Became the Wild West of Spyware*, POLITICO (Oct. 25, 2023, 10:57 AM), https://www.politico.eu/article/how-europe-became-wild-west-spyware/ [https://perma.cc/VGJ4-FGPW].; Hendrik Mildebrath, *Greece's Predatorgate: the Latest Chapter in Europe's Spyware Scandal?,* EUR. PARLIAMENT RSCH. SERV. (Sept. 2022) https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf [https://perma.cc/X77L-BGHH]; John Scott-Railton, et al., *CatalanGate: Extensive Mercenary Operation Against Catalans Using Pegasus and Candiru*, CITIZENLAB (Apr. 18, 2022), https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ [https://perma.cc/2LD8-VB2W]; Alan Charlish & Pawel Florkiewicz, *Polish Mayor Targeted by Pegasus Spyware-media*, REUTERS (Mar. 3, 2023, 2:35 PM), https://www.reuters.com/world/europe/polish-mayor-targeted-by-pegasus-spyware-media-2023-03-03/ [https://perma.cc/N7SX-MXGT]; Lorne Cook, *EU Lawmakers Warn of Hungary, Poland Spyware Abuses*, AP NEWS (May 9, 2023, 2:24 PM), https://apnews.com/article/eu-spyware-pegasus-hungary-poland-greece-cyprus-b1fdf33c11c54254a6e64bc296c78d4d [https://perma.cc/3H2Y-NMR3].

"PEGA," one Greece official commented, "We piss on PEGA."[173] This use, and accompanying attitudes, undercut the moral force of the Wassenaar controls.

Second, many member governments selectively enforced the intrusion software controls.[174] The EU formally implements Wassenaar export controls but leaves enforcement to individual states, resulting in a gap in political will and a lack of options for central enforcement.[175] For instance, Italy did not revoke the global export license for one of its most notorious sellers of such tools, Hacking Team, until 2016, even though the intrusion controls were first agreed upon in 2013.[176] Moreover, Italy did not revoke Hacking Team's license until after the company was hacked and rocked by an international public relations disaster.[177] Data supports this anecdote: researchers report that EU states denied only fourteen such export license applications between 2015 and 2017, granting over 317.[178]

Third, many European countries turned a blind eye when hacking companies sought to establish corporate entities in jurisdictions with such selective or lax enforcement. For instance, as Israel has tightened its export rules in the wake of scandals, Israeli companies created subsidiaries in Bulgaria, Cyprus, and Greece, which remain lax on export control implementation.[179]

Israel has also been a source of difficulty in curtailing international trade in intrusion software. A report by the Carnegie Endowment for International Peace found that fifty-six out of seventy-four governments using such software had acquired at least some technology

173. Tasos Telloglou et al., *Flight of the Predator*, LIGHTHOUSE REPS. (Nov. 30, 2022, 10:26 AM), https://www.lighthousereports.com/investigation/flight-of-the-predator/ [https://perma.cc/F9TT-HDJM].

174. *Draft Report of the Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware*, EUR. PARLIAMENT 5, 95 (Aug. 11, 2022), https://www.politico.eu/wp-content/uploads/2022/11/08/PEGA-draft-report-final-8-1117473.pdf [https://perma.cc/T7FB-GYHN].

175. Elaine Korzak, *Export Controls: The Wassenaar Experience and its Lessons for International Regulation of Cyber Tools*, *in* ROUTLEDGE HANDBOOK OF INT'L CYBERSECURITY 301 (Eneken Tikk & Mika Kerttunen, eds.) (2020).

176. *Hacking Team's Global License Revoked by Italian Export Authorities*, PRIV. INT'L (Apr. 8, 2016), https://privacyinternational.org/blog/1042/hacking-teams-global-license-revoked-italian-export-authorities [https://perma.cc/5KDK-FKDG]; Andy Greenberg, *Hacking Team Breach Shows a Global Spying Firm Run Amok*, WIRED (July 6, 2015, 10:26 AM), https://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/ [https://perma.cc/YNT2-PYCK].

177. *Id.*

178. Maaike Goslinga, *How European Spy Technology Falls into the Wrong Hands*, DE CORRESPONDENT (Feb. 23, 2017), https://thecorrespondent.com/6257/how-european-spy-technology-falls-into-the-wrong-hands/2168866237604-51234153 [https://perma.cc/UZ7K-LQ9A].

179. *Operating from the Shadows: Inside NSO Group's Corporate Structure*, AMNESTY INT'L (May 31, 2021), https://www.amnesty.org/en/documents/doc10/4182/2021/ en/ [https://perma.cc/F2LV-8ZKR]; Telloglou, *supra* note 173.

from an Israeli company.[180] Israel is not a member of the Wassenaar Arrangement, although it nominally "coordinates" its export control rules with the body's decisions.[181] Until the major scandal involving the NSO Group, an Israeli company, Israeli enforcement of these export controls was generally light. As controls tightened in response to this scandal, Israeli companies took advantage of lax European enforcement, as described above.

The most effective trigger of actual enforcement of existing export control regulations has been public scandals driven by investigative journalism or hacks. As mentioned above, in 2015, Hacking Team, an Italian company, was itself hacked, resulting in the release of over 400 gigabytes of data, including its customer list, which revealed purchases by many entities considered to violate human rights.[182] As described above, Italy only revoked Hacking Team's global export authorization after this hack. FinFisher, another such software team publicly accused of selling to human rights violators, shut down by March 2022 following coverage of an inquiry into its alleged violations of German export controls; it is also the subject of ongoing criminal complaints.[183] And, as discussed further below, the U.S. added NSO group to its entity list following investigative reporting about the Pegasus software, damaging the company financially.[184] The UN Special Rapporteur on freedom

180. Feldstein & Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Response*s, *supra* note 33, at 2, 16.

181. *Israel Export Control Information*, *supra* note 147.

