ARTICLE

CYBER HARDER

ANDREA M. MATWYSHYN†

I. INTRODUCTION

In 2017, malware dubbed 'NotPetya' infected businesses in over 20 countries,[1] causing an estimated $1.2 billion in damage.[2] Companies as diverse as shipping companies[3] and global law firms[4] suffered significant losses[5] as a re-

† Andrea M. Matwyshyn is a professor of law/ professor of computer science (by courtesy) at Northeastern University, an affiliate scholar of the Center for Internet and Society at Stanford Law School, and a Senior Fellow of the Cyber Statecraft Initiative of the Atlantic Council. She thanks the US-UK Fulbright Commission, who named her a US-UK Cyber Security Scholar in 2016-2017, and the Princeton Center for Information Technology Policy, where she was the Microsoft Visiting Professor of Technology Policy in 2014-2015 during the writing of this article. She also wishes to thank Steve Bellovin, Matt Blaze, Ian Brown, Christina J. DeVries, Jen Ellis, Ed Felten, Rebecca Green, Elizabeth Jex, Jake Kouns, Chris Hoofnagle, Yvette Liebsmann, Brian Martin, Bronwen Matthews, Nora Melley, Jennifer Mueller, Stephanie Pell, Martin Redish, Hope Rosen, Mara Tam, Alka Tandan, Abigail Slater, Marcia Tiersky, Greg Vetter, and Lindsey Wegrzyn-Rush for their helpful comments and critiques of this work.

[1] *See* Doug Olenick, *NotPetya attack totally destroyed Maersk's computer network: Chairman*, SC MEDIA US (Jan. 26, 2018), https://www.scmagazine.com/notpetya-attack-totally-destroyed-maersks-computer-network-chairman/article/739730/ [https://perma.cc/N878-L7FC].

[2] *See* Sarah Marsh, *US joins UK in blaming Russia for NotPetya cyber-attack*, GUARDIAN (Feb. 15, 2018, 17:45), https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine [https://perma.cc/86U6-S7K3].

[3] *See* John Leyden, *FedEx: TNT NotPetya infection blew a $300m hole in our numbers*, REGISTER (Sept. 20, 2017), https://www.theregister.co.uk/2017/09/20/fedex_notpetya_damages/ [https://perma.cc/VBL4-C2KF].

[4] *See* Jeff John Roberts, *Law Firm DLA Piper Reels Under Cyber Attack, Fate of Files Unclear*, FORTUNE (June 29, 2017), http://fortune.com/2017/06/29/dla-piper-cyber-attack/ [https://perma.cc/8DQC-FNUZ].

[5] For example, shipping company FedEx asserted that the NotPetya malware resulted in $300 million in lost business and remediation costs. See Danny Palmer, NotPetya cyber attack on TNT Express cost FedEx $300m, ZDNet (Sept. 20, 2017) https://www.zdnet.com/article/notpetya-cyber-attack-on-tnt-express-cost-fedex-300m/ [https://perma.cc/8KGE-9UPX].

sult of the malware, with some effects still lingering a year later.[6] Although NotPetya mimicked prior malware presumed to be written by financially-motivated criminals,[7] security experts deemed this resemblance likely superficial:[8] unlike some of its malware predecessors,[9] NotPeya was likely written by a nation state for purposes of targeted disruption.[10] Indeed, both the United States and the United Kingdom[11] publicly identified Russia as the author of the malware — allegedly a part of Russia's "hybrid warfare" aimed primarily at destabilizing Ukraine.[12]

The scale of the NotPetya problem calls to mind the Office of Personnel Management ("OPM") breach of 2015. In that breach of approximately 22 million government employees' data – including data of covert operatives[13] – was

---

[6] *See* Kim S. Nash, Sara Castellanos & Adam Janofsky, *One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs*, WALL ST. J. (June 27, 2018 12:03 PM), https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906.

[7] *See* Olivia Solon & Alex Hern, *'Petya' ransomware attack: what is it and how can it be stopped?*, GUARDIAN (June 28, 2017), https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how [https://perma.cc/8GBU-T8GA].

[8] *See* Josh Fruhlinger, *Petya ransomware and NotPetya malware: What you need to know now*, CSO (Oct. 17, 2017), https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html [https://perma.cc/9432-3LJ7]. In particular, the malware allegedly used a modified version of stolen and leaked NSA exploits, taking advantage of networks configured in permissive ways. *See* Iain Thomson, *Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide*, REGISTER (June 28, 2017, 3:19), https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/?page=1 [https://perma.cc/ZL7T-GABU].

[9] Variants of Petya have existed since 2016. *See* Symantec Security Response Team, *Petya ransomware outbreak: Here's what you need to know*, SYMANTEC (Oct. 24, 2017) https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper [https://perma.cc/P5XB-R8BG].

[10] *See UK and US blame Russia for 'malicious' NotPetya cyber-attack*, BBC (Feb. 15, 2018) https://www.bbc.com/news/uk-politics-43062113 [https://perma.cc/T4AQ-HVDL]. ("The Russian military was directly behind a "malicious" cyber-attack on Ukraine that spread globally last year, the US and Britain have said.").

[11] *See* Sam Jones, *Finger points at Russian state over Petya hack attack*, FIN. TIMES (June 30, 2017), https://www.ft.com/content/f300ad84-5d9d-11e7-b553-e2df1b0c3220.

[12] *See* Ellen Nakashima, *Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes*, WASH. POST (Jan. 12, 2018, 6:46 PM), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.841c91b6d46e.

[13] *See* Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST (July 9, 2015),

exposed, ostensibly due to avoidable variables.[14] Like the effects of NotPetya, the full impact of the OPM breach may also never be known. However, national security experts have opined that the OPM breach was "an absolute calamity"[15] whose national security impact may last forty years or more, and it is likely to have damaged an entire generation of national security operations.[16]

Recent legislative and public discussion of data breaches and security has significantly increased, yet in the last year alone, the security situation on the ground appears to have further deteriorated. The Mirai botnet remotely compromised Internet of Things devices such as DVRs[17] and overwhelmed some of the best-defended websites on the internet with a distributed denial of service attack, knocking them off the internet.[18] The WannaCry ransomware held thousands of National Health Services hospital administrative computers hostage, disrupted patient services, and threatened patient welfare.[19] Even the U.S. presidential election appears to have been impacted by attacks on vendors[20] and compromises of state voter registration systems - attacks which our intelligence services believe to have been the work of a foreign adversary.[21] Our cur-

https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/ [https://perma.cc/34HH-GTCC].

[14] *See* Aaron Boyd, *Contractor Breach Gave Hackers Keys to OPM Data*, FED. TIMES (June 23, 2015), http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/23/keypoint-usis-opm-breach/28977277/ [https://perma.cc/6NER-4M9Z].

[15] *See* Andrew Tilghman & David B. Larter, *Military Clearance OPM Data Breach 'Absolute Calamity'*, NAVY TIMES (June 17, 2015), http://www.navytimes.com/story/military/2015/06/17/sf-86-security-clearance-breach-troops-affected-opm/28866125/ [https://perma.cc/FTV7-L8HE].

[16] *See* Dan Verton, *Impact of OPM Breach Could Last More Than 40 Years*, FEDSCOOP (July 10, 2015), http://fedscoop.com/opm-losses-a-40-year-problem-for-intelligence-community [https://perma.cc/U5DZ-5738].

[17] Garrett M. Graff, *How A Dorm Room* Minecraft *Scam Brought Down the Internet*, WIRED (Dec. 13, 2017, 3:55 PM), https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/.

[18] Andy Greenberg, *The Reaper IOT Has Already Infected a Million Networks*, WIRED (Oct. 20, 2017, 5:45 PM), https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/.

[19] *See*, *NHS 'Could Have Prevented' WannaCry Ransomware Attack*, BBC NEWS (Oct. 27, 2017), http://www.bbc.com/news/technology-41753022 [https://perma.cc/FX8G-8MF6] (analyzing the National Audit Office's investigation report on the WannaCry ransomware attack).

[20] Pam Fessler, *Russian Cyberattack Targeted Elections Vendor Tied to Voting Day Disruptions*, NPR (Aug. 10, 2017, 3:47 PM), https://www.npr.org/2017/08/10/542634370/russian-cyberattack-targeted-elections-vendor-tied-to-voting-day-disruptions [https://perma.cc/A4MT-SNG9].

[21] Alex Ward, *Russia Hacked Voting Systems in 39 States Before the 2016 Presidential Election*, VOX (June 13, 2017, 2:00 PM),

rent "cybersecurity" approaches are clearly not succeeding, and the state of security looks bleak.

The predecessor article to this essay, *CYBER!*, [22] offered a fresh approach to security – the paradigm of reciprocal security. This essay continues where *CYBER!* concluded and offers elaborations on concrete policy suggestions for charting a new course for security in both the public and private sectors. Section II briefly introduces the argument in *CYBER!*. Sections III and IV offer implementation suggestions for the five sets of security policy proposals arising from the reciprocal security paradigm advocated by *CYBER!,* and Section V concludes.

II. A BRIEF SUMMARY OF THE ARGUMENT IN CYBER!

CYBER! introduced the problem of "*reciprocal security vulnerability*."[23] The problem of reciprocal security vulnerability refers to the security reality that security flaws and vulnerabilities in the private sector impact the public sector and vice versa.[24] Compartmentalization is impossible in security because both sectors rely on overlapping technology and people. *CYBER!* also highlighted three flawed assumptions that often cause current "cybersecurity" policy and legal conversations to be misframed. First, questions of privacy are often conflated with questions of security.[25] But, *CYBER!* explains, as a matter of technical computer science these are largely different inquiries focusing on different units of analysis.[26] Second, partially because of this *privacy conflation problem*[27] and a deficit of shared vocabulary,[28] a language barrier[29] between computer scientists and policymakers causes them to often talk past each other on matters of security – an *incommensurability*[30] *problem* that results in muddled policy. Finally, security is never simply "cyber" – physical security and digital security are inextricably interwoven. Thus, even the term "cybersecurity" itself misframes the conversation, reflecting an *internet exceptionalism problem*.[31] The fastest way to compromise the confidentiality, integrity, and availability of a particular system is often through physical access, and a review of many of the most severe data breaches illustrates this technical reali-

https://www.vox.com/world/2017/6/13/15791744/russia-election-39-states-hack-putin-trump-sessions [https://perma.cc/2C4K-YG98].

22 Andrea M. Matwyshyn, *CYBER!*, 2017 BYU L. REV. 1109 (2017).

23 *Id*. at 1121-26.

24 *Id*. at 1121.

25 *Id*. at 1135-44.

26 *Id*. at 1137-40.

27 *Id*. at 1135.

28 *Id*. at 1140-45.

29 *Id*. at 1146.

30 *Id*. at 1146.

31 *Id*. at 1154.

ty.[32] Security is about maintaining information and system control – regardless of whether the internet is involved or not. Therefore, approaching security with a lens of internet exceptionalism – the "cybering" of security – is counterproductive. [33] Digital security and physical security are inextricably interwoven parts of a single whole. Stated reductively, security is security.

The two dominant policy paradigms used in "cybersecurity" policy and law – information sharing[34] and deterrence[35] – misunderstand the nature of security and inadequately consider the problem of reciprocal security vulnerability.[36] In their place, *CYBER!* harnessed insights from the work of philosopher of science Michael Polanyi[37] and the cognitive exercise of The Monty Hall problem[38] to construct a new paradigm – the paradigm of reciprocal security.[39] Unlike the current paradigms, reciprocal security recognizes two key features about security. First, security is a polycentric problem, meaning it has multiple pieces that require coordination simultaneously.[40] Imagine a team attempting to construct a single jigsaw puzzle, with each person working on one segment while retaining a sense of the whole. In other words, digital security and physical security should be viewed together as part of the same whole and coordinated in tandem, as should various efforts across the government and the private sector on security generally.

Second, security requires a paradigm driven by adversarial perspective-taking. In other words, we need to think like attackers. Attackers do not generally distinguish between private sector and public sector targets – they strike wherever desirable information resides and where unpatched vulnerabilities allow for ease of security compromise. They also do not distinguish between physical and digital information access – attackers use whichever method is more expedient to them. Stated succinctly, *attackers exploit the problem of reciprocal security vulnerability in two ways simultaneously*: once in terms hunting access across *both the private and public sector* for their desired compromise, and a second time in terms of hunting for *either physical or digital data sources and access points* in furtherance of the desired compromise.

For these reasons, the paradigm of reciprocal security replaces the current policy focus on information sharing and deterrence with a focus on information vigilance infrastructure[41] and defense primacy.[42] Information vigilance infra-

32 *See id*. at 1157.
33 *Id*. at 1154-57.
34 *Id*. at 1127.
35 *Id*. at 1129
36 *Id*. at 1126-27.
37 *Id*. at 1161.
38 *Id*.
39 *Id*. at 1162.
40 *Id*. at 1164-65.
41 *Id*. at 1185.

structure refers to building baselines of shared security understanding and technical metrics that allow us to discuss and monitor security in meaningful ways.[43] Meaningful information sharing is impossible without correcting these deficits in our current policy and legal approaches.[44] Defense primacy, meanwhile, starts from the assumption that a portion of attacks will never be successfully deterred.[45] Attackers are often not deterrable, sometimes sponsored by nation-states,[46] and not within our jurisdictional reach. Our systems must, therefore, learn to prophylactically prevent, quickly recognize, and effectively mitigate compromise.[47] Currently, they do not.[48] As the severity and disruptive effects of attacks on both the public and private sectors continue to escalate, prevention, detection, and mitigation of the success of attacks must be the starting point for sound security policy, not simply trying to deter (often undeterrable) attackers.[49]

This essay expands on the five sets of recommendations made in *CYBER!* as a starting point for shifting to a model of reciprocal security. It provides a series of concrete legislative, regulatory and technical proposals that are presented in two groups, mirroring the two prongs of the reciprocal security paradigm – security vigilance infrastructure and defense primacy.[50]

Specifically, security vigilance infrastructure would be materially bolstered through the implementation of the following thwo sets of proposals:

Proposal 1: Creating new formal federal government security feedback loops51

A. Congress:

1. Congress should amend the Technology Assessment Act to create a new Congressional Office of Information Technology Assessment to assist policymakers and the public with analyzing technical questions of information technology, particularly security.

2. Congress should protect technical private sector security feedback by following the suggestion of the Copyright Office and making the

---

42 *Id*. at 1192.

43 *Id*. at 1179.

44 *Id*. at 1180.

45 *See id*. at 1182-83.

46 *See, e.g*., *Id*. at 1181 (describing an alleged attack by the government on Google to obtain information such as the identities of Chinese intelligence operatives).

47 *Id*. at 1182-83.

48 *Id*. at 1179-80.

49 *Id*. at 1194-95.

50 *Id*. at 1184.

51 *Id*. at 1185.

security research exemption to Section 1201 of the Digital Millennium Copyright Act permanent. Additionally, Congress should amend the Computer Fraud and Abuse Act, clarifying or replacing its key terms.[52]

3. Congress should instruct the Government Accountability Office to create an information security whistleblower "hotline" with a security ombudsman available to all government employees and government contractors.

B. Executive Branch:

1. The White House should expand future membership of the National Science and Technology Council ("NSTC") in the White House Office of Science and Technology Policy ("OSTP") to include all agencies and organizations directly engaged with information security enforcement.

2. The White House should encourage the creation of a visiting technologist and scholar-in-residence program at every major agency (and ask Congress to appropriate funds accordingly).

3. The White House should sign an executive order requiring that all government organizations comply with the principles embodied in ISO standards on security, in particular the principles reflected in ISO 30111 and 29147.

4. The Department of Justice should protect private sector technical feedback through security research by issuing advisory statements on CFAA enforcement and maintaining centralized CFAA indictment review, approval, and staffing.

