Michigan Technology Law Review

Article 4

2018

The Secrets We Keep…: Encryption and the Struggle for Software Vulnerability Disclosure Reform

Ian Williams
University of Michigan Law School, ianwill@umich.edu

THE SECRETS WE KEEP. . . : ENCRYPTION AND THE STRUGGLE FOR SOFTWARE VULNERABILITY DISCLOSURE REFORM

*Ian Williams**

Vulnerabilities within pieces of software can expose otherwise secure data to outside parties. Such vulnerabilities are exploited not just by malicious actors looking to exploit secured data for criminal reasons, but also by law enforcement and intelligence agencies. Government agencies have cultivated vulnerabilities as investigative tools and cyber weapons, and at times keep the vulnerabilities they have discovered secret from both the companies that produced the software and the consumers who rely upon it. While the US Government has created a vulnerability disclosure system to help decide when to keep a vulnerability secret, it does not do enough to balance the government's national security and law enforcement interests with the data security interests of the public. As debates over government access to encrypted data continue, a strong legal framework for deciding when and how government actors can keep vulnerabilities secret must be established.

I. INTRODUCTION

Like any product created by humans, software is never perfect. Imperfections in a piece of software can affect a program in a myriad of ways, but few are more problematic than those that affect the security of a computer program or system. In computer security, these "software vulnerabilities" are defined as any "programming mistake that allows an adversary access" into a computer system.[1] With knowledge of a vulnerability, malicious ac-

* Fellow for the Law & Mobility Program, University of Michigan Law School. J.D. 2018, University of Michigan Law School. Thank you to Gautam Hans, not only for shepherding the initial research that lead to this piece, but for being a friend and mentor. Thank you also to Professor Evan Caminker, for his notes and guidance. Finally, thank you to the staff of MTLR, for overlooking my tyrannical reign as their EIC when they agreed to continue working with me and publish this piece.

This piece was originally written in December of 2017. It is a snapshot of the discussed issues at that time—unfortunately technology often moves quickly, and there are developments in both case law and public policy since that time that are left undiscussed. Readers are encouraged to use this note as a primer for their own exploration of these issues.

1. Bruce Schneier, *Disclosing vs. Hoarding Vulnerabilities*, SCHNEIER ON SECURITY (May 22, 2014, 6:15 AM), https://www.schneier.com/blog/archives/2014/05/disclosing_vs_h.html.

tors can create "exploits," pieces of software that use a given vulnerability to their own advantage, often to circumvent standard security measures like passwords or encryption and provide a backdoor into a system.[2] The closest most users will get to these vulnerabilities is when they download updates to their programs, many of which are "patches" intended to fix vulnerabilities. Of course, depending on the age and sophistication of the system, patching vulnerabilities can be difficult and often requires some effort on the part of developers and users to be effective.[3] Often, however, the biggest stumbling block on the path toward fixing a vulnerability is not designing a patch or convincing end users to download updates, but rather is finding out the vulnerability exists in the first place. Vulnerabilities that have yet to be discovered by a program's developer or end user are known as "zero-day vulnerabilities," as the developer in question has had zero days to patch the problem and users have equally had zero days to implement the patch or other protective moves.[4]

Developers are naturally keen to find and patch such zero-day vulnerabilities and often rely on security researchers and "white hat" hackers to assist in that work.[5] To entice third-parties to help find vulnerabilities, many developers and organizations sponsor "bug bounties," with the promise of fame (via public credit for finding the issue) and fortune (via hard cash or items of value like frequent flyer miles) for those who uncover vulnerabilities.[6] In 2017 alone, bug bounty payouts totaled more than $6 million, a 211% increase from the total payouts in 2016,[7] and bug bounty programs had been launched not only by major tech companies like Google,[8] Mi-

2. Dave Piscitello, *Threats, Vulnerabilities and Exploits—oh my!*, ICANN: BLOG (Aug. 10, 2015), https://www.icann.org/news/blog/threats-vulnerabilities-and-exploits-oh-my ("Not all exploits involve software, and it's incorrect to classify all exploit-based attacks as hacking. Scams - socially engineering an individual or employee into disclosing personal or sensitive information - are an age-old kind of exploit that does not require hacking skills.").

3. Steven M. Bellovin, *Patching is Hard*, SMBLOG (May 12, 2017), https://www.cs.columbia.edu/~smb/blog//2017-05/2017-05-12.html.

4. ARI SCHWARTZ & ROB KNAKE, GOVERNMENT'S ROLE IN VULNERABILITY DISCLOSURE 3 (2016), https://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf [hereinafter SCHWARTZ & KNAKE].