182. Lorenzo Franceschi-Bicchierai, *The Vigilante Who Hacked Hacking Team Explains How He Did It*, VICE (Apr. 15, 2016, 4:24 PM), https://www.vice.com/en/article/3dad3n/the-vigilante-who-hacked-hacking-team-explains-how-he-did-it [https://perma.cc/RCH9-87DF].

183. Ryan Gallagher, *Spyware Vendor FinFisher Claims Insolvency Amid Investigation*, BLOOMBERG (Mar. 28, 2022, 3:00 AM), https://www.bloomberg.com/news/articles/2022-03-28/spyware-vendor-finfisher-claims-insolvency-amid-investigation?leadSource=uverify%20wall&sref=QmOxnLFz [https://perma.cc/BH3E-GXZ9].

184. Press Release, U.S. Dep't of Comm., 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#:~:text=NSO%20Group%20and%20Candiru%20(Israel,%2C%20academics%2C%20and%20embassy%20workers [https://perma.cc/C4B6-JZEU]; Davide Scigliuzzo, *Israel Spyware Firm NSO Seen at Risk of Default as Sales Drop*, BNN BLOOMBERG (Nov. 22, 2021), https://www.bnnbloomberg.ca/israeli-spyware-firm-nso-seen-at-risk-of-default-as-sales-drop-1.1685748 [https://perma.cc/SSR5-63ND]; *Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware Before the Permanent Select Committee on Intelligence*, 117th Cong. (July 27, 2022) (written testimony of John Scott Railston), https://docs.house.gov/meetings/IG/IG00/20220727/115048/HHRG-117-IG00-Wstate-Scott-RailtonJ-20220727.pdf [https://perma.cc/863U-79HY].

of expression also called for an international moratorium on the sale of this technology following the Pegasus Project's reporting.[185]

In tandem with these events, Russia, a member of the Wassenaar Arrangement, invaded Ukraine. This hostility and the accompanying changing political dynamics have dramatically impacted the Arrangement and the individual export decisions of certain countries, including Israel, which denied export licenses in response to Russian pressure.[186] The altered geopolitics of the Arrangement cast doubt on its ability to be a productive site of future cooperation on export controls, because of Russia's likely refusal to join in any consensus.[187]

C. Current State

The broad-scale coalition that came together to use Wassenaar to control "intrusion software" probably will not happen again—at least in that particular way. The new geopolitics, schisms within and among Western nations that developed over the botched implementation, and Western nations' own domestic use and reliance on these technologies all likely foreclose broad multilateral export controls as a source of controls.

Nevertheless, export controls as a vehicle for combatting perceived abuses of these kinds of technologies are not completely dead. Instead, states have refocused the debate on the term "spyware," emphasizing the narrow nature of the items they seek to restrict.[188] States have also started turning towards unilateral and regional export controls. In some countries, there is a shift from the first category of export controls (item-based) to end-user and use-based restrictions.[189] These moves are part of a more streamlined attempt after the misperception that the Wassenaar Arrangement changes were intended to regulate software tools more broadly.[190]

185. *Spyware Scandal: UN Experts Call for Moratorium on Sale of 'Life Threatening' Surveillance Tech*, UN OHCHR (Aug. 12, 2021), https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening [https://perma.cc/FDR3-V8CJ].

186. Ronen Bergman & Mark Mazzetti, *Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia*, N.Y. TIMES (Mar. 23, 2022), https://www.nytimes.com/2022/03/23/us/politics/pegasus-israel-ukraine-russia.html [https://perma.cc/M7CK-9Z38].

187. Sujai Shivakumar, Charles Wessner & Hideki Tomoshige, *Toward a New Multilateral Export Control Regime*, CSIS (Jan. 10, 2023), https://www.csis.org/analysis/toward-new-multilateral-export-control-regime [https://perma.cc/J88W-PPRD].

188. *See, e.g.*, Exec. Order No. 14093, 88 Fed. Reg. 18957 (Mar. 27, 2023). Hacking tools marketed primarily at police have also been the subject of ongoing policy conversations but are beyond the scope of this paper. For more analysis, *see, e.g.*, Mailyn Fidler, *Local Police Surveillance and the Administrative Fourth Amendment*, 36 SANTA CLARA HIGH TECH. L.J. 481, 485–518 (2020) (discussing such tools).

189. *See infra* Part IV.C.1–4.

190. Korzak, *supra* note 175, at 305.

The new vocabulary of export controls on this issue uses the terms "spyware" and "commercial spyware." These terms have largely become preferred to standalone terms like "zero-days" and the difficult "intrusion software" label.[191] The goal of this terminological shift appears to be to highlight the use of purchased (rather than government-developed) tools used specifically for espionage, a category narrower than the other terms appear, at least on the surface. President Biden issued an Executive Order nominally restricting the U.S.'s use of certain kinds of commercial spyware.[192] The Order's definition of commercial spyware focuses on "any end-to-end software suite that is furnished for commercial purposes," indicating its intentions to focus on "plug and play" software packages.[193]

Separately, the shift towards unilateral and regional export controls, as opposed to broad, coordinated multilateral controls, has already begun. For example, the U.S., in a move towards expanding user-based restrictions for this category of exports, added several foreign spyware companies to its "Entity List."[194] Among these companies are the NSO Group (the group implicated in the Pegasus exposes), Candiru (an Israeli company), and a lesser-known Russian and Singaporean company.[195] For these companies, this designation means that U.S. entities must get an export license from the U.S. government to export any item subject to the Export Administration Regulations (EARs).[196]