C. Judiciary:

1. The Federal Judicial Center ("FJC") should create a roster of trusted technical experts on information security as a technical feedback loop to assist the federal judiciary.

2. The Administrative Office of the U.S. Courts should use redundancy as a security measure by permitting universities, libraries, and

[52] This Computer Fraud and Abuse Act inquiry is addressed elsewhere. *See* Andrea M. Matwyshyn & Stephanie K. Pell, *Broken* (Aug. 5, 2018) (on file with author).

other approved parties to maintain backup archives of PACER at their own expense.

Proposal 2: Improving security disclosure infrastructure across both the public and private sector to allow for meaningful progress tracking.[53]

A. Update current structures around security vulnerability tracking and make them usable to consumers.

B. Create the option of uniformity in security advisories' form and require their accuracy.

C. Create the option of uniformity in data breach notification and a single point of public filing.

Meanwhile, defense primacy would be meaningfully introduced into both the public and private sectors with the following starter initiatives:

Proposal 3: Defending supply chains to improve integrity.[54]

Both public and private sector organizations should regularly assess their third-party providers of software, hardware, and security services in terms of their responsiveness to security incidents and vulnerabilities. Contracts with these providers should be evolved in their terms or terminated as needed based on the findings of these supply chain assessments.

Proposal 4: Defending entrepreneurship with security tax incentives and tools.[55]

A. Create federal and state security upgrade tax incentives for entrepreneurs

B. Build new consumer, entrepreneur, and government security tools through contests

Proposal 5: Defending market integrity[56]

A. Federal and state regulators should vet security statements in regulatory filings and advertisements for accuracy and substantiation.

---

53 Matwyshyn, *supra* note 23, at 1190.

54 *Id*. at 1192.

55 *Id*. at 1193.

56 *Id*. at 1194.

B. Market participants should vet security as part of assessment of corporate governance and risk.

These proposals explicitly blend the public and private sectors dynamics of security to address the problem of reciprocal security vulnerability. They view information security – both "cyber" and physical – as part of a bigger security whole, and they start us down the path of integrating "cybersecurity" into the broader security discourse. The sections that follow explain each in greater detail.

III. RECIPROCAL SECURITY: SECURITY VIGILANCE INFRASTRUCTURE

In January 2015, the movie *Blackhat* debuted in U.S. theaters.[57] The movie's plot focuses on the joint law enforcement efforts of a military officer in China's internet warfare unit and a convicted computer intruder, a "hacker"[58] named Hathaway.[59] Hathaway receives a temporary release from prison in exchange for his assistance in tracking an attacker who has remotely damaged a nuclear power plant and a futures market.[60] Curious about technical experts' reactions to the film, the producers of *Blackhat* held special screenings for information security professionals in Silicon Valley[61] and Washington D.C. prior to the movie's national release.[62] The feedback that the *Blackhat* producers re-

[57] *Blackhat*, IMDB, http://www.imdb.com/title/tt2717822 [perma.cc/92AA-BUYA] (last visited Aug. 14, 2015).

[58] *Hacker*, OXFORD DICTIONARIES, http://www.oxforddictionaries.com/definition/american_english/hacker [https://perma.cc/E5PU-HJL2] (last visited Apr. 23, 2018) (defining "hacker" as "a person who uses computers to gain unauthorized access to data"); *but see, e.g.*, *Hackers,* TECH MODEL RAILROAD CLUB OF MIT, http://tmrc.mit.edu/hackers-ref.html [https://perma.cc/3JDH-QVB3] (last visited Apr. 23, 2018) ("We at TMRC use the term 'hacker' only in its original meaning, someone who applies ingenuity to create a clever result, called a 'hack'. . . . This original benevolent meaning stands in stark contrast to the later and more commonly used meaning of a 'hacker', typically as a person who breaks into computer networks in order to steal or vandalize. Here at TMRC, where the words "hack" and 'hacker' originated and have been used proudly since the late 1950s, we resent the misapplication of the word to mean the committing of illegal acts. People who do those things are better described by expressions such as 'thieves', 'password crackers'. or 'computer vandals'. They are certainly not true hackers, as they do not understand the hacker ethic.").

[59] *Blackhat*, *supra* note 58.

[60] *Id.*

[61] Cade Metz, *Is Blackhat the Greatest Hacking Movie Ever? Hackers Think So*, WIRED (Jan. 16, 2015, 6:30 AM), http://www.wired.com/2015/01/blackhat-the-best-cyber-movie/.

[62] *See*, *Come to ShmooCon and Get a Ticket to Blackhat for $20!*, SCHMOOCON, (Jan. 15, 2015), http://shmoocon.org/2015/01/15/come-to-shmoocon-and-get-a-ticket-to-blackhat-for-20/ [https://perma.cc/SB9F-88YP].

ceived from these audiences diverged[63] on the entertainment quality and technical[64] accuracy[65] of the movie. However, the security experts all agreed on one thing: the severity of existing security vulnerabilities was not overstated.[66] Serious vulnerabilities in both the public and private sectors are known,[67] often unpatched,[68] and sit ripe for exploitation[69] by malicious attackers.[70]

Perhaps surprisingly, the degree of formalization reflected in this (fictional security) movie's feedback loop is often missing from our real-life security policy processes. For this reason, the first prong of the reciprocal security paradigm involves the creation of information security vigilance infrastructures, and an initial step involves the creation of robust, formalized feedback loops from technical experts.

---

[63] Kashmir Hill, *Hackers Got a Sneak Peek at Michael Mann's New Hacker Movie 'Blackhat.' Verdict: It Doesn't Suck*, SPLINTER NEWS (Jan. 14, 2015, 11:10 AM), http://fusion.net/story/38341/hackers-review-blackhat/ [https://perma.cc/BH89-HKQE] ("'It was just where the rubber hit the road that they made mistakes. People laughed because there were text comments in the binary code.'"); Metz, *supra* note 62.

[64] *Id*.

[65] The world of information crime depicted in the movie included, for example, screwdriver stabbings. *See*, *Blackhat*, ROTTEN TOMATOES, https://www.rottentomatoes.com/m/blackhat/ [https://perma.cc/2UET-CQMF]. In the fifteen years that I have regularly spoken at computer security conferences, I have to date neither witnessed nor been apprised of any screwdriver stabbings among security professionals.

[66] For example, nuclear power reactors have already been plagued by common variants of malicious code. Sean Gallagher, *German Nuclear Plant's Fuel Rod System Swarming with Old Malware,* ARS TECHNICA (Apr. 27, 2016, 11:58 AM), https://arstechnica.com/information-technology/2016/04/german-nuclear-plants-fuel-rod-system-swarming-with-old-malware [https://perma.cc/NQ76-G7QR].

[67] *See* NAT'L VULNERABILITY DATABASE, https://nvd.nist.gov/ [https://perma.cc/SNT6-QU5N] (last visited Jan. 16, 2018).

[68] Tom Spring, *Outdated, Unpatched Software Rampant in Businesses*, THREAT POST (May 10, 2016, 1:57 PM), https://threatpost.com/outdated-unpatched-software-rampant-in-businesses/117976/ [https://perma.cc/96HL-gL5P].

[69] For example, critical infrastructure and industrial control systems have been found vulnerable in the past. *See* Brian Prince, *Majority of Critical Infrastructure Firms in Americas Have Battled Hack Attempts: Survey*, SECURITYWEEK (Apr. 7, 2015), http://www.securityweek.com/majority-critical-infrastructure-firms-americas-have-battled-hack-attempts-survey [https://perma.cc/HWV7-FHCF]. Similarly, numerous exchanges have been compromised. *See, e.g.*, Stephanie Yang and Elena Holodny, *The Massive Hack of the Nasdaq that has Wall Street Terrified of Cyber Attacks*, BUS. INSIDER (July 17, 2014, 3:37 PM), http://www.businessinsider.com/nasdaq-attacked-by-hackers-2014-7 [https://perma.cc/CKA5-ZE3Y].

[70] Nathaniel Popper, *Wall Street's Exposure to Hacking Laid Bare*, N.Y. TIMES (July 25, 2013, 8:34 PM), https://dealbook.nytimes.com/2013/07/25/wall-streets-exposure-to-hacking-laid-bare/.

A. Proposal 1: Creating New Formal Federal Government Security Feedback Loops[71]

Security feedback loops blending insights from both the public and private sector can be added in a relatively streamlined manner across all three branches of government.

1. New Congressional Feedback Loops

a. Congress should amend the Technology Assessment Act to create a new Congressional Office of Information Technology Assessment ("OITA") to assist policymakers and the public with analyzing technical questions of technology, particularly security.

As recent Congressional hearings over mobile device encryption have highlighted, Congress sometimes struggles with understanding the functionality and security impact of new technologies.[72] While some members arrive in Congress with a background in computer science[73] or professional experiences working in technology-related fields,[74] the majority of members of Congress do not. Instead, they tend to rely on (already overworked) members of their staff – who themselves usually do not necessarily possess expertise in technology policy – to get them up to speed. Witness testimony in hearings provides a useful source of information, but witnesses may not present all aspects of a particular technology policy issue or may conflict in their presentations. Outside of hearings, various interest groups may share information on technology

[71] Matwyshyn, *supra* note 23, at 1185.

[72] *See, e.g.*, Tony Romm, *'I can understand about 50 percent of the things you say': How Congress is struggling to get smart on tech*, WASH. POST (June 6, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/06/06/i-can-understand-about-50-percent-of-the-things-you-say-how-congress-is-struggling-to-get-smart-on-tech/?utm_term=.e6e9078e2b1a. *See also Deciphering the Debate over Encryption: Industry and Law Enforcement Perspectives: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 114th Cong. (2016).

[73] *See, e.g.*, *Sole House Dem with Computer Science Degree Will "Fight Like Hell" Against Trump*, UNITED STATES REPRESENTATIVE TED LIEU (Jan. 11, 2017), https://lieu.house.gov/media-center/in-the-news/sole-house-dem-computer-science-degree-will-fight-hell-against-trump [https://perma.cc/F8TK-35U4] (describing some members of Congress who have computer science degrees).

[74] *See, e.g.*, Mary M. Shaffrey & Carol S. Hook, *10 Things You Didn't Know About Mark Warner*, U.S. NEWS & WORLD REP. (June 9, 2017, 1:06 PM), https://www.usnews.com/news/articles/2008/11/05/10-things-you-didnt-know-about-mark-warner [https://perma.cc/787W-WZ4J] (describing Mark Warner's technology background before becoming a Virginia senator).

policy issues with members of Congress, but again they may be likely to present the issues only in part or in the best light for their own interests. In other words, the existing inputs on technical information for members of Congress can create an inconsistent stream of information, both across members and across issues. Meanwhile, particularly in the case of information security policy, the issues are both technically and legally complex. It is unreasonable to expect each member of Congress to acquire mastery of security independently. However, a supplemental information stream – one that is more efficient, technically rigorous, and neutral than current methods – is possible. In fact, historical precedent and Congressional authorization for it already exist; only updating and appropriation are required.

In 1972 the Technology Assessment Act[75] established the Congressional Office of Technology Assessment[76] ("OTA") with the goal of creating a feedback loop[77] of bi-partisan[78] technology expertise to inform lawmaking.[79] Congress

---

[75] Pub. L. No. 92–484, 86 Stat. 797 (1972).

[76] *Id*. at § 3(c), 86 Stat. at 797 (stating in relevant part that "[t]he basic function of the Office shall be to provide early indications of the probable beneficial and adverse impacts of the applications of technology and to develop other coordinate information which may assist the Congress").

[77] The Technology Assessment Act states as follows:

> The Congress hereby finds and declares that: (a) As technology continues to change and expand rapidly, its applications are — (1) large and growing in scale; and (2) increasingly extensive, pervasive, and critical in their impact, beneficial and adverse, on the natural and social environment. (b) Therefore, it is essential that, to the fullest extent possible, the consequences of technological applications be anticipated, understood, and considered in determination of public policy on existing and emerging national problems. (c) The Congress further finds that: (1) the Federal agencies presently responsible directly to the Congress are not designed to provide the legislative branch with adequate and timely information, independently developed, relating to the potential impact of technological applications, and (2) the present mechanisms of the Congress do not and are not designed to provide the legislative branch with such information. (d) Accordingly, it is necessary for the Congress to— (1) equip itself with new and effective means for securing competent, unbiased information concerning the physical, biological, economic, social, and political effects of such applications; and (2) utilize this information, whenever appropriate, as one factor in the legislative assessment of matters pending before the Congress, particularly in those instances where the Federal Government may be called upon to consider support for, or management or regulation of, technological applications.

Id. at § 2, 86 Stat. at 797.

[78] *See id*. at § 4(a), 86 Stat. at 798; Jathan Sadowski, *The Much-Needed and Sane Congressional Office That Gingrich Killed Off and We Need Back*, THE ATLANTIC (Oct. 26, 2012), https://www.theatlantic.com/technology/archive/2012/10/the-much-needed-and-sane-congressional-office-that-gingrich-killed-off-and-we-need-back/264160/ [https://perma.cc/V745-LXZW] (explaining that OTA was "overseen by the 'Technology Assessment Board' which was made up of 13 members: a non-voting director, six senators (three each from the minority and majority party), and six representatives (three each again)").

[79] *Id*.

created OTA during the height of the Cold War in part to advise members on the briskly changing landscape of national security technologies[80] and advancing U.S. leadership in the Space Race.[81] OTA's formation recognized that highly technical fields such as aerospace engineering rely upon complex engineering and science research that is difficult for non-specialists to fully process,[82] and Congress lacked an internal trusted source for rigorous technical analysis.[83] Therefore, the role of OTA was to offer Congress a definitive source of technical analysis, presenting a full spectrum of policy options on particular technology topics with assessments of the feasibility of each.[84] OTA acted as a non-partisan information source and did not advocate for a specific policy; rather, it allowed policy-makers in Congress to weigh the choices themselves.[85] Additionally, OTA analyzed not only short-term technology policy, but also long-term policy patterns in order to recognize key trends across time.[86] In other words, OTA aimed to be a type of neutral "think tank" for Congress.

During its existence between 1972 and 1995, OTA released over 750 studies,[87] and its legacy continues to this day.[88] However, as the Cold War wound down, OTA seemed less essential to many members of Congress.[89] Its budget was zeroed out, and it was defunded in 1995.[90]

Two decades later, our changed economic and national security circumstances warrant reconsideration of this Congressional appropriations decision. While the 1990's and 2000's presented an era with the easing of these traditional Cold War tensions, the current decade is marked by their resurgence. These new international security tensions are driven in particular by concerns over information security threats to national security[91] and preserving U.S.

---

80 *See id*.

81 *See id*.

82 *Id*.

83 *See* § 2, 86 Stat. at 797.

84 Sadowski, *supra* note 79.

85 *Id*.

86 *See id*.

87 *Id*.

88 *See* Celia Wexler, Opinion, *Bring Back the Office of Technology Assessment*, N.Y. TIMES (May 28, 2015), http://www.nytimes.com/roomfordebate/2015/05/28/scientists-curbing-the-ethical-use-of-science/bring-back-the-office-of-technology-assessment. OTA's studies function as an important historical record of innovation policy in the U.S. in the 1970's and 1980's. Also, OTA's success was noticed internationally, as the United Kingdom and the European Union created corollary technical advisory bodies modeled on OTA. *Id*.

89 Sadowski, *supra* note 79.

90 Wexler, *supra* note 89.

91 *See* Jim Garamone, *Cyber Tops List of Threats to U.S., Director of National Intelligence Says*, U.S. DEP'T OF DEF. (Feb. 13, 2018)

leadership as the world's leading innovation economy.[92] Succinctly stated, information security is likely today's version of both the Cold War and Space Race. It is a highly technical, complex field full of nuance that, much like rocket science, is difficult for outsiders to fully process. Also, much like the Cold War, failing to address it threatens to lead to avoidable loss of life,[93] significant financial expense,[94] and reputational harm to the U.S.

Admittedly, OTA in its 1972 incarnation and structure[95] may not be a perfect fit for today's political reality. As such, Congress should update the Technology Assessment Act by creating (and providing an appropriation for[96]) an updated version of the OTA- a new "Office of Information Technology Assessment" or "OITA." This new OITA would maintain a bi-partisan advisory mission, but, unlike the past incarnation of OTA, it would be significantly more limited in scope to matters of information technology policy. In particular, the new OITA would advise Congress on the technical and policy aspects of information security, producing public reports on both short-term and long-term issues in technical aspects of security.

To best address the risks of reciprocal vulnerability, the composition of the new OITA should include career and rotating members from both the public and private sectors – a non-voting (career) director, a set of six staff technology and policy analysts,[97] and an advisory board of six computer science and legal academics selected by the National Academies, as well as six private sec-

https://www.defense.gov/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/ [https://perma.cc/3TYX-R4UW].

92 DEP'T OF COMMERCE INTERNET POL'Y TASK FORCE CYBERSECURITY, INNOVATION AND THE INTERNET ECONOMY 1 (2011), https://www.nist.gov/sites/default/files/documents/itl/Cybersecurity_Green-Paper_FinalVersion.pdf [https://perma.cc/52ZX-EDHN].

93 *See, e.g.*, Alex Hern, *Hacking Risk Leads to Recall of 500,000 Pacemakers Due to Patient Death Fears,* THE GUARDIAN (Aug. 31, 2017, 8:23 AM), https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update [https://perma.cc/J4FH-H4RE] (describing how half a million pacemakers were recalled by the US Food and Drug Administration due to fears that the devices could be hacked to drain the batteries or alter the patient's heartbeat).

94 *See, e.g.*, Adam Shepherd, *Emergency Patches Cost Companies Almost $100,000 Every Month*, ITPRO (June 1, 2017), http://www.itpro.co.uk/security/28756/emergency-patches-cost-companies-almost-100000-every-month [https:// perma.cc/CZM6-UXT7] (explaining that the issuance of emergency patches for newly-discovered security threats are costing business $100,000 per month).

95 *See* Sadowski, *supra* note 79.

96 Because OTA was merely defunded, the zeroed-out budgetary line item could be resurrected through an appropriation.

97 Three of these analysts would be selected by majority party and three by the minority party.

tor technology professionals selected on the basis of their areas of expertise.[98] OITA would consult with Congress on current legislative initiatives and author brief "white papers" explaining the state of technology without making policy recommendations. It would also engage in long term "futures" thinking, identifying and anticipating likely information technology trends and their possible technological consequences for our economy and our national security.[99] All OITA documents would be intended for public distribution.[100]

Because of its hybrid public-private sector team, OITA would incorporate private sector insights directly into its analysis, improving knowledge integration between the two sectors, among members of Congress, and among citizens[101] who wish to learn from OITA's reports. Meanwhile, having a single point of contact inside Congress for technical security inquiries would create efficiencies,[102] both for members of Congress and their staff. Members of Congress would be free to focus on normative policy and legal questions in hearings, knowing that a shared baseline of technical information is available to their colleagues. Staff would be free to supplement with additional policy analysis, but they would be spared from performing duplicative technical background research, both on issues at hand and on the context of broader historical technical trends. None of the Congressional Research Service,[103] the

[98] Three of these professionals would be selected by the majority party and three by the minority party.

[99] OTA was critiqued for failing to include adequate "anticipatory aspects of technology assessment more rigorously in its approach." Sadowski, *supra* note 79.

[100] For example, they might be disseminated through the OITA website and social media, such as the OITA Twitter feed.

[101] One way that citizens could learn about security might be from official government sources like Congressional Research Service Reports, however these reports have traditionally not been shared with the public. See, e.g., Chris Mooney, *Requiem for an Office*, 61 BULL. OF THE ATOMIC SCIENTISTS 41, 47 (2005), http://sciencepolicy.colorado.edu/students/envs_5100/Mooney.pdf [https://perma.cc/T6NM-V322] (commenting that CRS reports are also not available to the public for scrutiny or comment.). *But see* Joe Mullin, *Congress Will Finally Make Its Research Reports Public*, ELEC. FRONTIER FOUND. (Apr. 2, 2018), https://www.eff.org/deeplinks/2018/04/you-always-wanted-read-crs-reports-now-you-can [https://perma.cc/JZL4-W6G9] ("The [2018 Consolidated Appropriations Act — now Public Law 115-141] specifies that the [Congressional Research Service] reports must be "searchable, sortable, and downloadable, including downloadable in bulk.").

[102] Although it was eliminated for ostensibly budgetary reasons, OTA appears to have been cost-effective. For example, it conducted a critique of a Social Security Administration plan to procure computers, saving "$368 million—the yearly cost of operating OTA many times over." *Id.* at 48.

[103] The Congressional Research Service offers analyses to Congress on legislative topics upon request, but it tends not to follow issues in a long-term manner. *See*, *About CRS*, CONG. RESEARCH SERV. (LIBRARY OF CONG.), https://www.loc.gov/crsinfo/about/ [https://perma.cc/Z9PE-B6QE] (last visited Sept. 9, 2017). It describes itself as "shared staff to con-

Government Accountability Office[104] or the National Academies[105] currently fills this role.

b. Congress should protect technical feedback by following the suggestion of the Copyright Office and making the security research exemption to Digital Millennium Copyright Act ("DMCA") Section 1201 permanent.

As previously described in *CYBER!*,[106] the DMCA has historically chilled a portion of security research that benefits the safety of both the public and private sector:[107] until 2015, the absence of a robust security research exemption under Section 1201 negatively impacted much-needed research on information security.[108] However, in 2015, the Library of Congress agreed to remedy this

gressional committees and Members of Congress . . . [who] assist at every stage of the legislative process — from the early considerations that precede bill drafting, through committee hearings and floor debate, to the oversight of enacted laws and various agency activities . . . [and] reports on major policy issues, tailored confidential memoranda, briefings and consultations, seminars and workshops, expert congressional testimony, [and] responses to individual inquiries." *Id*.

[104] The current incarnation of the Government Accountability Office also does not provide the type of issue-specific technical expertise that members of Congress require for meaningful deliberation. Its current role focuses primarily on evaluation of ongoing programs. GAO described itself as the "congressional watchdog," investigating how the federal government spends taxpayer dollars. U.S. GOV'T ACCOUNTABILITY OFFICE, https://www.gao.gov/about/index.html (last visited Sept. 9, 2017) [https://perma.cc/4JS3-N43V].

[105] The National Academy of Sciences works to provide independent, objective analysis and advice to the nation and conduct other activities to solve complex problems and inform public policy decisions. NAT'L ACAD. OF SCI., http://www.nasonline.org/about-nas/mission/ [https:// perma.cc/5W4B-LP6J] (last visited Sept. 9, 2017).

[106] Matwyshyn, *supra* note 23, at 1146-49.

[107] *See, e.g.*, *Long Comment Regarding a Proposed Exemption under 17 U.S.C. 1201*, U.S. COPYRIGHT OFF., at 3-4 http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_SecurityResearchers_Class25.pdf [https://perma.cc/B2BP-STFB] (last visited Feb. 23, 2017) (recounting various instances of security research that has not been performed on advice of counsel or performed only because of intervention and direct request from a Secretary of State and stating that "[a]ttorneys regularly counsel . . . that the DMCA is an unclear statute and that undertaking any such research exposes the researcher to legal risk. As such, attorneys usually counsel against continuing the research.").

[108] *Id*. Copyright holders are perceived to sometimes use threats of litigation to silence security researchers, preventing them from alerting both the public and regulators to unreasonable security deficits. Kim Zetter, *With Lock Research, Another Battle Brews in the War Over Security Holes*, WIRED (May 6, 2015), https://www.wired.com/2015/05/lock-research-another-battle-brews-war-security-holes/ [https://perma.cc/JKT4-XP3S].

constraint and granted the request of a group of academic proponents[109] for a broad security research exemption to Section 1201 of the DMCA.[110]

Specifically, the proponents had argued that DMCA Sections 1201(f), (g), and (j)[111] when read together with Section 1201(i),[112] particularly in context of legislative history, demonstrate that Congress never intended for the DMCA to create an opportunity for copyright owners to engage in frivolous strike suits that harm national security and consumer protection through inhibiting information security research.[113] In fact, in 1201(i), Congress expressly contemplated research by creating a right for purchasers to investigate and understand how products collect data about them.[114] The Copyright Office and Library of Congress's grant of this exemption was a significant moment for both security and consumer protection. As the record demonstrated, ample support existed for the exemption, and the request was supported by both public[115] and private sector[116] organizations. In this way, it highlighted that the basics of good security policy span both the public and private sectors.

---

[109] This author acted as counsel to four computer scientists whose research focuses on security. The group was dubbed "The Security Researchers" by the Copyright Office. *See id*.

[110] Jen Ellis, *New DMCA Exemption is a Positive Step for Security Researchers*, RAPID7: BLOG (Oct. 28, 2015), https://blog.rapid7.com/2015/10/28/new-dmca-exemption-is-a-positive-step-for-security-researchers/ [https://perma.cc/6GRU-5HRZ].

[111] *Long Comment Regarding a Proposed Exemption under 17 U.S.C. 1201*, *supra* note 108, at 4. The exemption clarified the scope of statutorily allowed research in Sections 1201(f), (g) and (j) in light of the ambiguities created by new types of information security threats facing companies, consumers, and our country's national security.

[112] *Id*. at 5. Section 1201(i) on its face demonstrates that Congress specifically contemplated and sought to protect the public from malfunctioning, flawed or vulnerable code that harms consumers: Section 1201(i) states that a consumer's investigation of code functionality on a privately-owned system in order to determine whether a privacy harm is happening does not constitute an impermissible circumvention. In this spirit of 1201(i), this exemption empowers consumers with access to better information about how computer code is behaving on their systems and the systems upon which their safety relies.

[113] *Id*. at 4-5.

[114] *Id*. at 5.

[115] *See Class 25 Comments on the Recommendations of the National Telecommunications and Information Administration to the Register of Copyrights*, NAT'L TELECOMM. AND INFO. ADMIN., at 72 (Sept. 18, 2015), https://www.copyright.gov/1201/2015/2015_NTIA_Letter.pdf [https://perma.cc/9HCJ-GN86] ("After reviewing the record, NTIA is convinced that good faith security researchers and academics are currently being deterred from engaging in noninfringing activities due to the threat of litigation under Section 1201.").

[116] *See Short Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201*, INTERNET ASS'N, https://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_InternetAssociation_Class25.pdf [https://perma.cc/2FWK-YTXQ] ("[I]f the exemption is granted, security researchers inside

With the approval of this broad exemption to Section 1201[117] for security research on consumer-used products,[118] the security research climate has mate-

companies will be better able to defend corporate intellectual property assets, as well as the data of the consumers who trust us with their information. Similarly, external security researchers would more readily report any malfunctions, flaws or vulnerabilities to us in order to assist us in improving our offerings – a practice we support and financially reward through bug bounty programs."). In particular, a group of companies signed a petition, expressing concern over the legal uncertainty surrounding security research under the DMCA, believing it to damage their businesses and the future of U.S. innovation. *See*, *Petition for Proposed Exemption under 17 U.S.C § 1201*, U.S. COPYRIGHT OFF., at 5, https://copyright.gov/1201/2014/petitions/Bellovin_1201_Intial_Submission_2014.pdf [https://perma.cc/A9PS-LJ8A].

[117] The granted exemption to Section 1201 of the DMCA reads as follows:

(i) Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates solely for the purpose of good-faith security research and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code; and provided, however, that, except as to voting machines, such circumvention is initiated no earlier than 12 months after the effective date of this regulation, and the device or machine is one of the following:

(A) A device or machine primarily designed for use by individual consumers (including voting machines);

(B) A motorized land vehicle; or

(C) A medical device designed for whole or partial implantation in patients or a corresponding personal monitoring system, that is not and will not be used by patients or for patient care.

(ii) For purposes of this exemption, ''good-faith security research'' means accessing a computer program solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, where such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.

Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 C.F.R. § 201.40(7) (2015).

[118] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65,944, 65,956 (Oct. 28, 2015) ("[T]he Register recommended adopting an exemption to enable good-faith security research on computer programs within devices or machines primarily designed for use by individual consumers (including voting machines), motorized land vehicles, and implanted medical devices and their corresponding monitoring systems . . . . The Register concluded that good faith security research into computer programs used to operate such devices and machines is likely a noninfringing fair use of those programs or, in the case of vehicle software, may be a noninfringing use under section 117. The Register also concluded that the permanent exemptions in sections 1201(f), 1201(g), and 1201(j) are inadequate to accommodate the proposed research activities due to various limitations and conditions contained in those provisions. Further, with respect to computer programs used to operate the types of devices and ma-

rially improved.[119] However, the exemption requires renewal every three years.[120] For this reason, in a June 2017 Review of Section 1201, the Copyright Office expressly urged Congress to protect the technical feedback loop of security research by creating a permanent security research exception using the language of the current security research exemption as a starting point.[121]

Thus, Congress should implement the Copyright Office's suggestion to amend DMCA Section 1201 with a permanent security research exemption covering consumer-used products. As the Copyright Office explained, an amendment of this type would defend an important technical feedback loop. It would encourage security research production – *i.e.* the creation of new creative works – without altering any of the numerous other legal remedies copyright holders have at their disposal.[122] As recognized by the Copyright Office, security researchers are the first line of defense against the problem of reciprocal security vulnerability. [123]

Security research is a key technological audit mechanism that is critical to the ongoing safety of computer code and preserving public trust in U.S. innovation policy and our economy. In addition to academic and private sector individual researchers, security-conscious companies[124] and public sector organ-

chines encompassed by the recommended exemption, the Register additionally found that legitimate security research has been hindered by TPMs that limit access to those programs").

[119] The exemption has already facilitated secondary analysis and critique by the press to arise regarding security of consumer products. *See, e.g.*, *Antivirus Software Buying Guide*, CONSUMER REPORTS, https://www.consumerreports.org/cro/antivirus-software/buying-guide/index.htm [https://perma.cc/8LP9-3QHL] (last updated Nov. 2017) (including ratings of various security products).

[120] 17 U.S.C. § 1201(a)(1)(B)-(D) (2012).

[121] The Copyright Office described its rationale for recommending that Congress create a permanent exception for security research in Section 1201 of the DMCA. The report states that:

> [E]ven some stakeholders content with the current statute acknowledged the legitimate interests of good-faith security researchers. In light of stakeholder comments and the past experiences of the triennial rulemaking, the Copyright Office recommends that Congress consider reforming this exemption to better accommodate a broader range of legitimate security research, without compromising copyright's core objectives. . . . [T]he Office believes that this measured approach will help accommodate critical cybersecurity concerns while preserving the copyright objectives in the anticircumvention provisions [and] . . . that the exemption adopted in 2015 can be a useful starting point . . . .

U.S. COPYRIGHT OFFICE, SECTION 1201 OF TITLE 17, at 74 (June 2017), https://www.copyright.gov/policy/1201/section-1201-full-report.pdf [https://perma.cc/68UM-GEJP] [hereinafter SECTION 1201].

[122] *See id.*

[123] *See id.*

[124] *See, e.g.*, Luke Larsen, *How Google's 'Project Zero' Task Force Races Hackers to Snuff Out Bugs*, DIGITAL TRENDS (Mar. 2, 2018, 3:00 AM),

izations are themselves engaging in security research into other companies' products in order to safely interoperate with them.[125] Reports of malfunctions, security flaws and vulnerabilities now frequently come from one company to another.[126] While technology creators tend to test their code for errors, not all errors are known at the time of release,[127] and some companies do not test well. [128] Even companies in the same industry diverge in their handling of basic information security corrections to flaws in their products.[129] For example, in a recent notable case, a researcher found vulnerabilities in a medical device that resulted in an FDA warning letter[130] and a recall notice, urging patients to report to health care providers for a firmware update.[131] Yet, the

https://www.digitaltrends.com/computing/google-project-zero-holding-the-industry-accountable-cybersecurity [https://perma.cc/9NM5-5HRQ].