More broadly, the U.S. government has revived export controls as a more central tool of foreign relations. For instance, the U.S. has incorporated broad-ranging controls on Russia and Belarus and multiple controls on exports to China, including on semiconductors, in a move that echoes the tech politics of the 1980s.[197] On the Chinese semiconductor sanctions, the U.S. was notably unable to achieve multilateral

191. *See supra* Parts II.A and IV.B.
192. Exec. Order No. 14093, 88 Fed. Reg. 18957 (Mar. 27, 2023).
193. *Id.*
194. *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities, supra* note 184.
195. *Id.*; *About the Pegasus Project*, FORBIDDEN STORIES, https://forbiddenstories.org/about-the-pegasus-project/ [https://perma.cc/4QVF-7U7B] (last visited Dec. 1, 2023) (discussing the NSO Group's connection with the Pegasus Project).
196. *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities, supra* note 184.
197. Emily Kilcrease, *The New Russia Export Controls*, CNAS (Mar. 7, 2022), https://www.cnas.org/press/press-note/noteworthy-the-new-russia-export-controls [https://perma.cc/DJR3-J23X]; *Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the PRC*, DEP'T OF COMM. (Oct. 7, 2022), https://china.usembassy-china.org.cn/commerce-implements-new-export-controls-on-advanced-computing-and-semiconductor-manufacturing-items-to-the-peoples-republic-of-china-prc/ [https://perma.cc/AK64-TK3S]; Chad P. Brown, *The Return of Export Controls*, FOREIGN AFFS. (Jan. 24, 2023), https://www.foreignaffairs.com/united-states/return-export-controls [https://perma.cc/67ML-47JH].

cooperation, facing continued resistance primarily from the Netherlands and Japan.[198] Additionally, countries have started exercising more discretion in individual export control decisions to forestall opposition to these controls, attempting to go after truly bad actors.[199] This discretion means export controls remain as a tool, but licenses will often be granted.

Placing entities that traffic in spyware on entity lists, as the U.S. has done, sends a strong political signal that the government regards this issue as a national security problem.[200] But the interactions between the entity list and the EARs do not punish software companies as much as hardware companies.[201] The interaction effectively means, for instance, that an American company cannot sell its controlled software directly to the NSO Group. But NSO Group has other avenues still open to it to obtain that same software, unlike, say, a Chinese company reliant on exports of American semiconductor chips.[202] One of these options is to *contract* to use U.S.-based cloud services—software as a service (SaaS)—rather than purchasing software itself. Software as a service is not currently covered by these export regulations, a considerable loophole that renders export controls essentially ineffective.[203]

The EU has also taken steps towards expanded export controls on a regional level. In 2021, the EU passed an updated export control regulation, with new controls for "cyber-surveillance items."[204] The regulation requires authorizations for certain listed cyber-surveillance items exported for military uses and implements red flag provisions for non-listed cyber-surveillance items that the exporter has been

198. Brown, *supra* note 197.

199. I thank Trey Herr for this observation.

200. Charles Capito et al., *Recent Additions to Entity List Part of Broader U.S. Efforts Targeting Spyware*, LAWFARE (Nov. 29, 2021, 8:01 AM), https://www.lawfaremedia.org/article/recent-additions-entity-list-part-broader-us-effort-targeting-spyware [https://perma.cc/Z2QX-BK4Q].

201. For instance, NSO's active presence in the Israel-Palestine conflict as of November 2023 demonstrates that it has not been too badly hurt by the sanctions imposed on it. *See* Sam Sabin, *Israel's NSO Unleashes Controversial Spyware in Gaza Conflict*, AXIOS (Nov. 14, 2023), https://www.axios.com/2023/11/14/pegasus-nso-hamas-israel-spyware [https://perma.cc/B255-KEWV].

202. *Id*. That said, even Chinese companies that are so reliant have found ways around these provisions, renting U.S. chips through cloud-based services. *See, e.g.*, William Reinsch & Margot Putnam, *Addressing Gaps in U.S. Export Controls*, CSIS (May 15, 2023), https://www.csis.org/analysis/addressing-gaps-us-export-controls [https://perma.cc/RN5V-5B73].

203. Letter from C. Randall Wheeler, Dir., Info. Controls Tech. Div., to redacted, Bureau of Information and Security Advisory Opinion on Cloud-based Storage Fronts (Nov. 13, 2014), https://www.bis.doc.gov/index.php/documents/advisory-opinions/1098-cloud-based-storefronts/file [https://perma.cc/TBZ5-9ME3].

204. Cyber-surveillance items are defined as "dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analyzing data from information and telecommunication systems." Regulation 2021/821, 2021 O.J. (L 206) II, 20.

"informed . . . that the items . . . are or may be intended . . . for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law."[205] The regulation also gives states more leeway in passing additional export controls on human rights grounds.[206] Given the dysfunctional background context of spyware controls in the EU, it is hard to assess what effect the updated EU regulation has had so far.[207] On its surface, though, it seems to be a positive development, requiring more of potentially-reluctant member states in terms of export controls on spyware-related items.

1. New Export Control and Sanction Approaches

The definitional debacle that accompanied the Wassenaar intrusion software restrictions, along with the technological limitations of how "export" is defined, has also forced policymakers to be more creative. In the U.S., four export-control-adjacent methods have emerged as ways to skirt these definitional problems: restricting a broad range of support given to designated foreign military, security, or intelligence agencies; restricting the ability of former U.S. intelligence personnel to share expertise with foreign governments; placing financial and travel sanctions on entities designated as human rights abusers, or on those supplying such designees, under the Global Magnitsky Act; and placing visa restrictions on individuals profiting from or involved in misuse of spyware.

2. Export Control Reform Act of 2018

In 2018, Congress passed the Export Control Reform Act of 2018 (ERCA), which opened a new path for controlling the development and use of spyware through use-based controls.[208] This Act added controls over the activities of U.S. persons in support of "foreign military intelligence services."[209] In 2022, this language was broadened to include "foreign military, security, or intelligence services," possibly another

205. *Id.* art. 4 ¶ 1, art. 5 ¶ 1.
206. *Id.* art. 4 ¶ 3.
207. See Mark Bromley & Kolja Brockmann, *Implementing the 2021 Recast of the EU Dual-use Regulation: Challenges and Opportunities*, EU NON-PROLIFERATION & DISARMAMENT CONSORTIUM, Sept. 2021, https://www.sipri.org/publications/2021/eu-non-proliferation-and-disarmament-papers/implementing-2021-recast-eu-dual-use-regulation-challenges-and-opportunities [https://perma.cc/9JM8-Z5DF], for an assessment of some remaining challenges.
208. Wolf, *supra* note 133.
209. Kevin Wolf, Thomas McCarthy & Andrew Schlossberg, *The Export Control Reform Act and Possible New Controls on Emerging and Foundational Technologies*, AKIN (Sept. 12, 2018), https://www.akingump.com/en/insights/alerts/the-export-control-reform-act-of-2018-and-possible-new-controls [https://perma.cc/PH34-CRYE].

consequence of the Pegasus revelations.[210] These controls extend to U.S. persons' "support" of these activities, which ranges beyond the provision of goods on the export control lists. The definition of support in ECRA is broad, encompassing "[p]erforming any contract, service, or employment you know may assist or benefit" the prohibited uses.[211] As of August 2023, countries to whom these limitations apply are Belarus, Burma, Cambodia, China, Russia, Venezuela, Iran, Cuba, North Korea, and Syria.[212] This list of countries is admittedly limited and does not cover many of the governments accused of using spyware in violation of human rights.[213]

The most notable use of these powers came in October 2022, when BIS put "all U.S. persons" on notice that activities supporting the development of certain semiconductors in China require a license.[214] As of November 2023, ECRA has not yet been used with respect to spyware.

A related change to the law occurred in 2022 when Congress passed additional restrictions on former intelligence agency employees helping intelligence agencies of foreign governments.[215] This legislation came about after stories about Project Raven broke, which detailed a team of former U.S. National Security Agency employees working in and for the United Arab Emirates surveillance operations.[216] The 2022 law restricts permanently holding certain positions in certain foreign countries and requires individuals to wait thirty months after leaving a covered U.S. position before holding any covered position in a foreign country.[217] This move essentially places specific, additional "labor" export controls on a select class of Americans, former intelligence personnel.

In addition, three persons involved in Project Raven itself have been criminally charged in the U.S. for their involvement, the first time the Department of Justice has used the International Traffic in

210. 50 U.S.C. § 4812(a)(2)(F).
211. 15 C.F.R. § 744.6(b)(6)(iv) (2023).
212. 15 C.F.R. § 744.6(b)(5) (2023).
213. *See* WINNONA DESOMBRE ET AL., *supra* note 34 (calling for targeted restrictions on countries that have purchased from or contracted with certain spyware companies, especially software-as-a-service spyware companies).
214. 15 C.F.R. § 744.6(c)(2) (2023).
215. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No 117-263, § 6301, 136 Stat. 2395, 3498 (2022).
216. Christopher Bing & Joel Schectman, *Inside the UAE's Secret Hacking Team of American Mercenaries*, Reuters (Jan. 30, 2019), https://www.reuters.com/investigates/special-report/usa-spying-raven/ [https://perma.cc/KMJ9-ARKF].
217. 50 U.S.C. § 3073a(a)(1)(B).

Arms Regulations to prosecute this kind of conduct.[218] The cases were resolved with lenient deferred prosecution agreements.[219]

3. Beyond Export Controls: The Global Magnitsky Act

The Global Magnitsky Act, passed in 2016, is another possible unilateral tool the U.S. government could leverage against human rights violators dealing in spyware, although it has not yet been used in that capacity. The Act imposes financial and travel sanctions and is not an export control regime. This Act enables the president to designate and sanction individuals responsible for or aiding in particular human rights abuses or corruption.[220] In 2017, President Trump issued Executive Order 13818, which builds upon the statutory language.[221] Together, the Act and the Executive Order are termed the "Magnitsky Program." Designated entities become ineligible for admission to the U.S. and face freezing of U.S. financial assets and transactions.[222] Other, mostly Western, nations have followed suit and implemented similar lists.[223] Senator Wyden, along with seventeen other members of Congress, has called for its use to combat bad-actor spyware companies, although the U.S. government has not, as of this writing, done so.[224]

The Act allows sanctions to be imposed related to "gross violations of internationally recognized human rights."[225] That term is defined elsewhere in the U.S. Code to include "torture or cruel, inhuman, or degrading treatment or punishment, prolonged detention without charges and trial, causing the disappearance of persons by the abduction and clandestine detention of those persons, and other flagrant denial of the right to life, liberty, or the security of person."[226] The Executive Order uses the less restrictive term "serious human rights abuse."[227] Under the Order, the State Department has sanctioned entities for such activities as using live ammunition on protesters (Sudan), forced labor