[125] *Id*.

[126] *See, e.g*., Adrianne Jeffries, *Google Engineers Found over Half the Bugs in Microsoft's Latest Security Update*, THE VERGE (Feb. 13, 2013, 9:00 AM), http://www.theverge.com/2013/2/13/3983846/googlers-found-over-50-percent-of-the-bugs-in-microsofts-massive-update [https://perma.cc/C9QV-Q36C].

[127] Also, some less responsible copyright holders refuse to correct serious, known vulnerabilities, even when demands for correction come directly from government bodies. *See, e.g*., *Advisory (ICSA-14-084-01) Festo CECX-X-(C1/M1) Controller Vulnerabilities*, INDUS. CONTROL SYS. CYBER EMERGENCY RESPONSE TEAM, DEPT. HOMELAND SECURITY (Apr. 24, 2014), https://ics-cert.us-cert.gov/advisories/ICSA-14-084-01 [https://perma.cc/3XH2-RUR3] (stating that a vendor "has decided not to resolve these vulnerabilities, placing critical infrastructure asset owners using this product at risk").

[128] *See* Charlie Osborne, *A SSHowDowN in security: IoT devices enslaved through 12 year old flaw*, ZDNET (Oct. 12, 2016), https://www.zdnet.com/article/a-sshowdown-in-security-iot-devices-attack-devices-through-12-year-old-flaw/ [https://perma.cc/Y3YR-F47M] ("[T]he research team found that the continual failure of IoT device vendors to secure IoT and implementing [sic] default and hard-coded credentials is throwing the door wide open for attackers to exploit them.").

[129] *See, e.g*., Jim Finkle, *J&J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking*, REUTERS (Oct. 4, 2016, 7:05 AM), https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e/jj-warns-diabetic-patients-insulin-pump-vulnerable-to-hacking-idUSKCN12411L [https://perma.cc/W9AP-75VR] (demonstrating that some medical device manufacturers proactively communicate security warnings to consumers without FDA recall).

[130] Letter from Capt. Sean M. Boyd, MPH, USPHS, Deputy Dir. for Regulatory Affairs, U.S. Food and Drug Admin., to Mike Rousseau, President, Abbott Cardiovascular and Neuromodulation (Apr. 12, 2017) (on file with the U.S. Food and Drug Administration), https://www.fda.gov/iceci/enforcementactions/warningletters/2017/ucm552687.htm [https://perma.cc/ZJ4Z-X75N].

[131] *Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication*, U.S. FOOD & DRUG ADMIN. (Aug. 29, 2017),
https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm [https://perma.cc/7ETT-9Y7K].

medical device company, nevertheless, sued the security researcher over the truthful disclosure of security flaws.[132] Meanwhile, other medical device companies foster cooperative relationships with researchers.[133]

c. Congress should instruct the Government Accountability Office ("GAO") to create an information security whistleblower "hotline" with a security ombudsman available to all government employees and government contractors.

In 2013, a defense contractor employee named Edward Snowden shared national security information with the press, detailing a potentially unconstitutional domestic surveillance program.[134] When asked why he chose to go to the press rather than using the chain of command and established channels, Snowden asserted that he had exhausted those remedies and received no satisfactory attention for his concerns.[135] Regardless of whether the particular facts of Snowden's case are ultimately determined to be as alleged,[136] the question of contractors and whistleblowing indeed requires attention. Some of the largest public sector data breaches have occurred allegedly because of the actions of private sector contractors.[137]

For example, consider the Office of Personnel Management data breach which exposed personnel records of an estimated eighteen million federal employees,[138] described by the House of Representatives Oversight and Government Reform Committee as a breach that "jeopardized our national security for

[132] Justine Bone, *Independent Research Confirms St. Jude Security Vulnerabilities*, MEDSEC (Mar. 2018), https://medsec.com/entries/stj-lawsuit-response.html [https://perma.cc/D6GZ-WNFM].

[133] Finkle, *supra* note 130.

[134] *Edward Snowden Fast Facts*, CNN, https://www.cnn.com/2013/09/11/us/edward-snowden-fast-facts/index.html [https://perma.cc/Y53F-HSXS] (last updated June 14, 2017, 5:32 PM).

[135] Julian Hattem, *Email Suggests Snowden Went to NSA First*, THE HILL (May 29, 2014, 10:23 AM), http://thehill.com/policy/technology/207563-snowden-went-to-nsa-bosses-before-press [https://perma.cc/39QS-SCMX].

[136] Kim Zetter, *NSA Releases Snowden Email, Says He Raised No Concerns about Spying*, WIRED (May 29, 2014, 3:16 PM), https://www.wired.com/2014/05/snowden-email-to-nsa/.

[137] *See, e.g.*, Jon Swaine, *NSA Contractor Reality Winner Accused of Leaking File on Russia Election Hacking,* GUARDIAN (June 6, 2017, 4:23 PM), https://www.theguardian.com/us-news/2017/jun/05/reality-winner-russia-us-election-hack-nsa-leak [https://perma.cc/2FZX-TRNL] (identifying an NSA contractor as the source of an NSA data leak).

[138] Evan Perez & Shimon Prokupecz, *First on CNN: U.S. Data Hack May Be 4 Times Larger than the Government Originally Said*, CNN (June 24, 2015, 2:59 AM), http://edition.cnn.com/2015/06/22/politics/opm-hack-18-milliion/index.html [https://perma.cc/KJ26-BTCT].

more than a generation."[139] The most recent forensic information appears to demonstrate that a private sector contractor was at least partially allegedly at fault[140] – another example of the problem of reciprocal vulnerability. But, the Government Accountability Office has also warned of inadequate security inside federal departments and agencies for over a decade.[141]

Consider a situation where a private sector contractor on assignment to a federal agency recognizes that the system she is being asked to update is dangerously vulnerable, risking significant national security consequences if compromised. Imagine that this contractor alerts the management of the particular agency, but the key decision makers in the agency fail to understand the gravity of the situation or are unwilling to reallocate budget toward security correction. That contractor has used the correct reporting channels but failed. The channels are exhausted, and no obvious whistleblowing path currently exists for this contractor outside the agency.[142] She may view her only option to be going to the press and risking personal criminal consequences. Yet, her warning is certainly desirable and important from a national security perspective.[143] Additional governmental reporting channels can and should be created for this information.

Congress can provide an additional outlet for whistleblowers' concerns by creating a security hotline inside the GAO[144] and establishing a process for referring credible security threats to an appropriate Congressional oversight

---

[139] MAJORITY STAFF OF H. COMM. ON OVERSIGHT AND GOV'T REFORM, 114TH CONG., THE OPM DATA BREACH: HOW THE GOVERNMENT JEOPARDIZED OUR NATIONAL SECURITY FOR MORE THAN A GENERATION (2016), https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf [https://perma.cc/4BNH-FKA8].

[140] Aaron Boyd, *Contractor Breach Gave Hackers Keys to OPM Data*, FED. TIMES (June 23, 2015), https://www.federaltimes.com/smr/opm-data-breach/2015/06/23/contractor-breach-gave-hackers-keys-to-opm-data/ [https://perma.cc/8CN2-SJKH].

[141] *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-05-827T, CRITICAL INFRASTRUCTURE PROTECTION: CHALLENGES IN ADDRESSING CYBERSECURITY (2005).

[142] Her employer is unlikely to be willing to intercede with the agency for fear of losing a government contract.

[143] For a discussion of the First Amendment and leaks of national security information, see, for example, Heidi Kitrosser, *Free Speech Aboard the Leaky Ship of State: Calibrating First Amendment Protections for Leakers of Classified Information*, 6 J. NAT'L SEC. L. & POL'Y 409, 441 (2013) (arguing in favor of the balancing test in *Pickering v. Board of Education*, 391 U.S. 563 (1968), in the context of civil and administrative sanctions and strict scrutiny for criminal sanctions).

[144] The GAO "is an independent, nonpartisan agency that works for Congress. Often called the 'congressional watchdog,' GAO investigates how the federal government spends taxpayer dollars. The head of GAO, the Comptroller General of the United States, is appointed to a 15-year term by the President from a slate of candidates Congress proposes." U.S. GOV'T ACCOUNTABILITY OFF., https://www.gao.gov/about/index.html [https://perma.cc/K746-HNPZ] (last visited April 25, 2018).

committee. A new official feedback loop of this sort may both prevent a portion of security compromises and also assist in catching any gross institutional mismanagement of government information early. The cost of setting up a whistleblower hotline in GAO would be minimal[145] and in line with GAO's mission.[146]

Again, some historical precedent exists. In 2013, GAO launched a pilot program in collaboration with individual agencies and departments that was intended to provide increased whistleblower protections for contractors.[147] However, in its 2017 assessment of the program, GAO found that some agencies "did not forward investigation findings to the appropriate entities," and that "[s]ome contractors . . . were unaware of their obligations under the pilot program."[148] Also, GAO's follow-up recommendations from this pilot were agency-specific[149] and, apparently, not always implemented.[150] While individual agency and department changes likely improved security and facilitated whistleblowing at least in part,[151] they did not address the situation where a prospective whistleblower believes the intra-agency reporting channels have stalled or failed. Indeed, since the pilot program, GAO has continued to raise concerns about the adequacy of whistleblower channels in various agencies

[145] GAO already performs auditing functions consistent with the type of follow-up inquiry a whistleblower report would require. *Id*. GAO also engages in "auditing agency operations to determine whether federal funds are being spent efficiently and effectively; investigating allegations of illegal and improper activities; reporting on how well government programs and policies are meeting their objectives; performing policy analyses and outlining options for congressional consideration; and issuing legal decisions and opinions, such as bid protest rulings and reports on agency rules." *Id*.

[146] *Id*. ("Our Mission is to support the Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government for the benefit of the American people. We provide Congress with timely information that is objective, fact-based, nonpartisan, nonideological, fair, and balanced.")

[147] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-17-227, CONTRACTOR WHISTLEBLOWER PROTECTIONS PILOT PROGRAM, IMPROVEMENTS NEEDED TO ENSURE EFFECTIVE IMPLEMENTATION (2017).

[148] *Id*.

[149] *Id*.

[150] *Id*.

[151] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-860T, WHISTLEBLOWER PROTECTIONS: DOD HAS IMPROVED OVERSIGHT FOR REPRISAL INVESTIGATIONS BUT CAN TAKE ADDITIONAL ACTIONS TO STANDARDIZE PROCESS AND REPORTING (2016).

and departments.[152] In particular, in 2016, GAO issued a report asserting that whistleblower channels related to critical infrastructure were inadequate.[153]

An external whistleblower reporting mechanism managed by GAO and an appropriate Congressional committee would directly address the situation where an agency does not address internal security deficits or where the whistleblower fears internal retribution. A GAO whistleblower hotline – one not monitored by individual agencies but rather by GAO itself – offers a straightforward secondary backstop for this type of security situation. If even a single Snowden-like information leak is prevented through the existence of this hotline, the averted damage and expense would render the hotline highly cost-effective.

2. New Executive Branch Feedback Loops

a. The White House should expand future membership of the National Science and Technology Council ("NSTC") in the White House Office of Science and Technology Policy ("OSTP") to include all agencies directly engaged with information security.

The White House Office of Science and Technology Policy has traditionally included a National Science and Technology Council.[154] This council has historically been comprised of various departments, agencies, and governmental organizations that directly interact with some aspect of technology regulation.[155] In particular, organizations concerned with security such as the Central Intelligence Agency, the Department of Defense, and the Department of Justice were represented on the council.[156] However, many of the other agencies directly involved with security enforcement were absent from OSTP's NSTC.[157] This absence potentially creates an undesirable imbalance between

[152] *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-618, DEPARTMENT OF ENERGY: WHISTLEBLOWER PROTECTIONS NEED STRENGTHENING (2016) (raising concerns about the adequacy of whistleblower protections inside governmental organizations).

[153] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-572, CRITICAL INFRASTRUCTURE PROTECTION: IMPROVEMENTS NEEDED FOR DHS'S CHEMICAL FACILITY WHISTLEBLOWER REPORT PROCESS (2016).

[154] *NSTC*, THE WHITE HOUSE: OBAMA ARCHIVE, https://obamawhitehouse.archives.gov/administration/eop/ostp/nstc [https://perma.cc/25T2-AL8V] (last visited Jan. 24, 2018).

[155] *Id.*

[156] *NSTC Members*, THE WHITE HOUSE: OBAMA ARCHIVE, https://obamawhitehouse.archives.gov/administration/eop/ostp/nstc/about/members [https://perma.cc/X5GW-5DNM] (last visited Jan. 24, 2018).

[157] Not all agencies whose missions directly impact innovation policy were included in NSTC under the Obama administration. *See id.* For example, the Federal Trade Commis-

criminal and civil security enforcement: it means that private sector innovation, competition, and consumer protection concerns are comparatively underrepresented in OSTP consultations on security policymaking.[158]

Specifically, the NSTC should be expanded to include representatives of all governmental organizations directly involved in information security enforcement and innovation policy formulation, including the Chair of the Federal Trade Commission, the Chair of the Securities and Exchange Commission, the Chair of the Commodity Futures Trading Commission, the Director of the Consumer Financial Protection Bureau, and the Commissioner of the Food and Drug Administration. Each of these organizations engages in enforcement of some aspect of security. Their involvement would ensure that the council adequately considers the impact of security decisions on the private sector, our economy, and the future of innovation policy.[159]

b. The White House should encourage the creation of a visiting technologist and scholar in residence program at every major agency (and ask Congress to appropriate accordingly).

sion, the Securities and Exchange Commission, and the Food and Drug Administration were not included despite their ongoing enforcement and policy activity in security. *Id.*

[158] Members of the NSTC have, in the past, included the President, the Vice President, the Secretary of the U.S. Department of State, the Secretary of the U.S. Department of the Treasury, the Secretary of the U.S. Department of Defense, the Attorney General, representing the U.S. Department of Justice, the Secretary of the U.S. Department of the Interior, the Secretary of the U.S. Department of Agriculture, the Secretary of the U.S. Department of Commerce, the Secretary of the U.S. Department of Labor, the Secretary of the U.S. Department of Health and Human Services, the Secretary of the U.S. Department of Homeland Security, the Secretary of the U.S. Department of Transportation, the Secretary of the U.S. Department of Energy, the Secretary of the U.S. Department of Education, the Secretary of the U.S. Department of Veterans Affairs, the Administrator of the Environmental Protection Agency, the Administrator of the National Aeronautics and Space Administration, the Director of the Central Intelligence Agency, the Director of the National Institutes of Health, the Director of the National Science Foundation, the Director of the Office of Management and Budget, the Director of the Office of Science and Technology Policy, the Chair of the Council of Economic Advisors, the Chair of the Council on Environmental Quality, the Assistant to the President for Domestic Policy, Domestic Policy Council, the Assistant to the President for Economic Policy and Director of the National Economic Council, the Assistant to the President for National Security Affairs, National Security Council, the Secretary of the Smithsonian Institution, and the Assistant to the Vice President for Domestic Policy, Office of the Vice President. *NSTC Members, supra* note 157.

[159] Existing White House councils addressing information security have raised concern over their exclusion of private sector representatives or governmental organizations most engaged with the private sector, thus, arguably, exacerbating the problem of reciprocal vulnerability. *See, e.g.*, Stephanie K. Pell & LTC James Finocchiaro, *The Ethical Imperative for a Vulnerabilities Equities Process and How the Common Vulnerability Scoring System Can Aid that Process,* 49 CONN. L. REV. 1549 (2017) (discussing the White House Vulnerability Equities Process, one of the councils that has been critiqued along these lines).