218. Brandon L. Van Grack & Joseph Folio, *Prosecuting Project Raven: A New Frontier for Export Control Enforcement,* LAWFARE (Oct. 20, 2021, 8:01 AM), https://www.lawfaremedia.org/article/prosecuting-project-raven-new-frontier-export-control-enforcement [https://perma.cc/22EC-4WPE].
219. *Id.*
220. 22 U.S.C. § 10102(a).
221. Exec. Order No. 13818, 82 Fed. Reg. 60839 (Dec. 20, 2017).
222. § 10102(b)(2).
223. The list includes Estonia, Canada, Lithuania, Latvia, Kosovo, Gibraltar, the UK, and the EU. *See* Adam Gomes-Abreu, *Are Human Rights Violations Finally Bad for Business? The Impact of Magnitsky Sanctions on Policing Human Rights Violations*, 20 J. INT'L BUS. & L. 173, 177, 180–81 (2021).
224. Ron Wyden et al., *supra* note 61.
225. 22 U.S.C. § 10102(a)(1). The Act also allows sanctions for corruption—a topic which is not discussed in this Article.
226. 22 U.S.C. § 2304(d)(1).
227. Exec. Order No. 13818, 82 Fed. Reg. 60839 (Dec. 20, 2017).

on fishing vessels (China), arbitrary arrests and detentions (Tibetan Autonomous Region), and physical abuse of prisoners (Iran).[228]

Of critical importance for the spyware use scenario is the Magnitsky Program's allowance of sanctions on those who have "materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of" violators."[229] This inclusion means the Magnitsky Program could be used to designate foreign spyware companies as material supporters of human rights abuses, with financial and travel consequences in the U.S. and other countries with Magnitsky-like programs.

For a spyware company to be designated under the Magnitsky Program, the following would need to occur: First, a qualifying human rights violation, or attempted violation, would need to be established.[230] Second, an entity would (likely) need to be identified as responsible for that violation, and that entity would (likely) need to be designated under the Magnitsky Program.[231] Third, a link between the spyware company and the designated human rights violator would need to be identified.[232] Fourth, the spyware company would need to meet the definition of material supporter.

To see how the Magnitsky Program might apply to a spyware vendor, consider the recent case involving Egyptian politician Ahmed Eltantawy (also styled Tantawy). Eltantawy is a former member of parliament who has announced his intention for a presidential bid. Egypt has arrested at least ten of Eltantawy's family members and friends on suspicions of terrorist activity, but human rights groups have decried the arrests as solely based on expressions of support for Mr. Eltantawy's candidacy.[233] The State Security Agency subsequently detained them.[234] The arbitrary nature of these arrests is in line with other acts

228. 2022 Global Magnitsky Human Rights Accountability Act Annual Report, 88 Fed. Reg. 19344, 19345, 19348 (Mar. 3, 2023).

229. Exec. Order No. 13818, 82 Fed. Reg. 60839 (Dec. 20, 2017). The Order's definition of "material support" is more expansive than the Act's definition. *See* 22 U.S.C. §10102(a)(4).

230. Michael Weber, CONG. R. SERV. R46981, THE GLOBAL MAGNITSKY HUMAN RIGHTS ACCOUNTABILITY ACT 5 (Dec. 3, 2021).

231. The Program's language leaves open the possibility that a material supporter could be designated without the primary violator also being designated, but so far, that has not occurred. I thank Andrew Self for this observation.

232. For example, a link could be demonstrated through proof of a contract between a spyware company and a particular government agency.

233. Farah Saafan, *Egyptian Ex-MP Planning Presidential Bid Says Relatives Arrested*, REUTERS (May 4, 2023, 3:34 PM), https://www.reuters.com/world/africa/egyptian-ex-mp-planning-presidential-bid-says-relatives-arrested-2023-05-04/ [https://perma.cc/PE4T-VH7M]. *Egypt: Mass Arrests Target Family*, *Supporters of Ex-MP*, HUMAN RIGHTS WATCH (May 5, 2023, 2:45 PM), https://www.hrw.org/news/2023/05/05/egypt-mass-arrests-target-family-supporters-ex-mp [https://perma.cc/F6K6-5LD5].

234. *See Egypt: Mass Arrests Target Family*, *Supporters of Ex-MP, supra* note 231.

that the Magnitsky Act has considered human rights abuses.[235] This information so far identifies both a human rights violation (arbitrary arrests of supporters of an opposition politician) and an actor (the State Security Agency). Citizenlab, a research group that conducts forensic investigations into spyware, concluded that Mr. Eltantawy was targeted with spyware by the Egyptian government, based on the nature of the particular attack on his phone and Egypt's past identification as a government user of this product.[236] Citizenlab identifies the spyware vendor as Cytrox's Predator product.[237] This information establishes a link between a spyware vendor and the human rights violator. Cytrox's Predator product likely fits the definition of material support, given that such a product is clearly technological support and capable of identifying supporters of Mr. Eltantawy. Taken together, this scenario provides sufficient information for the Magnitsky Act to be used to designate the State Security Agency, or another part of the Egyptian government, as a human rights violator, and designate Cytrox as providing material support.

Cytrox was recently added to the U.S. Entity list, requiring U.S. entities to receive licenses before exporting certain items. Sanctioning Cytrox under the Magnitsky Act would add the sting of visa and financial restrictions on the company and its employees. Magntisky sanctions would also, as discussed above, likely be more effective against a software company that might otherwise slip through the cloud-related loopholes in U.S. export control laws.

Cytrox is but one example; numerous other cases can be made against similar companies. The letter sent by members of Congress urging the use of the Magnistky program in this manner identified four additional companies as providing material support to human rights abusers: DarkMatter, Nexa Technology, NSO Group, and Trovicor.[238] A company would need to have financial ties to the U.S. for the Magnitsky sanctions to affect it, but many possible linkages exist. One example includes the Francisco Partners, a private equity firm with two U.S. offices, which held a large stake in NSO Group from 2014 to 2019.[239]

235. *See supra* notes 225–228 and accompanying text (discussing sanctions for human rights abuses under the Magnitsky program).

236. Bill Marczak, *Predator in the Wires*, CITIZEN LAB (Sept. 22, 2023), https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/ [https://perma.cc/D35C-L2R6]; Clement Lecigne & Christian Resell, *Protecting Android Users from 0-Day Attacks*, GOOGLE (May 19, 2022), https://blog.google/threat-analysis-group/protecting-android-users-from-0-day-attacks/ [https://perma.cc/2HTF-XU3V].