A common private sector strategy for infusing fresh ideas into an organization involves bringing in outsiders as consultants. This model also exists in some agencies in the federal government. The White House should encourage federal agencies to build a private sector feedback loop of the type successfully launched at the FTC[160] and other agencies[161] through security expert-in-residence programs. As described in *CYBER!,* one of the most challenging elements of nudging information security policy in harmonized directions across the public and private sectors involves the absence of shared language and terminology.[162] Fixed-term private sector technical and legal experts can nudge security policymaking inside agencies in ways that career employees and political appointees cannot, and formalized exchanges of this nature facilitate tacit security knowledge exchange in both directions. Bringing an "outsider" from academia or the private sector into government is likely to provide a new perspective, knowledge base, and interpersonal network for the government and *vice versa*.[163] For example, the FTC, the agency perhaps most engaged with the private sector security research community, built its relationships into the private sector security community partially with the assistance of a visiting law professor[164] and visiting computer scientists.[165]

---

[160] *See, e.g.*, Steve Dent, *Meet the FTC's New Chief Technologist*, ENGADGET (Dec. 4, 2015), https://www.engadget.com/2015/12/04/lorrie-cranor-ftc-chief-technologist/ [https://perma.cc/ZMH4-YU3D].

[161] *See, e.g.*, *Technologist in Residence Program,* ENERGY.GOV, http://energy.gov/eere/cemi/technologist-residence-program [https://perma.cc/GLJ8-E4NR] (last visited Mar. 4, 2017) (describing the Department of Energy's Technologist in Residence program, which "pairs senior technical staff from national laboratories and manufacturing companies to work together towards long-term strategic collaborative partnerships and impactful manufacturing solutions.").

[162] Matwyshyn, *supra* note 23, at 1150-51.

[163] *See, e.g.*, PAULA JARZABKOWSKI ET AL., *Reviewing the State of Academic Practitioner Relationships*, *in* ACADEMIC–PRACTITIONER RELATIONSHIPS: DEVELOPMENTS, COMPLEXITIES AND OPPORTUNITIES 126, 132 (Jean M. Bartunek & Jane McKenzie eds., 2017).

[164] Kashmir Hill, *The FTC's Controversial Battle to Force Companies to Protect Your Data*, FORBES (Aug. 21, 2014), https://www.forbes.com/sites/kashmirhill/2014/08/21/the-ftcs-controversial-battle-to-force-companies-to-protect-your-data/ [https://perma.cc/SDV3-KQ8A] ("The FTC recently brought in Andrea Matwyshyn, an Internet security lawyer and law professor, who has been attending Defcon for a decade as a senior policy advisor. It was her idea to run the robocall contest at Defcon this year.").

[165] *See* Press Release, Federal Trade Commission, Federal Trade Commission Appoints Ashkan Soltani as Chief Technologist (Oct. 21, 2014), https://www.ftc.gov/news-events/press-releases/2014/10/federal-trade-commission-appoints-ashkan-soltani-chief [https://perma.cc/M2WT-APFB]; Press Release, Federal Trade Commission, FTC Names Latanya Sweeney as Chief Technologist; Andrea Matwyshyn as Policy Advisor (Nov. 18, 2013), https://www.ftc.gov/news-events/press-releases/2013/11/ftc-names-latanya-sweeney-chief-technologist-andrea-matwyshyn [https://perma.cc/PCD7-GZVR]; Carl Franzen, *FTC Appoints New Chief Technologist: Steve Bellovin*, TALKING POINTS MEMO, (Sept. 7, 2012),

c. The White House should execute an executive order requiring that all government organizations comply with the principles embodied in ISO standards on security, in particular the principles visible in ISO 30111 and 29147.

A key step in addressing the problem of reciprocal vulnerability involves creating shared baselines of conduct for both the public and private sectors – "floors" below which security conduct must not fall. While the optimal implementation of these baselines of security will vary across organizations and sectors, international standards exist in security. In particular, the International Standards Organization has released several security process standards that articulate baselines of security processes for any organization. Two ISO standards, 29147[166] and 30111,[167] set forth one set of floors for the private sector with respect to organizational structure and processes in responding to security vulnerabilities. The principles embodied by these two standards make sense for organizations in the public sector as well.[168] An executive order mandating compliance with the ideas embodied in these two standards would materially improve security inside some parts of government and assist in mitigating the problem of reciprocal security vulnerability in both the public and private sector.

ISO 29147 addresses basic processes related to an organization's *external* capabilities in vulnerability disclosure and receiving external reports.[169] It describes the goals of vulnerability disclosure as the following: "ensuring that identified vulnerabilities are addressed; minimizing the risk from vulnerability; providing users with sufficient information to evaluate risks from vulnerabilities to their systems; [and] setting expectations to promote positive communication coordination among involved parties."[170] Specifically, the scope of this

http://talkingpointsmemo.com/livewire/ftc-appoints-new-chief-technologist-steve-bellovin [https://perma.cc/QPB8-2Q89]; *see also* Press Release, Federal Trade Commission, FTC Names Edward W. Felten as Agency's Chief Technologist; Eileen Harrington as Executive Director (Nov. 4, 2010), https://www.ftc.gov/news-events/press-releases/2010/11/ftc-names-edward-w-felten-agencys-chief-technologist-eileen [https://perma.cc/E3K3-NRBG].

166 INT'L ORG. FOR STANDARDIZATION, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – VULNERABILITY DISCLOSURE, ISO/IEC 29147:2014 (2014) [hereinafter ISO 29147:2014].

167 INT'L ORG. FOR STANDARDIZATION, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – VULNERABILITY HANDLING PROCESSES, ISO/IEC 30111:2013 (2013) [hereinafter ISO 30111:2013].

168 Meanwhile, the courts are likely to begin to incorporate these baselines of conduct into tort determinations of liability, creating a harmonized approach across both the public and private sectors.

169 ISO 29147:2014, *supra* note 168, at 1.

170 *Id.* at v.

ISO standard provides guidelines for vendors on how to receive information from external finders about potential vulnerabilities in their products or online services.[171] It describes a five step process of receipt of vulnerability reports, verification, resolution development, release, and post release processes (which may involve cycling back to resolution development multiple times).[172] In particular, it highlights the importance of an overall vulnerability disclosure policy that includes basic information to enable vulnerability finders to contact the vendor efficiently and provide necessary information about the nature of the flaw.[173] It specifies that vendors should acknowledge receipt of all vulnerability reports within seven calendar days and coordinate with finders in order to be able to issue accurate advisories about the nature of the vulnerability.[174] In contrast, ISO 30111 provides an overview of *internal* vulnerability handling processes.[175] It stipulates that organizations should have a process and an organizational structure to conduct vulnerability investigations and remediation after an external report arrives.[176] Organizations should perform root cause analysis, meaning that they should determine the reason for the vulnerability[177] and not merely treat its symptoms. The process of handling vulnerabilities may also involve organizations' attempts to coordinate with others depending on the type of security vulnerability at issue.[178]

While it may not be appropriate to require that public sector organizations comply directly with ISO standards, the ideas and principles embodied in these international standards highlight the existence of consensus around the baselines of due care in security governance. The key elements described above for each of these two standards are relevant for public sector and private sector organizations alike and would assist in creating shared floors of conduct that benefit both sectors.

d. The Department of Justice should protect technical private sector feedback through security research by issuing advisory statements on CFAA enforcement and maintaining centralized CFAA indictment review, approval, and staffing.

Just as the legal uncertainty surrounding the DMCA has historically chilled security research, so too has the legal confusion with respect to the Computer Fraud and Abuse Act ("CFAA"). Enacted in 1986, "[t]he [CFAA] has long

171 *Id*. at 1.

172 *Id*. at 8.

173 *Id*. at 12.

174 *Id*.

175 *See generally* ISO 30111:2013, *supra* note 169.

176 *Id*.

177 *Id*.

178 *Id*.

been a source of consternation for jurists and legal scholars alike."[179] A statute marred by long-standing circuit splits over basic terminology and definitions, [180] the CFAA has strained under the weight of technological evolution. Legal scholarship has long voiced concerns over the CFAA, including whether certain provisions are void for vagueness,[181] create opportunity for abuse of prosecutorial discretion,[182] and give rise to unintended negative impacts on employee mobility and innovation.[183] After thousands of pages of law review ink spilt[184] on attempting to theoretically resuscitate this necessary but flawed statute, it is apparent that something more than a minor Congressional correction of the statute is required.[185]

The CFAA presents a more challenging legislative correction than the DMCA: it lacks the legal feedback loop of the exemption request process Congress provided in the DMCA.[186] While several attempts at legislative amendments have occurred[187] and additional attempts have been proposed,[188] they have not ended in successful correction of the CFAA's problems. Until such time as Congress amends the CFAA, the most immediate and promising path for a feedback loop to prevent the CFAA from harming security research, security information sharing, and digital entrepreneurship rests with the Department of Justice ("DOJ"). Through two voluntary public acts of prosecutorial

---

[179] Andrea Matwyshyn, *Starting with Consent*, J. THINGS WE LIKE (LOTS) (May 19, 2017), https://cyber.jotwell.com/starting-with-consent/ [https://perma.cc/Z5V3-8PAH] (reviewing James Grimmelmann, *Consenting to Computer Use*, 84 GEO. WASH. L. REV. 1500 (2016)).

[180] *See, e.g.*, Andrea M. Matwyshyn, *The Law of the Zebra*, 28 BERKELEY TECH. L.J. 155, 159 (2013) [hereinafter Matwyshyn, *The Law of the Zebra*].

[181] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1562 (2010).

[182] *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 HARV. L. REV. 751, 753 n.24 (2013) ("To whatever extent prosecutorial discretion might provide some redeeming amount of government participation in the criminal context, such participation is absent in civil cases between private parties.").

[183] Matwyshyn, *The Law of the Zebra*, *supra* note 182, at 177-78, 206.

[184] According to a Westlaw query under "CFAA," over 2,700 articles have been written referencing the CFAA.

[185] In particular, the central term of the statute – authorization – is not statutorily defined. As the CFAA has morphed through amendments to encompass not only criminal but also civil conduct, the meaning of "authorized access" has become progressively more slippery and difficult to anticipate.

[186] *See, e.g.*, SECTION 1201, *supra* note 122, at 20 (describing the triennial review process).

[187] *See, e.g.*, Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act,* 84 GEO. WASH. L. REV. 1442, 1443 (2016) (discussing the incremental statutory changes to the CFAA).

[188] *Id.* at 1444.

self-restraint, DOJ would materially improve the current uncertainty around CFAA interpretation and prosecution.

First, DOJ should publicly announce that until further notice, all CFAA prosecutions must obtain approval (not merely consultation) and staffing through main Justice. Although regional offices currently conduct CFAA prosecutions in consultation with the Computer Crime and Intellectual Property Section ("CCIPS"),[189] CCIPS attorneys are not always staffed on these local prosecutions and appear not to retain veto power in their handling.[190] Centralization of CFAA offenses within the control of CCIPS would limit the discretion of regional US Attorney's offices – traditionally the primary source of concern over overzealous CFAA prosecutions.[191] A structural shift of this sort would reflect DOJ's sensitivity to the uncertainty that permeates the security research community regarding uneven interpretation of the CFAA and particularly prosecutorial discretion on the local level.[192]

Second, just as DOJ regularly engages in antitrust enforcement policy statements[193] and Foreign Corrupt Practices Act guidance,[194] it could also issue

---

[189] *See, e.g.*, Memorandum from Office of the Att'y Gen. to the U.S. Att'ys and Assistant Att'y Gens. for the Crim. and Nat'l Sec. Divs. 6 (Sept. 11, 2014), https://www.justice.gov/criminal-ccips/file/904941/download [https://perma.cc/9G8M-VVSR].

[190] A recent prosecution of a security researcher credited with stopping the WannaCry malware has again raised concerns over local prosecutorial discretion. *See, e.g.*, Andy Greenberg, *Hacker Who Stopped WannaCry Charged with Writing Banking Malware*, WIRED (Aug. 3, 2017, 3:40 PM), https://www.wired.com/story/wannacry-malwaretech-arrest/.

[191] *See, e.g.*, Doug Lieb, *Vindicating Vindictiveness: Prosecutorial Discretion and Plea Bargaining, Past and Future,* 123 YALE L.J. 1014, 1016 (2014) (discussing concerns over prosecutorial discretion in computer intrusion cases).

[192] The prosecution of Aaron Swartz in particular raised questions for many observers regarding the appropriate balance between prosecutorial discretion and centralization of CFAA prosecutions. *See, e.g.*, Justin Peters, *A Year after Aaron Swartz's Death, our Terrible Computer Crime Laws Remain Unchanged*, SLATE (Jan. 13, 2014, 6:00 PM), http://www.slate.com/blogs/crime/2014/01/13/aaron_swartz_cfaa_a_year_after_aaron_swartz_s_death_the_computer_fraud_and.html [https://perma.cc/6ZZN-H6XE].

[193] *See, e.g.*, FED. TRADE COMM'N & U.S. DEP'T OF JUSTICE, STATEMENT OF ANTITRUST ENFORCEMENT POLICY REGARDING ACCOUNTABLE CARE ORGANIZATIONS PARTICIPATING IN THE MEDICARE SHARED SAVINGS PROGRAM (2011), https://www.justice.gov/sites/default/files/atr/legacy/2011/10/20/276458.pdf [https://perma.cc/BPN4-WS87]; U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, STATEMENTS OF ANTITRUST ENFORCEMENT POLICY IN HEALTH CARE (Aug. 1996), https://www.justice.gov/sites/default/files/atr/legacy/2007/08/15/1791.pdf [https://perma.cc/XY24-GF7E].

[194] *See, e.g.*, Eric W. Sitarchuck & Alison Tanchyk, *Department of Justice Quietly Revises Foreign Corrupt Practices Act Resource Guide*, NAT'L L. REV. (Aug. 5, 2015), http://www.natlawreview.com/article/department-justice-quietly-revises-foreign-corrupt-practices-act-resource-guide [https://perma.cc/G5UE-CJ7X].

advisory statements,[195] opinion procedure releases,[196] a resource manual,[197] investigation closure statements,[198] or create a notice filing regime similar perhaps in structure to the antitrust leniency program[199] in order to offer guidance on DOJ's interpretations of the CFAA.[200] Indeed, in 2014, DOJ entered into precisely this type of voluntary self-restraint statement jointly with the FTC in the context of security information sharing and antitrust.[201] Further, in 2017 DOJ issued a framework for vulnerability disclosure programs for online systems[202] providing advice on the basics of reasonable corporate response to reports of vulnerabilities and security compromise. These types of statements can be used by DOJ as the model for its own further CFAA and security-related advisories.[203] A series of CFAA advisory statements on the DOJ website[204]

---

[195] *See, e.g.,* STATEMENTS OF ANTITRUST ENFORCEMENT POLICY IN HEALTH CARE, *supra* note 194.

[196] Foreign Corrupt Practices Act Opinion Procedure Releases, U.S. DEP'T OF JUSTICE., https://www.justice.gov/criminal-fraud/opinion-procedure-releases [https://perma.cc/Y592-A6DU] (last visited Jan. 24, 2017).

[197] Sitarchuck & Tanchyk, *supra* note 195.

[198] Press Release, U.S. Dep't of Justice, Statement of the Department of Justice's Antitrust Division on Its Decision to Close Its Investigation of Highmark's Affiliation Agreement with West Penn Allegheny Health System (Apr. 10, 2012), https://www.justice.gov/opa/pr/statement-department-justice-s-antitrust-division-its-decision-close-its-investigation [https://perma.cc/EH6V-6C2V].

[199] *See* U.S. DEP'T OF JUSTICE, FREQUENTLY ASKED QUESTIONS ABOUT THE ANTITRUST DIVISION'S LENIENCY PROGRAM AND MODEL LENIENCY LETTERS (Jan. 26, 2017), https://www.justice.gov/atr/page/file/926521/download [https://perma.cc/Q395-P23U].

[200] Antitrust law and securities regulation present two somewhat parallel examples of regimes with broad statutes creating both civil and criminal recourse for aggrieved parties.

[201] U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, ANTITRUST POLICY STATEMENT ON SHARING OF CYBERSECURITY INFORMATION (2014), https://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcybertheatstmt.pdf [https://perma.cc/T5L5-9QSX].

[202] U.S. DEP'T OF JUSTICE, A FRAMEWORK FOR A VULNERABILITY DISCLOSURE PROGRAM FOR ONLINE SYSTEMS: VERSION 1.0 (2017), https://www.justice.gov/criminal-ccips/page/file/983996/download [https://perma.cc/GE9M-EAVY].

[203] For example, a recent noteworthy presentation by a DOJ CCIPS attorney at a leading security conference revealed that DOJ does not usually consider port scanning to rise to the level of a CFAA violation in most cases. This DOJ position was new, welcome information to the security researcher community. But, because it was shared in a venue with at most a few hundred people in attendance, this knowledge was, unfortunately, not widely disseminated in the legal community. Leonard Bailey, *Take a Hacker to Work Day: How Federal Prosecutors Use the CFAA*, YOUTUBE (Dec. 29, 2015), https://www.youtube.com/watch?v=IHm4KZsMtsU [https://perma.cc/QP72-DC4R].

[204] Although useful informal insights on DOJ's CFAA prosecutorial stance have begun to filter into the security research community through the (laudable) outreach work of individual DOJ attorneys, these information sharing mechanisms would benefit from formaliza-

would greatly assist the public and security researchers in trying to conform conduct to DOJ's current interpretations of the requirements of an unclear law. This change would create an important and currently absent feedback loop mechanism from DOJ on CFAA interpretation, giving Congress time to amend the troubled statute.

3. New Judicial Branch Feedback Loops

a. The Federal Judicial Center ("FJC") should create a roster of trusted technical experts on information security as a technical feedback loop to assist the federal judiciary.

In light of the pace of technological change in security, judges face a formidable challenge in staying abreast of technological developments that impact the cases over which they preside. Yet, judges may also be understandably wary of seeking technological advice and education from unvetted third parties. For this reason, an expansion of the offerings of the Federal Judicial Center offers a logical way to create an additional technical feedback mechanism for judges and their clerks.

The Federal Judicial Center[205] self-describes as "the research and education agency of the judicial branch of the United States Government."[206] Additional feedback loops for more directed and flexible technical exchanges would naturally fall within its mission. The FJC is a natural point of contact for judges and clerks looking for independent expertise in security. Specifically, the FJS with the help of computer science and legal academics should compile a roster of vetted technology experts, particularly security experts, to assist judges on an as-needed basis.

By creating a pre-vetted roster of technical experts available to consult with judges, the FJC would bridge this technology and security education gap for judges. The technical experts on the roster might fulfil two functions. First, they could offer judges and their clerks the opportunity for one-on-one tutorials when the specific functionality of particular technologies becomes relevant to the types of cases heard by the court. Particularly in the context of security, in-

tion. The DOJ website – a logical place for a citizen to search for the information – does not offer much direct guidance on current interpretations of the CFAA. *See* U.S. DEP'T OF JUSTICE, https://www.justice.gov/ [https://perma.cc/397K-89A7].

[205] The governing board of the FJC is composed of the Chief Justice of the United States, seven federal judges elected by the Judicial Conference of the United States, and the Director of the Administrative Office of the U.S. Courts. *See* FED. JUDICIAL CTR., https://www.fjc.gov/ [https://perma.cc/CA85-9NBS].

[206] *About the FJC*, FED. JUDICIAL CTR., https://www.fjc.gov/about [https://perma.cc/9BEB-P6GM]. The FJC runs interactive in-person programs, audio and video conferences, e-learning programs, instructional videos, podcast, publications, and discussion forums for judges and court staff. The goal of this curriculum is to provide the continuing legal education necessary for staff throughout the judiciary. *See id*.

dividualized interaction with technical security experts provides the most efficient method for answering factual technical questions. Second, in cases where a judge wishes to seek out a disinterested technical opinion, the roster might serve as a pre-vetted list of experts that the court could engage formally as a court-appointed expert.[207] An FJC roster of consulting information security experts would enable judges to obtain advice on their own schedule and enable security experts to donate their time in small amounts but with meaningful policy impact.

Also, these trusted security experts would be able to assist the FJC in drafting manuals, monographs, and guides and creating instructional videos and podcasts on technical matters of interest to the federal judiciary.[208] Specifically, FJC should create on-demand educational offerings on information security through its website. FJC already runs many educational conferences for judges with some content on technology topics,[209] but offerings in information security law and policy appear few or nonexistent.[210] To the extent any traditional education programs on information security may already exist, these are structured around a set schedule and destination, rather than a particular judge's availability.[211] These practical constraints limit the ability of judges and their clerks to attend because of time commitment and expense. In contrast, on-demand FJC offerings, such as instructional web videos and podcasts on information security issues, would offer an option with a high return on educational investment for both FJC and chambers.

b. The Administrative Office of the U.S. Courts should use redundancy as a security measure for PACER by permitting universities, libraries, and other approved parties to maintain to backup archives at their own expense.

[207] Court appointed experts are currently used in various legal contexts. In particular, in bankruptcy law, courts sometimes appoint a Privacy Ombudsman to assist the court in determining the appropriate disposition of databases of consumer information that are part of a corporate debtor's estate. *E.g.*, *Court Orders Privacy Ombudsman in Bankruptcy Case*, WINSTON & STRAWN (Aug. 14, 2014), https://www.winston.com/en/privacy-law-corner/court-orders-privacy-ombudsman-in-bankruptcy-case.html [https://perma.cc/Y93T-M9C3].

[208] For the current catalog of FJC publications see *Publications*, FED. JUDICIAL CTR., https://www.fjc.gov/publications [https://perma.cc/X5UE-XGSG].

[209] *Education Programs*, FED. JUDICIAL CTR., https://www.fjc.gov/education/education-programs [https://perma.cc/8XBP-WXUQ] (last visited Apr. 26, 2018).

[210] Currently, there are no information security educational materials readily available through the FJC website. *See Publications*, *supra* note 209.

[211] *See Programs and Resources for Judges*, FED. JUDICIAL CTR., https://www.fjc.gov/education/programs-and-resources-judges [https://perma.cc/7M5C-BMBN] (last visited Apr. 26, 2018). Judicial schedules are not always flexible enough to attend conferences in other cities, and judges may have precise technical questions.

The Administrative Office of the U.S. Courts currently administers Public Access to Court Electronic Records (PACER) – "an electronic public access service that allows users to obtain case and docket information online from federal appellate, district, and bankruptcy courts"[212] — and the Office has struggled to maintain the service in a technically-robust and cost-effective manner.[213] Indeed, PACER at one point made some older cases unavailable, though ultimately restoring access[214] due to public outcry.[215] By permitting universities, libraries, and other approved parties to maintain backup archives of PACER at their own expense, the Administrative Office of the U.S. Courts would create a security and efficiency win-win. Redundancy of information and networks is widely recognized as a defensive security strategy against data corruption,[216] malicious attack or catastrophic hardware failure. In much the same way that consumers defend against hardware failures of their laptops by backing up to an external drive or to "the cloud," PACER's allowing trusted third parties to maintain redundant copies of the corpus of court filings and decisions offers a useful buffer in case of catastrophic failure or system compromise.

Also, multiple third-party subsidized copies of PACER documents would offer more cost-effective access to legal filings – an essential feedback loop for both the public and private sectors. Because of the speed of legal evolution in information security, the inability to afford PACER access creates information 'haves' and 'have nots.' PACER rates[217] are currently cost-prohibitive for most members of the public[218] and even many attorneys, both inside and outside the government. For example, computer science students and faculty, have resort-

[212] PUBLIC ACCESS TO COURT ELECTRONIC RECORDS (PACER), https://www.pacer.gov/ [https://perma.cc/67Z8-SWST], (last visited July 22, 2018).

[213] *Everything Wrong with PACER,* AM. LEGALNET (Mar. 2, 2017), http://www.alncorp.com/everything-wrong-with-pacer/ [https://perma.cc/47D2-L4JL].

[214] *Restoration of Electronic Access to Legacy Case Information*, PACER, https://www.pacer.gov/announcements/general/webpacer.html [https://perma.cc/GX2R-PPGL] (last visited Mar. 4, 2017).

[215] Mike Masnick, *PACER Deleting Old Cases; Time to Fix PACER*, TECHDIRT (Aug. 25, 2014), https://www.techdirt.com/articles/20140821/07015128275/pacer-deleting-old-cases-time-to-fix-pacer.shtml [https://perma.cc/D9BY-VP6B].

[216] Bev Littlewood & Lorenzo Strigini, *Redundancy and Diversity in Security*, *in* COMPUTER SECURITY – ESORICS 2004, at 423 (Pierangela Samarati et al. eds., 2004).

[217] *See Electronic Public Access Fee Schedule,* PACER (Dec. 1, 2013), https://www.pacer.gov/documents/epa_feesched.pdf [https://perma.cc/F2CG-PYCV].

[218] David Greene, *Opportunity Missed: Why We're Not Thrilled by Restoration of PACER Access to "Old" Court Records*, ELEC. FRONTIER FOUND. (Sep. 19, 2014), https://www.eff.org/deeplinks/2014/09/opportunity-missed-why-were-not-thrilled-restoration-pacer-access-certain-court [https://perma.cc/2W86-PX5V].

ed to hit-or-miss self-help remedies[219] because of the prohibitive expense of using PACER. In particular, for security researchers and computer science students, the inability to review recent computer intrusion indictments and pleadings places them at additional risk of running afoul of the CFAA. They see media reports of a regular stream of civil suits or indictments, but they lack access to the legal information they need to be certain that their technical conduct conforms to the evolving state of the law. Thus, in addition to the new backup archives' providing security redundancy, they would also assist in providing more cost-effective access to indictments, cases, and other filings as a feedback loop on the law of information security. This additional access would benefit not only attorneys counseling clients, both inside and outside the government, but also individual members of the public, such as students or small business owners who wish to understand the law impacting them.

Pragmatically, permitting backup copies would also perhaps help the Administrative Office of the U.S. Courts extricate itself from the currently pending class action litigation over the (in)appropriateness of PACER fees.[220] Privately-hosted backup copies of PACER in the hands of trusted third parties may also make similar class actions less likely in the future: multiple sources for obtaining the same information would exist.

While these PACER improvements would assist legal security knowledge dispersal, the second piece of a successful security vigilance infrastructure involves technical knowledge dispersal. The creation and improvement of security structures for improved technical information dispersal is also a necessary prerequisite to meaningful information sharing on security.

B. Proposal 2: Improve security disclosure infrastructure across both the public and private sector to allow for meaningful progress tracking.[221]

Three improvements to security disclosure structures would swiftly improve security vigilance infrastructure – updating vulnerability tracking, creating a uniform security advisory notice structure, and creating a uniform data breach notification form and central data breach notification repository. In all three cases, cooperation among State Attorneys General, the National Conference of Commissioners on Uniform State Laws ("NCCUSL"), and technical experts will yield the next steps toward improvement.

1. Update current structures around security vulnerability tracking and make them usable to consumers.

---

[219] *See, e.g.*, *RECAP Project – Turning PACER Around*, FREE LAW PROJECT, https://free.law/recap/ [https://perma.cc/2EPY-KKNR] (last visited Mar. 4, 2017).

[220] Nat'l Veterans Legal Servs. Program v. United States, 235 F. Supp. 3d 32 (D.D.C. 2017).

[221] Matwyshyn, *supra* note 23, at 1190.

Security vulnerabilities are currently indexed by the MITRE Corporation through the CVE system.[222] The Common Vulnerability and Exposures ("CVE") number is a unique identifier that assists in indexing and tracking particular vulnerabilities.[223] CVE numbers can be assigned in multiple ways – by MITRE itself or by certain approved entities who request a block of numbers and allocate them as needed.[224] Each vulnerability also generally receives a score of severity – a CVSS score.[225] However, the current structure suffers from several limitations, and MITRE has historically struggled to keep up with the volume of vulnerabilities.[226] Most recently the increased volume generated by the Internet of Things has strained existing vulnerability indexing structures.[227]

Although updating indexing structures and severity ratings is best left to the technical experts with respect to the substance of scoring, the current structures of vulnerability indexing are not scaling effectively and are completely opaque to most consumers and companies new to security. For these reasons, a coalition of state attorneys general[228] might convene a working group in conjunction with vulnerability indexing and database experts – a small but highly engaged community. This working group would have two goals. First, this working group would ask those technical experts to envision a more functional indexing structure and to assist them in its smooth implementation as needed. Second, the working group would cooperate to improve information accessibility and create a consumer-usable version of this vulnerability information. This new consumer-usable vulnerability database would be hosted on websites of state attorneys general and built in such a way as to allow consumers to type in the products they use and monitor their exposure to vulnerabilities. While

---

[222] *See, e.g.*, *CVE List Home*, CVE, https://cve.mitre.org/cve/ [https://perma.cc/FDJ2-YWMB] (last visited Feb. 22, 2017); *but see, e.g.*, Steve Ragan, *Over 6,000 Vulnerabilities Went Unassigned by MITRE's CVE Project in 2015*, CSO (Sept. 22, 2016, 4:00 AM), https://www.csoonline.com/article/3122460/techology-business/over-6000-vulnerabilities-went-unassigned-by-mitres-cve-project-in-2015.html [https://perma.cc/7VPA-LXDT].

[223] CVE, https://cve.mitre.org/about/index.html [https://perma.cc/X6PK-539W] (last visited Feb. 22, 2017).

[224] Ragan, *supra* note 223.

[225] *Id*. While the current CVSS scoring system has evolved over time, it been critiqued for overvaluing some types of flaws and undervaluing others. Nevertheless, a CVSS score provides a usable metric for the severity of a vulnerability on a scale up to ten (where ten is most severe). *See* Stephanie K. Pell & James Finocchiaro, *The Ethical Imperative for a Vulnerability Equities Process and How the Common Vulnerability Scoring System Can Aid That Process*, 49 CONN. L. REV. 1549, 1565 (2017).

[226] *See Id*.

[227] Ragan, *supra* note 223.

[228] It is also possible that a federal agency such as the Department of Homeland Security or the Federal Trade Commission could convene this group and host the resulting consumer-facing database.

this type of website will still be too complicated for many consumers to understand, it would reflect a valuable step toward bridging a knowledge gap among the vulnerability indexing community, enforcers, and consumers.

2. Create uniformity in security advisories and improve their accuracy

Prudent companies seek to preserve customer goodwill and reputation through issuing timely security advisories – software safety warnings – when vulnerabilities are discovered in their code.[229] However, leading vulnerability database managers have noted that these advisories vary substantially in quality, accuracy, and timeliness.[230] Consequently, the ability to aggregate data, analyze vulnerability trends, and track security progress in particular products is substantially hampered. In other words, the success of information sharing is limited by the quality and comprehensibility of the information shared: important categories of security data analytics cannot be performed currently due to the low quality of data available in some companies' security advisories.

The same working group of state attorneys general and vulnerability database experts who collaborate on the point of scaling CVE should also cooperate with NCCUSL to create a uniform technical security advisory disclosure form.[231] Provided that such a form is widely adopted, meaningful analysis of vulnerability information and trends would be dramatically improved and facilitated.