237. Marczak, *supra* note 236.

238. *See* Wyden et al., *supra* note 61.

239. Sarah McKune, *The Surveillance Industry and Human Rights*, UN OFF. OF THE HIGHER COMM'R FOR HUMAN RIGHTS 5–6 (Mar. 2, 2019) (available at https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/SARAH_MCKUNE.pdf [https://perma.cc/Z9G4-RHSY]).

This route has several advantages over export control approaches. First, it allows countries to target bad actor spyware companies while leaving other companies unaffected because it does not rely on defining a particular technology to be controlled. Second, the financial sanctions would have more of a bite for software companies than export controls. As discussed elsewhere in this Article, spyware companies often have alternatives that soften the consequences of being designated on export control lists. Relatedly, unlike some forms of export controls, the Magnistky Program can easily punish spyware companies skirting export controls through software-as-service models.

The primary challenges of using the Magnitsky Act to sanction spyware companies come from identifying the primary rights violator and connecting the spyware company to that violator—step three in the outline of the process above. While nothing in the language of the Act or the Order requires that the primary human rights violator be formally named before material supporters can be sanctioned, it is so far typical practice to do so.[240] So, if it is unclear who committed a human rights violation, or who deployed spyware in furtherance of a human rights violation, the State Department may not be able to designate a primary rights violator.[241] Moreover, although the use of spyware to further human rights abuses can often be identified, the entity responsible for its deployment may not always be as clear. For instance, researchers can prove that spyware infected the phone of a journalist who later ended up dead, but who killed the journalist, who infected the phone with spyware, and whether those two entities are related, can remain uncertain.[242] Depending on the level of proof desired by the Magnitsky Program's administrators, these unclear linkages may prove a challenge to its use in this area. The forensics required to connect dots, let alone meet a legal burden of proof, are difficult and often inconclusive.

The Magnitsky approach carries another potential hurdle that has hampered similar end-user focused approaches in the past: it necessitates labeling an entity a human rights violator. Doing so carries a range of possible political consequences. A country may wish to try to control spyware without imposing this label on another country or entity—which may explain the preference for tech-focused export controls up to this point. Egypt provides a clear example; the Eltantawy case may be exactly the kind of case that deserves sanctions, but U.S.-Egypt relations and partnerships on other issues complicate

240. I thank Andrew Self for this information.
241. I thank Andrew Self for discussion of this scenario.
242. *See, e.g.*, Nina Lakhani, *Revealed: Murdered Journalist's Number Selected by Mexican NSO Client* (July 18, 2021, 12:28 PM), https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto [https://perma.cc/9QDR-9E6X].

that decision.[243] That said, if the U.S. is willing to designate an entity a "material supporter" without designating the primary violator, the Magnitsky program could offer a powerful tool for combating spyware without running into the trickiest political calculations about labeling a government a human rights violator.

4. Beyond Export Controls: Standalone Visa Restrictions

The U.S. took a step in the direction of creative, Magnitsky-style sanctions in February 2024, announcing a new policy that allows "the imposition of visa restrictions on individuals involved in misuse of commercial spyware."[244] This policy allows the State Department to implement visa restrictions on individuals involved in commercial spyware misuse, which includes use of such software to target "journalists, activists, [dissidents], members of marginalized communities or vulnerable populations, or the family members [of such people]."[245] It also allows restrictions on those "believed to facilitate or derive financial benefit from the misuse" of such software, including those "developing, directing, or operationally controlling" such companies.[246] The policy also allows visa restrictions on such persons immediate family members.

This strategy is particularly praiseworthy for its imposition of restrictions on an individual, for ties with misuse of spyware, regardless of whether that person's company shifts corporate form. It implements half of the non-export-control sanctions available through the Magnitsky Act, while dodging the political ramifications of designating countries as rights violators. That said, this option does not carry with it the financial penalties that the Magnitsky Act allows. Examining if, and who, these visa restrictions apply to will be crucial to understand in assessing the success of alternative sanctions for spyware.

5. The Multilateral Horizon: New Options for Control

The European Parliament adopted recommendations to counter the misuse of spyware by member countries in June 2023.[247] These recommendations were the work of a committee set up to investigate these

243. *See The U.S.-Egypt Relationship*, DEP'T OF STATE (Jan. 28, 2023), https://www.state.gov/the-u-s-egypt-relationship/ [https://perma.cc/C48C-W8L6].
244. Blinken, *supra* note 60.
245. *Id.*
246. *Id.*
247. *Spyware: MEPs Call for Full Investigations and Safeguards to Prevent Abuse*, EURO. PARLIAMENT (June 15, 2023), https://www.europarl.europa.eu/news/en/press-room/20230609IPR96217/spyware-meps-call-for-full-investigations-and-safeguards-to-prevent-abuse [https://perma.cc/TB7Q-HWFT].

abuses after the Pegasus reporting revealed them.[248] The recommendations included a call for a U.S.-E.U. joint strategy to combat spyware, and a *de facto* moratorium on use of spyware until further safeguards can be put in place.[249]

In March 2023, a group of countries—Australia, Canada, Costa Rica, Denmark, France, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States—published a joint statement on their intent to cooperate to prevent spyware abuses domestically and internationally.[250] Several other initiatives were launched in tandem, including a voluntary code of conduct for government use of surveillance technologies and for implementing export controls.[251]

A series of proposals for broader multilateral mechanisms to control spyware has bloomed over the last few years. Fionnuala Ní Aoláin, the United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, released a 2023 report calling for a new framework controlling spyware. Such a framework should be international, rely on states' enforcement power rather than nongovernmental enforcement power, be strictly limited to spyware, create actual legal obligations on states and private parties with judicial remedies, and place obligations on spyware companies to demonstrate compliance.[252] This proposal is marked with best practices of multilateral frameworks, but leaves open the major question of political will.