Similarly, this new uniform security advisory form should offer a summary in plain English to assist consumers (and attorneys) in better understanding the importance of particular security advisories and which code requires patching. Particularly when time is of the essence in responding to the most serious security vulnerabilities, more comprehensible security advisories would materially assist in improving security in both the public and private sectors. The exist-

[229] *See, e.g.*, *Cisco Issues New Patches For Critical Firewall Software Vulnerability*, THREATPOST (Feb. 6, 2018, 10:34 AM), https://threatpost.com/cisco-issues-new-patches-for-critical-firewall-software-vulnerability/129793/ [https://perma.cc/Z5ZG-SMJP]; *Oracle Issues 'Massive' Security Update*, FORTUNE (Jan. 20, 2017), http://fortune.com/2017/01/20/oracle-massive-security-update/ [https://perma.cc/4K6C-XE2W]. Security advisories may also be triggered by vulnerabilities in libraries or other incorporated code used in a product's code base. See e.g., THE HEARTBLEED BUG, http://heartbleed.com/ [https://perma.cc/99JH-TEDT] (last visited July 22, 2018) ("The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library.").

[230] STEVE CHRISTEY & BRIAN MARTIN, BUYING INTO THE BIAS: WHY VULNERABILITY STATISTICS SUCK (July 11, 2013), https://media.blackhat.com/us-13/US-13-Martin-Buying-Into-The-Bias-Why-Vulnerability-Statistics-Suck-Slides.pdf [https://perma.cc/M8TU-RJ5M].

[231] This form should include elements such as those listed on Appendix A to ISO 29147 A-3.

ence of a legally-suggested form would also add gravitas to the security advisory process inside companies, helping security teams to obtain adequate corporate budget and encouraging general counsel to verify the accuracy of the information being publicly disclosed. A centralized database of security advisory notices should also be created and maintained by (any or all) state attorneys general.[232]

Meanwhile, fraudulent, misleading, or grossly negligent information on these uniform advisories can, in turn, provide subsequent basis for suit or enforcement activity. States can mandate the use of the form through, for example, amending their data breach notification statutes accordingly or through interpreting their "Little FTC Acts" relating to unfair trade practices to mandate use of the form. This improved information stream will, in turn, pave the way for increased state level security enforcement.

3. Create uniformity in data breach notification and the option of a single point of public filing, while respecting states' rights to vary regarding enforcement

Data breach compliance personnel in the private sector consistently voice frustrations regarding two elements of state data breach notification requirements - variation across required formats for disclosure and variation in the correct point of state level regulator notification.[233] In essence, a situation parallel to the historic inefficiencies created by state securities regulation blue sky laws has emerged. Just as many states have agreed to recognize a standardized notice filing in form specified by the SEC[234] to comply with their blue sky law notification requirements, so too many states would undoubtedly be willing to accept a uniform data breach notification filing in a form specified by a coalition of state attorneys general or NCCUSL. A single point of shared filing across voluntarily cooperating states is also possible.

---

[232] A centralized, public filing database indexing these security advisory forms will assist both corporate security teams and attorneys with models of how to adequately fill out the necessary details of a security advisory. The system would also automatically archive a copy to allow for government and private sector customers to be alerted of the need to patch their systems, and users of the database could sign up to receive alerts notifying them when products or services they use have been impacted by a need for a security update.

[233] *See Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?: Hearing Before the Subcomm. on Commerce, Mfg., and Trade of the H. Comm. on Energy and Commerce*, 113th Cong. 45 (2013) (statement of Dr. Andrea M. Matwyshyn, Assistant Professor of Legal Studies and Business Ethics, on behalf of The Wharton School, University of Pennsylvania).

[234] SEC. & EXCH. COMM'N, *Filing and Amending a Form D Notice*, https://www.sec.gov/info/smallbus/secg/formdguide.htm [https://perma.cc/4W65-RXY2] (last updated Aug. 4, 2017) ("Many states also require the filing of Form D notices and amendments . . . .").

Thus, a standardized format for data breach notification filings can be drafted by the working group of NCCUSL,[235] State Attorneys General, and vulnerability indexing experts to generate a suggested default breach notification form. This new uniform data breach notification form should contain a clear explanation of the technical elements currently articulated in state level data breach notification statutes, expanded to include additional information that will assist in tracking security progress.[236] Specifically, a uniform data breach notification disclosure should contain at least the following categories of information:

- Date of start of breach (if known)
- Length and extent of intrusion
- Date of detection
- Name and contact information of the forensic investigator/head of incident response
- Date of consumer notification
- Total number of records impacted
- Total number of consumers impacted
- States of residency of impacted consumers and the number of records per state
- Manner of notice provided to consumers (written, electronic, telephone, other)
- Services offered to impacted consumers
- Type of attack/ technical description of breach (third-party intrusion, inadvertent disclosure, stolen or lost hardware, insider wrongdoing, other)
- Presence of encryption and identification of the version of software used
- Description of compromised information
- Root cause of breach
- Description of completed or planned improvements to information security in response to the breach
- Name and contact information for a designated individual at the company to answer consumer questions

[235] *See, e.g.*, *About the ULC*, UNIFORM LAW COMMISSION, http://www.uniformlaws.org/Narrative.aspx?title=About%20the%20ULC [https://perma.cc/GB3F-46M7] (last visited Mar. 4, 2017).

[236] These disclosures should be written in plain English. Plain English initiatives exist in other bodies of law, perhaps most notably in securities regulation. *See Plain Writing Initiative*, SEC. & EXCHANGE COMMISSION, https://www.sec.gov/plainwriting.shtml [https://perma.cc/USX2-37MM] (last updated Apr. 13, 2016).

- Dates of previous breach notifications in the last ten years

Provided the form is adequately robust, states can agree to accept this form in lieu of their current statutory disclosure requirements. Any state that accepts the form can then create a digital repository of all such forms, allowing citizens to search for information about the frequency of data breaches at particular companies with which they do business.[237]

This type of technology solution would offer a win-win-win scenario for industry, consumers, and regulators. It would streamline notification for companies and materially improve speed of getting information about data breaches into the hands of consumers and regulators – a situation where time is of the essence in protecting consumers from information criminals.

Because these uniform data breach notification forms would be archived by the repository, data breach notifications would become centralized and searchable. Thus, consumers would be able to access and review them whenever they wish. The repository could even offer personalized notification alerts to consumers where the consumer preemptively requests email notifications of any future data breach filings for particular companies. In this way, jurisdictional variation in the quality and speed of breach notification will be offset through improved internet availability to the public. Similarly, journalists, security experts, and consumer advocates will be able to better analyze breach severity and impact in historical context, even before breach notifications arrive in the mail in some states. Indeed, the regulatory purpose for data breach notification statutes – advising consumers of the existence of a breach– would be buttressed under this proposed approach.

Through the creation of a uniform breach form and a public, searchable breach notification database maintained by state attorneys general, the two concerns of data breach compliance personnel -- variation across required formats for disclosure and variation in the correct point of state level regulator notification -- would also be improved. The proposed approach would ask data breach compliance personnel to complete a single, thorough notification form, which could then be shared with individual state regulators in either automated or manual fashion. Depending on the degree of voluntary cooperation from state regulators, the compromised entity would need to engage in fewer regulatory filings (in addition to statutorily-required direct consumer notification). The result would yield a dramatically streamlined and more cost-effective process that many companies will appreciate. Similarly, state and national data security enforcers would have a useful, single point of information acquisition, receiving access to breach information potentially more quickly and thoroughly than their own state law requires.[238]

---

[237] Federal agencies that suffer data breaches should lead by example by using the model form and making their data breach notification disclosures available on their websites.

[238] In fact, because of higher quality, faster information for some participating state regulators than their current state's regimes offer, state data security enforcers may realize im-

State data breach notification statutes and state level data security enforcement authority would remain identical under this proposed approach. State adoption of either or both of the new standardized security advisory and data breach notification forms would be entirely voluntary. A centralized form repository and the notification engine could similarly, in state regulators' discretion, either push information at users incrementally or allow them to login and pull information about new security advisories and breach notifications whenever they wish. Thus, even if not all states accept the standardized form or host a data breach notification centralized filings repository, *any* state doing so with a public website would offer improved access to high-quality security information for consumers and enforcers. Similarly, even if only a portion of states accept the standardized form and host a breach notification internet repository, companies will experience efficiencies in filing, and consumers across jurisdictions will more readily get access to security advisory and breach information.[239]

IV. RECIPROCAL SECURITY: DEFENSE PRIMACY

Having introduced the proposals aimed at building an information security vigilance infrastructure, we now turn to three proposals that aim to bolster defense primacy. These proposals involve defending supply chains, defending entrepreneurship, and defending market integrity. They similarly each mitigate the problem of reciprocal security vulnerability.

C. Proposal 3: Defending supply chains to improve integrity.[240]

Persistent vulnerability in both the public and private sector sometimes arises because organizations fail to keep track of the software and hardware prod-

provements in their ability to efficiently make decisions regarding which breaches warrant enforcement using published data from other states' use of the new standard forms.

[239] Another path would involve a federal agency such as the FTC creating a centralized repository and point of filing. However, federally streamlining data breach notification should not preempt states' rights to regulate information security conduct - both with respect to sanctions for a failure to disclose or correctly notify consumers and with respect to inadequacy of information security measures. Limiting states' rights to impose liability in tort or through regulatory action for information security misconduct will further erode consumer trust and damage innovation in the United States. Similarly, any federal limitation of liability for unreasonable information security conduct would actively damage the attempts of regulatory agencies to stimulate security improvements within the scope of their respective missions. Currently, the best course of action with respect to liability is one exercising deference to federalism concerns and states' regulatory interests in redressing the harms of their citizens for information security harms. Different states engage with consumer protection questions in different ways, and no national consensus currently exists with respect to the best course of action for information security liability imposition.

[240] Matwyshyn, *supra* note 23, at 1192.

ucts they use (and the components included in those products).[241] Consequently, they fail to monitor adequately for the security vulnerabilities that directly impact them.[242] For example, software and hardware products often rely on incorporated code libraries[243] and internal components manufactured by third parties.[244] If one of those libraries or components is found to have a serious vulnerability, every product a company builds or uses that relies on that code library or component is also vulnerable. However, without being aware of the software and hardware within each product, an organization may not even realize it needs to patch or needs to supervise a third party in patching.

In the public sector, either through Congressional action[245] or a presidential executive order, the Office of Management and Budget should institute the creation of a binding legal obligation on all government organizations to conduct an annual internal government organization assessment of these "supply chain" vulnerabilities for all products and services purchased by the government.[246] Vendors that fail to patch on a timely basis,[247] have demonstrated a

---

[241] *See* Andrea M. Matwyshyn, *The Big Security Mistakes Companies Make When Buying Tech*, WALL ST. J. (Mar. 13, 2017), https://www.wsj.com/articles/the-big-security-mistakes-companies-make-when-buying-tech-1489372011.

[242] *Id*.

[243] A library is a collection of precompiled routines that a program can use. *See, e.g.*, Vangie Beal, *Library*, WEBOPEDIA, https://www.webopedia.com/TERM/L/library.html [https://perma.cc/C2HG-US5B] (last visited Mar. 31, 2018). For example, Heartbleed impacted the OpenSSL library. THE HEARTBLEED BUG, *supra* note 230 (the "weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).").

[244] Consider, for example, Mirai botnet - a botnet of remotely control devices that recently overwhelmed several of the most popular websites on the Internet and made them inaccessible through a distributed denial of service attack. This botnet of Internet of things devices such as DVR's and home webcams came into existence because of shared vulnerable components in each of these devices. In order to be able to quickly determine whether particular software or devices are vulnerable to a new vulnerability or attack, consumers and organizations must be able understand what code and components exist within that device. Mirai's severity and success was partially rooted in an information deficit regarding which devices were vulnerable to compromise. *See e.g.*, Manos Antonakakis et al., *Understanding the Mirai Botnet*, RESEARCH AT GOOGLE, https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/46301.pdf [https://perma.cc/EH6N-QBBU].

[245] One such bill, the Cyber Supply Chain Management and Transparency Act of 2014, has been introduced in a past Congressional session. H.R. 5793, 113th Cong. (2014).

[246] Open source products in particular present security challenges. *See, e.g.*, Dan Geer & Joshua Corman, *Almost Too Big to Fail*, 39 USENIX 66, 68 (2014) ("In closed source development domains, the command structure will know who uses what and can thus ascertain what code trees have to be rippled when a common component is revised. This is not the case with open source, nor will it be. . . . The more widespread the use of a particular open

lack of responsiveness to external reports of security concerns or otherwise fail to comport with recognized standards of care in security,[248] should be blacklisted from procurement vendor lists. Because of the purchasing power of U.S. government, this approach that combines reporting requirements[249] and blacklists would trigger significant security improvements in supply chain integrity in both the public and private sectors. Through these supply chain audits, OMB and GAO may be able to acquire enough data to create an annually-updated "preferred government provider" list based on these reports regarding the quality of vendor information security conduct. Finally, OMB and/or GAO should draft a report card on security health of government organizations' supply chains, expanding on the existing security assessments performed by GAO.

In the private sector, this type of oversight should be performed by the board of directors of each organization. In particular, with respect to all subsequent new purchases, both government organizations and private entities should ensure that all agreements with vendors include contractual provisions with robust remedies for security failures and audit rights. Specifically, the failure to provide, accurate security reporting data or failure to maintain substantiated and robust security standards should constitute a material breach by a vendor under the contract, creating an immediate right of exit for the other party. This contract breach should also trigger the addition of the vendor to a blacklist for future contracts. Demands for security improvements from public companies will create network effects of security improvements in their vendors' conduct,[250] as do the purchasing requirements of the U.S. government.[251] Hence,

source library, the more common mode failure among otherwise unrelated product spaces becomes.").

[247] Vendors should update their reports on a quarterly basis and at the time of any new product purchase. On the basis of these aggregated reports, government organizations can be tracked in their security improvements and held responsible for buying less vulnerable products over more vulnerable products.

[248] For example, this noncompliance may include failing to adhere to the types of elements identified by ISO 29147 and 30111 and NIST standards deemed on point.

[249] This annual review might consist of providing OMB and GAO information on the state of its supply chain security, confidentially disclosing the fully aggregated list of all code in use inside its organization (both third party custom products and regular commercial/consumer products), its known flaws, patching history, results of third-party security audits, and future expected security risks in products currently in use. In particular, all organizations should be required to disclose whether any code in use is currently unsupported or projected to be unsupported in the next 5 years. The CISO of each organization should personally certify the truth of the report, modeling the verification requirements after those under the Sarbanes-Oxley Act with respect to personal certification of financial statements. *See* Sarbanes Oxley Act of 2002 § 302, 15 U.S.C. § 7241 (2012).

[250] Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 161 (2005).

[251] Matwyshyn, *supra* note 23, at 1192.

this supply chain security monitoring would stimulate significant improvements in supply chain integrity in both the private and public sector.

D. Proposal 4: Defending entrepreneurship with security tax incentives and tools.[252]

Cash-strapped startups and consumers often face challenges in learning about and implementing security.[253] Yet, their vulnerable products may be the most likely candidates for becoming harnessed into a botnet,[254] potentially attacking critical infrastructure or healthcare[255] targets. Two strategies may assist in helping to translate the importance of security to these less knowledgeable populations – tax incentives for startups and more accessible security tools.

1. Create federal and state security upgrade tax incentives for entrepreneurs.

Security investment tax incentives[256] for entrepreneurs would nudge material security improvements[257] in much the same way tax incentives were used to nudge environmental improvements.[258] Congress should instruct the Depart-

[252] *Id*. at 1193.

[253] For a discussion of startups and security see Luis A. Aguilar, *The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses*, U.S. SEC. & EXCHANGE COMMISSION (Oct. 19, 2015), https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html [https://perma.cc/R9PG-UCEB].

[254] For a discussion of botnets and security risks, see *Botnets*, F-SECURE, https://www.f-secure.com/en/web/labs_global/botnets [https://perma.cc/YM2B-R9CN] (last visited Mar. 31, 2018).

[255] Hospitals currently face a ransomware problem, and threats of targeting from botnet operators are likely the next round of attack. *See, e.g.*, *12 Healthcare Ransomware Attacks of 2016*, BECKER'S HEALTH IT & CIO REPORT (Dec. 29, 2016), http://www.beckershospitalreview.com/healthcare-information-technology/12-healthcare-ransomware-attacks-of-2016.html [https://perma.cc/P4VF-UTNT].

[256] *See* Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 416 (2016) ("The government could provide companies with a tax credit for investments in qualified cybersecurity expenditures up to a certain annual amount.").

[257] For a discussion of the potential of tax incentives to nudge corporate and consumer behavior, see Shlomo Benartzi et al., *Governments are Trying to Nudge us Into Better Behavior. Is it Working?,* WASH. POST (Aug. 11, 2017), https://www.washingtonpost.com/news/wonk/wp/2017/08/11/governments-are-trying-to-nudge-us-into-better-behavior-is-it-working/?utm_term=.8d8c3f0f2e93 [https://perma.cc/4G69-7FS6].

[258] *See, e.g.*, Allison Casey, *Energy Efficiency Tax Credits, Rebates, and Financing: What Options are Available for You?,* ENERGY.GOV (Mar. 23, 2015),

ment of Commerce and the Internal Revenue Service to construct a tax incentive structure aimed at providing phased-out tax credits to small businesses who wish to invest in their information security through hiring additional staff, obtaining training or purchasing security services.[259]

Small businesses present one of the most vulnerable sectors of our economy, particularly in the age of the Internet of Things.[260] Operating on shoe-string budgets and often lacking in-house security expertise, most small businesses face significant security challenges and the fewest resources to identify and address them.[261] Yet, small businesses are the often the ventures building some of the most sensitive internet-connected consumer gadgets – gadgets such as internet-connected baby monitors.[262] These types of consumer product startups are arguably most in need of robust security audit in light of their products' propensity to cause harms, both to individual consumers and to national security.

Consider the Mirai botnet, a remotely-controlled malicious aggregation of consumer Internet of Things devices.[263] While each individual device allowed for the remote compromise of the home network to which it was attached, the greater harm arose from the combined computing power of all of these compromised devices working as a single attacking force.[264] The compromised Internet of Things devices harnessed in the Mirai botnet engaged in a successful distributed denial of service attack against Twitter, Reddit, and other popular websites.[265] While, in this instance, damaging the availability of these websites primarily caused inconvenience to consumers and lost revenue for the impacted websites, a parallel attack might target critical infrastructure or healthcare targets, resulting in loss of life and physical harm to impacted consumers. Even if only a portion of the companies currently manufacturing vulnerable Internet of Things devices improve their security practices as a result of a tax incentive, a significant aggregate risk mitigation for national security results.

---

https://www.energy.gov/articles/energy-efficiency-tax-credits-rebates-and-financing-what-options-are-available-you [https://perma.cc/DV6C-VNRF].

259 *See* Kosseff, *supra* note 257.

260 Matwyshyn, *supra* note 242.

261 *Id.*

262 *See generally* MARK STANISLAV & TOD BEARDSLEY, HACKING IOT: A CASE STUDY ON BABY MONITOR EXPOSURES AND VULNERABILITIES (2015), https://information.rapid7.com/iot-baby-monitor-research.html [https://perma.cc/ZZ49-WCC9].

263 Graff, *supra* note 18.

264 *Id.*

265 Robinson Meyer, *How a Bunch of Hacked DVR Machines Took Down Twitter and Reddit*, THE ATLANTIC (Oct 21, 2016), https://www.theatlantic.com/technology/archive/2016/10/how-a-bunch-of-hacked-dvr-machines-took-down-twitter-and-reddit/505073/ [https://perma.cc/MK2G-Q6ET].

To wit, improving security in Internet of Things devices should constitute both a private sector and national security priority. Security tax incentives for entrepreneurial ventures offer the potential for substantially improving security in our economy in the short term. Specifically, the IRS might propose a series of tax incentives to assist small businesses in affording access to security consultants, part-time CISOs, penetration testers and other security professionals. A phased out program across the first five to ten years of a company's life would allow for security basics to take root in the culture of companies, building a culture with security by design and not as an afterthought.

2. Build new consumer, entrepreneur, and government security tools through contests.

As a recent Hewlett Foundation report explained, we suffer from a shortage of security "translators" – experts who can bridge the technical and policy questions.[266] The same type of problem exists in bridging the divide between highly technical solutions (that require baselines of security knowledge and technical skill to implement) and the technical abilities of most entrepreneurs, government decision makers, and consumers. As a consequence, one missing piece of security policy involves the creation of accessible technical tools to bridge this gap.

One potential strategy may be to sponsor the creation of consumer-usable tools through federal contests. Agencies have already demonstrated the success of the America Competes Act as renewed,[267] as a way to use contests to build security solutions and stimulate security entrepreneurship.[268] The FTC has successfully used contests on multiple occasions to build tools to combat unwanted robocallers.[269] DARPA similarly recently used this contest structure to run a "Cyber Grand Challenge" where it asked participants to build an artificially intelligent security system and then to compete against each other in real time,

[266] Michael J. Gaynor, *Why the U.S. Needs More Cyber Translators,* HEWLETT FOUND. (Mar. 12, 2018), https://www.hewlett.org/u-s-needs-cyber-translators/ [https://perma.cc/TFX7-P7SR].

[267] American Innovation and Competitiveness Act, Pub. L. No. 114-329, 130 Stat. 2969 (2017) (renewing, in substantial part, repealed America COMPETES Act, H.R. 2272, 110th Cong. (2007)).

[268] *See generally* Stuart Minor Benjamin & Arti K. Rai, *Fixing Innovation Policy: A Structural Perspective,* 77 GEO. WASH. L. REV. 1, 5 (2008) (explaining the provisions of the America COMPETES Act and its impact on innovation); Sapna Kumar, *The Other Patent Agency: Congressional Regulation of the ITC,* 61 FLA. L. REV. 529, 578 (2009) (questioning Congressional commitment to the America COMPETES Act in light of under-appropriation); Roberta Romano, *Does the Sarbanes-Oxley Act Have a Future?*, 26 YALE J. ON REG. 229, 276 (2009) (discussing the relationship of the America COMPETES Act and Sarbanes-Oxley).

[269] *See, e.g.*, *DetectaRobo*, FED. TRADE COMMISSION, https://www.ftc.gov/news-events/contests/detectarobo [https://perma.cc/AX24-APPR].

attacking and defending.[270] This type of contest approach can be dramatically expanded by other agencies to stimulate security entrepreneurship and accessible consumer security tools.

In essence, this security contest approach reflects a constructive use of gamification to advance security.[271] The idea of gamifying security is not new. For example, bug bounty programs have essentially gamified the process of obtaining third-party security audit of products and services in a structured way. Indeed, while "dogfooding" – the process of a company using its own technology internally with the help of "friends and family" – has long been a common testing process, the security community has pioneered a gamified, more robust model of audit – one that might be called "catfooding." Catfooding involves putting out incentives for participation to anyone who possesses the skills to engage with the challenge, much the way someone might leave a plate of food out on the patio for any cat in the neighborhood who happened to be passing by to consume. This "catfooding" model of security is arguably the zeitgeist underlying both bug bounty programs and the spirit embodied by the America Competes Act, as renewed. Thus, every agency that qualifies under the America Competes Act structures should create appropriate security contest opportunities in line with its mission, stimulating the creation of new, accessible consumer and small business security tools.

E. Proposal 5: Defending Market Integrity

In addition to the proposed defense primacy measures described in the previous sections, a necessary component of ensuring a baseline of security across sectors involves more rigorous enforcement – both by the relevant regulatory agencies and by organizations themselves. Without more rigorous enforcement, our markets cannot effectively reward companies who deserve consumer trust because of their strong security practices.

1. Federal and state regulators should vet security statements in regulatory filings and advertisements for accuracy.

---

[270] *See, e.g.*, *The World's First All-Machine Hacking Tournament*, CYBER GRAND-CHALLENGE, http://archive.darpa.mil/cybergrandchallenge/ [https://perma.cc/J46S-6TZB] (last visited Mar. 31, 2018).

[271] The law review literature has discussed the ways that "gamification" has changed the dynamics of various business fields. *See generally* Julie E. Cohen, *The Zombie First Amendment,* 56 WM. & MARY L. REV. 1119, 1141 (2015) (discussing gamification and brand messaging); Frank Pasquale, *Redescribing Health Privacy: The Importance of Information Policy,* 14 HOUS. J. HEALTH L. & POL'Y 95, 116 (2014) (discussing health data and gamification); Nicolas P. Terry, *Will the Internet of Things Transform Healthcare?*, 19 VAND. J. ENT. & TECH. L. 327, 336 (2016) (discussing gamification in healthcare).

Defense primacy also involves facilitating market mechanisms through consumer protection on questions of security. Because different agencies have different missions and enforcement capabilities, a set of bilateral interagency enforcement taskforces should be created to coordinate security enforcement. These sets of task forces should include representatives from DHS, FTC, SEC, DOJ, FDA, CFPB, FCC, and any other agency interested in participating in coordinated enforcement. Cases involving private sector security deficits would be "claimed" for enforcement by the agency in the pair best situated to engage in enforcement due to its mission and authority or enforcement might be joint. The task forces' dockets should include enforcement against entities who fail to fix known security flaws, provide inadequate security advisories, violate open source licenses' security terms, and make false or unsubstantiated claims of security in their products or operations.

For example, the FTC is the agency most frequently engaged in security enforcement, but its mission and authority grant limit this activity in some fields. Other agencies may be better situated to trigger material security improvements in some contexts. For example, but for limited circumstances, the FTC does not perceive itself to have robust authority to fine or to write regulations, but many other agencies do have robust grants of this authority. Because of the FTC's mission, in the context of medical device security, for example its enforcement authority is limited to policing medical device advertising, rather than the functionality of the medical device's security itself. In contrast, the FDA's enforcement authority makes it the more ideal agency for policing medical device security as a substantive matter, and the FDA has issued "cybersecurity" guidance on the substance of addressing medical device security in device manufacturing.[272] Nothing stops the two agencies from creating a more formal, shared team of enforcers who actively cooperate on medical device security for greater enforcement impact. Collaboratively, the new task force team would create efficiencies in enforcement and enhanced security information sharing using the new joint capabilities. In particular, the team might decide that the FTC and FDA might jointly issue guidance stating that security claims in medical contexts are subject to a duty of expert substantiation, much like

[272] The FDA has issued guidance on security. *See, e.g.*, U.S. DEP'T HEALTH & HUMAN SERVICES, U.S. FOOD & DRUG ADMIN., GUIDANCE FOR INDUSTRY: CYBERSECURITY FOR NETWORKED MEDICAL DEVICES CONTAINING OFF-THE-SHELF (OTS) SOFTWARE (2005) http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm077812.htm [https://perma.cc/5N4C-6YZ8]. It has also recently begun to notify consumers of information security vulnerabilities in medical devices and hospital systems. *See, e.g.*, U.S. FOOD & DRUG ADMIN., VULNERABILITIES OF HOSPIRA LIFECARE PCA3 AND PCA5 INFUSION PUMP SYSTEMS: FDA SAFETY COMMUNICATION: FDA SAFETY COMMUNICATION (2015), http://wayback.archive-it.org/7993/20170722144742/https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm [https://perma.cc/TN9P-CRQR] (last visited Apr. 14, 2018).

advertising with medical claims.[273] Meanwhile, in a parallel manner to the FDA's requirements for nutritional labels disclosing food ingredients, [274] the FTC and FDA task force might assert that this security substantiation requirement means that any company marketing code-reliant medical devices must make a "security health" label available to consumers for examination prior to purchase or use of the device. As such, in the event of an alleged misrepresentation of security capabilities of a medical device, the manufacturer would face enforcement activity from both agencies simultaneously and with a united front.

Meanwhile, the FTC could also create parallel enforcement teams (and security substantiation guidance) with the DOT/NHTSA on auto security, the SEC on market regulation and security, and CFPB on security of credit reporting agencies and financial products. In other words, with significantly improved, formalized interagency cooperation and information sharing using bilateral taskforces, regulatory gaps in security enforcement and policy can be remedied and harmonized.[275]

2. Market participants should vet security as part of assessment of corporate governance and risk.

In order to ensure that companies are rewarded in the market for adopting a defense primacy posture and prioritizing security in their operations, consumers, market makers, and institutional investors should increase their analysis of public companies' security profiles, as well as their histories of vulnerability management. In 2005, I argued that the SEC should issue guidance instructing publicly traded companies to disclose the existence of information security deficits and breaches as material events for purposes of quarterly and annual reporting.[276] In 2011, the SEC mirrored these recommendations and issued its "Cybersecurity Guidance," urging public companies to disclose "cybersecurity

[273] Under Section 5 of the FTC Act, 15 U.S.C. §45, the FTC has authority to designate certain categories of advertising – those involving health claims, expert claims, and celebrity endorsements, for example - that require an advertiser to conduct independent scientific testing to validate the truth of promises in advertising when not mere puffery. *See, e.g.*, FTC Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255 (2009).

[274] *See, e.g.*, Ellen P. Goodman, *Visual Gut Punch: Persuasion, Emotion, and the Constitutional Meaning of Graphic Disclosure*, 99 CORNELL L. REV. 513, 515-16 (2014) (discussion of labeling).

[275] Particularly because a robust body of security tort law has not yet developed, these regulatory gaps are acutely felt in practice when vulnerable devices cause damage to consumer, corporate, and government security.

[276] *See* Matwyshyn *supra* note 251, at 187.

risks and cyber incidents."[277] In 2018, the SEC has expanded this guidance, again signaling the importance of corporate security practices in ensuring accurate investor market information. Specifically, the 2018 guidance addresses not only security risks and incidents, but also "the importance of cybersecurity policies and procedures and the application of disclosure controls and procedures, insider trading prohibitions, and Regulation FD and selective disclosure prohibitions in the cybersecurity context."[278] Yet, public companies' disclosure practices have not uniformly improved in their discussions of security since 2011, and the SEC has not engaged in enforcement against public companies for inadequacies in their security disclosures.

Presumably the securities litigation class action bar will view the 2018 SEC guidance as an indication of a firm basis for securities suits by private litigants. However, a swifter avenue for security improvements may arise from market makers, institutional investors, and other key market players demanding improved security governance information from the companies they consider for investment. In this way, directed questions on security by key corporate constituencies will apply pressure on officers and directors to engage in more careful oversight of companies' security governance processes.

This market pressure may incentivize companies to prioritize security in governance, particularly if combined with increased enforcement by securities regulators, courts and state legislatures, and evolution of fiduciary duties to specifically address corporate security decisions.[279] Because private sector and public sector security concerns are reciprocal, these improvements in private sector corporate governance on security will indirectly impact the public sector as well.

V. CONCLUSION

This essay has offered a series of concrete proposals to operationalize the paradigm of reciprocal security introduced in *CYBER!*. While no single policy or legal intervention will meaningfully address the severe deficits in security that exist today across both the public and private sector, the combination of the proposals contained herein offers a path toward material incremental security improvement.

---

[277] Division of Corporation Finance, Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2 Cybersecurity, October 13, 2011, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[278] Press Release, Sec. & Exchn. Comm'n, SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018), https://www.sec.gov/news/press-release/2018-22 [https://perma.cc/S7XX-W5U3].

[279] Andrea M. Matwyshyn, *Imagining the Intangible*, 34 DEL. J. CORP. L. 965, 980 (2009).