Ní Aoláin's proposal follows an earlier one made by David Kaye, UN Special Rapporteur on Freedom of Expression, who called for an international moratorium on the sale of spyware in 2019, drawing on the global campaign to ban landmines.[253] Civil society organizations

248. This Author testified before this committee in November 2022, presenting the core of what became this draft.

249. *Spyware*, *supra* note 247.

250. Press Release, The White House, Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware (Mar. 30, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/ [https://perma.cc/2DQH-B7RW].

251. Press Release, The White House, Fact Sheet: Advancing Technology for Democracy (Mar. 29, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/29/fact-sheet-advancing-technology-for-democracy-at-home-and-abroad/ [https://perma.cc/HL5M-T94R].

252. Fionnuala Ní Aoláin, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*, UN Human Rights Special Proc. (2023).

253. Press Release, UN Off. Of the Higher Comm'r For Human Rights, UN Spyware Scandal: UN Experts Call for Moratorium on Sale of 'Life Threatening' Surveillance Tech (Aug. 12, 2021), https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening [https://perma.cc/FDR3-V8CJ]; David Kaye, *Here's What World Leaders Must Do About Spyware*

have also called for a similar ban.[254] Kaye's proposal also places human rights at its center but struggles from a problem of political will.

Taking a different approach, Asaf Lubin argues for a "Commercial Spyware Accreditation System," a binding multilateral approach that would place certain standards on commercial spyware providers to mitigate human rights risks.[255] This system is modeled on the private (nonbinding) standards regulating private military contractors.[256] Governments have adopted these requirements in procurement procedures, giving them real force. One of this proposal's most notable aspects would be essentially requiring companies to participate in VEP-like procedures.[257] Lubin's proposal is novel and addresses aspects of the vulnerability lifecycle that other proposals leave untouched.[258] That said, this proposal will face extraordinary pushback from spyware vendors themselves, who will almost certainly oppose such direct government involvement in their businesses and, as a binding multilateral mechanism, faces the same obstacle of political will as Ní Aoláin's proposal.[259]

V. RECOMMENDATIONS

These recommendations are based on two primary criteria. First, they are informed by the lessons across both domestic and multilateral efforts to rein in the zero-day and spyware market. Second, they prioritize solutions that have a fighting chance when a failure of political

in ZERO-CLICK SPYWARE: ENEMY OF THE PRESS, COMM. TO PROTECT JOURNALISTS 26, 27 (2022).

254. Letter from various civil society organizations to all states, Joint Open Letter by Civil Society Organizations and Independent Experts Calling on States to Implement an Immediate Moratorium on the Sale, Transfer and Use of Surveillance Technology (July 27, 2021), https://www.amnesty.org/en/documents/doc10/4516/2021/en/ [https://perma.cc/B8LQ-ZBWE].

255. Asaf Lubin, *Selling Surveillance* 42 (IND. UNIV., LEG. STUDIES RSCH. PAPER SERIES, Paper No. 495, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323985 [https://perma.cc/U9J9-R3JZ]; Asaf Lubin, *Regulating Commercial Spyware*, LAWFARE (Aug. 9, 2023, 9:00 AM), https://www.lawfaremedia.org/article/regulating-commercial-spyware [https://perma.cc/CQ73-83DZ]; Asaf Lubin, *Selling Surveillance*, 85 OHIO ST. L.J. (forthcoming) (providing the author's updated analysis of this topic).

256. *See* Lubin, *Selling Surveillance, supra* note 255, at 43–45.

257. *See id.*

258. Sarah McKune and David Kaye have also noted parallels to, or recommended models based on private military contractor regulation, but Lubin's piece is the most developed proposal. *See* McKune, *supra* note 239; David Kaye, *The Spyware State and the Prospects for Accountability*, (U.C IRVINE SCH. OF L., Paper No. 2021-58, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3990249 [https://perma.cc/5TKG-W5G4].

259. Not to mention criticism from human rights advocates. David Kaye & Sarah McKune, *The Scourge of Commercial Spyware–and How to Stop it*, LAWFARE (Aug. 25, 2023, 2:00 PM), https://www.lawfaremedia.org/article/the-scourge-of-commercial-spyware-and-how-to-stop-it [https://perma.cc/85BG-LNDU].

will has marked both contexts. I recommend (1) funding investigative journalism and related analysis, (2) emphasizing entity- and use-based export controls, (3) instituting non-export control sanctions, (4) prioritizing multilateral coalitions of the willing, and (5) expanding transparency requirements.

A. Fund Investigative Journalism and Multidisciplinary Analysis

Nearly every major reform in this issue area came in the wake of an investigative report or leak. On the U.S. domestic side, the Snowden revelations,[260] reporting on the Heartbleed vulnerability,[261] and the Shadow Brokers[262] leak all played major roles in the changes to the VEP ecosystem over the last ten years.[263] Reporting on Pegasus led to an Israeli crack-down, at least temporarily, on major vendors, prompted the European Parliament's investigation, and fed into the call for a moratorium.[264] Investigative journalism and related analysis threads through most of the concrete restrictions that have been implemented over the past ten years. Investigative journalism funding need not necessarily come from the government, sidestepping the problem of political will and placing needed pressure on governments. Investigative journalism is a blunt instrument, though, and what journalists will find and what specific changes in government reports will prompt are beyond the control of those who fund the investigations.

B. Emphasize Entity- and Use-Based Export Controls

Rather than focusing on particular products that should be restricted in export, governments should focus on identifying human rights

260. *See, e.g.,* Ed Pilkington, *Guardian and Washington Post Win Pulitzer Prize for NSA Revelations*, THE GUARDIAN (Apr. 14, 2014), https://www.theguardian.com/media/2014/apr/14/guardian-washington-post-pulitzer-nsa-revelations [https://perma.cc/TU7Y-6M2A].

261. *See, e.g.*, Kim Zetter, *Has the NSA Been Using the Heartbleed Bug as an Internet Peephole?*, WIRED (Apr. 18, 2014, 6:30 AM), https://www.wired.com/2014/04/nsa-heartbleed/ [https://perma.cc/MGQ9-GB5G].

262. *See, e.g.*, Lily Hay Newman, *Why Governments Won't Let Go of Secret Software Bugs*, WIRED (May 16, 2017, 7:30 AM), https://www.wired.com/2017/05/governments-wont-let-go-secret-software-bugs/ [https://perma.cc/T39P-4U4J].

263. This reporting has often been based on leaked or hacked documents. Elsewhere, I have argued for public interest exceptions and mitigations to leaking and hacking laws and prosecutions. *See, e.g.*, Mailyn Fidler, *First Amendment Sentence Mitigation: Beyond a Public Accountability Defense for Whistleblowers*, 11 HARV. NAT'L SEC. J. 214 (2020).

264. *See* Feldstein & Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Response*s, *supra* note 33 at 12; *see generally Pegasus Project*, THE GUARDIAN, https://www.theguardian.com/news/series/pegasus-project [https://perma.cc/FL7T-E9J8] (last visited Dec. 1, 2023) (providing background on the Pegasus Project).

violators and other bad actors, both companies and governments, and restricting a broad range of interactions with those particular actors. This approach has the advantage of skirting technological definitional problems and the software-as-a-service limitation of traditional export controls. The U.S. government has started to do this with the Export Control Act of 2018. This approach, as a unilateral one, means a government can decide to implement this approach without coordination, lowering the political will "activation energy" required. That said, politics will still certainly come into play when deciding what companies and countries count as "bad actors." Increasing domestic legal penalties for companies that fail to do due diligence about their customers also has a role to play in these systems.

C. Shift Towards Sanctions

Use the Global Magnitsky Program and similar visa restrictions to target human rights violators using spyware and spyware companies materially assisting human rights violators. Both approaches allow the targeting of bad actors rather than trying to sort, on the technological end, wheat from the chaff. The Magnitsky Program leverages financial and travel sanctions to impose consequences that are less easily avoided than software export controls; visa restrictions leverage travel restrictions. Further, these approaches can apply equally to vendors using spyware as a service business models. Pursuing alternative sanctions for spyware can mean placing human rights violations front and center, and naming particular entities as human rights violators can have more, or different, political consequences than erecting hurdles to the export of items from within a country's own borders. Still, the last ten years have demonstrated that both the realities of human rights violations with spyware and the fumbles taking tech-first approaches mean putting the abuses at the core of a regulatory strategy may be worthwhile.

D. Prioritize Multilateral Coalitions of the Willing

The international political environment has drastically shifted over the last ten years, rendering cooperation on most things more difficult. The Wassenaar Arrangement debacle over the scope of controls and Russia's membership in that Arrangement makes it an unlikely future home for spyware controls. But that does not mean that multilateral cooperation is dead. Like-minded multilateral coalitions of the willing—that is, countries both alike in conceiving of the spyware industry as a problem and willing to act—should coordinate their own unilateral export control mechanisms to combat spyware abuses. We have already seen these efforts starting in the joint statement of one group of like-minded countries in March 2023. What counts as a like-minded and/or willing country may shift over time, and different efforts emerge and

overlap.[265] These smaller coalitions will obviously be more limited in their scope than something more truly global. Still, their more aligned values will hopefully translate into more license denials on the ground and peer pressure on non-involved countries.

E. Expand Transparency Requirements

Transparency has limits. The consensus among people I spoke with for this piece was that increased transparency around the VEP would be neither harmful nor helpful. Transparency may not be helpful because what the government chooses or is required to be transparent about may not be particularly revelatory for governance purposes. For instance, as the VEP is currently structured, knowing how many zero-days the government discloses would be nice but not particularly helpful. The helpfulness is limited without knowing how many the government kept and how many did not enter the VEP process in the first place because, for instance, they came through a government contractor. At the very least, though, countries should be transparent about the fact of whether they have *established* a VEP.[266] I continue to push for transparency of the correct information because transparency is critical for democratic governance—and to evaluate how well the VEP is working.[267] I argue for transparency of the correct and complete information, understanding that probably will not happen. There is scope to be creative with transparency, including, for instance, mandating the disclosure of the participating entities in the VEP each year. There is more to be done on transparency, even though it is not a silver bullet.

VI. CONCLUSION

The details of the last ten years of regulatory efforts to control the shifting technology and shifting vocabulary of zero-day vulnerabilities, exploits, intrusion software frameworks, cybersecurity items, cyber-surveillance items, and now spyware reveal some lessons amidst their failures. Move towards regulating the harm—and away from the overly technological specifics of item-based export controls. Bring in the light—with transparency about the fact of regulatory frameworks, if not also their contents. Leverage a range of responses—not just ones focused on the technology or on exports. Spyware might simplify surveillance, but the conclusion does not follow that it is unrestrained.

265. *See, e.g.*, Eyal Benvenisti & George Downs, , 60 STAN. L. REV. 595, 620 (2007) (describing and providing one explanation for this phenomenon of overlap).
266. *See supra* note 78 (referencing the inability to confirm existence of VEPs in the Netherlands and Germany).
267. *See, e.g.*, Anstis et al., *supra* note 126.