5. *See* G. Burningham, *The Rise of White Hat Hackers and the Bug Bounty Ecosystem*, NEWSWEEK (Jan. 31, 2016, 1:02 PM), http://www.newsweek.com/2016/02/12/white-hat-hackers-keep-bug-bounty-421357.html.

6. BUGCROWD INC., THE STATE OF THE BUG BOUNTY 4 (June 2016), https://ww2.bugcrowd.com/rs/453-IJC-858/images/state-of-bug-bounty-2016.pdf?utm_source=website&utm_medium=resources_page&utm_content=state-of-bug-bounty-2016.

7. BUGCROWD INC., 2017 STATE OF THE BUG BOUNTY REPORT 1 (2017), https://ww2.bugcrowd.com/rs/453-IJC-858/images/Bugcrowd-2017-State-of-Bug-Bounty-Report.pdf?utm_source=website&utm_medium=resources_page&utm_content=Bugcrowd-2017-State-of-Bug-Bounty-Report.

8. *Google Vulnerability Reward Program (VRP) Rules*, GOOGLE APPLICATION SECURITY, https://www.google.com/about/appsecurity/reward-program/ (last visited Dec. 20, 2017).

crosoft,[9] Facebook,[10] and PayPal[11] but also "real-world" companies like United Airlines.[12] In 2016, the Department of Defense ran a pilot program bug bounty that "exceeded all expectations," with 138 unique vulnerabilities being discovered within the Department's computer systems.[13] These programs are part of a greater vulnerability disclosure ecosystem that includes paid bounties and other unpaid reporting schemes.[14]

Zero-day vulnerabilities have also attracted interest from civilian government actors, as they offer a valuable tool for criminal investigations and espionage. The utility of these vulnerabilities leaves governments in a precarious situation—should they protect end users by revealing the vulnerabilities, thereby allowing developers to patch them, or should they keep them secret to serve the needs of law enforcement and intelligence agencies? By keeping a zero-day vulnerability secret, government agencies can retain them as novel means of accessing a suspect or intelligence target's computer, as a target will be unaware that any security flaw exists. In August of 2016, the precarious nature of this situation played out in full view of the public, as a group of hackers calling themselves the "Shadow Brokers" began advertising that it had stolen a number of exploits from the NSA.[15] In May of 2017 some of those exploits were used (possibly by North Korean hackers) as part of the "WannaCry" ransomware attack that struck at computers worldwide.[16] The situation was further complicated in November of 2017, when the White House released details on a new "Vulnerabilities Equities Policy and Process" (VEP) for the US government, detailing how and when vulnerabilities discovered by government entities would be made public.[17]

The fight over vulnerability disclosure plays out across the backdrop of a long-running debate over government access to secured information. As

---

9. *Microsoft Bug Bounty Program*, MICROSOFT, https://technet.microsoft.com/en-US/security/dn425036 (last visited Dec. 20, 2017).

10. *Information*, FACEBOOK (Sept. 12, 2018), https://www.facebook.com/whitehat.

11. *PayPal Bug Bounty Program*, PAYPAL, https://www.paypal.com/us/webapps/mpp/security-tools/reporting-security-issues (last visited Dec. 20, 2017).

12. *United Airlines bug bounty program*, UNITED, https://www.united.com/web/en-US/content/contact/bugbounty.aspx (last visited Dec. 20, 2017).

13. *HACK THE PENTAGON*, HACKERONE, https://www.hackerone.com/resources/hack-the-pentagon (last visited Dec. 20, 2017).

14. *See Bug Bounty List*, BUGCROWD, https://www.bugcrowd.com/bug-bounty-list/ (last visited Dec. 20, 2017).

15. Bruce Schneier, *Who Are the Shadow Brokers?*, ATLANTIC (May 23, 2017), https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

16. *See* Olivia Solon, *WannaCry ransomware has links to North Korea, cybersecurity experts say*, GUARDIAN (May 15, 2017, 6:58 PM), https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group.

17. *See* THE WHITE HOUSE, *Vulnerabilities Equities Policy and Process for the United States Government* (Nov. 15, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF [hereinafter 2017 VEP].

computer security and encryption have grown stronger, the US government has sought means to break that security and retain the access to communications (for both intelligence purposes and criminal investigation) that it had in the pre-digital era. In the 1990s, this played out in the "Crypto Wars," a series of policy and legal battles between the government and technology advocates, which ended with the government loosening restrictions on cryptographic technology and abandoning attempts to force hardware developers to include government backdoors into their products.[18] However, as encryption technology has become more advanced and more commonplace,[19] figures in the law enforcement[20] and intelligence communities[21] have begun to raise the issue of requiring backdoors once more.

The issues around vulnerability disclosures and government backdoors are complicated and expansive, and it would be presumptuous, if not foolhardy, to claim this paper will cover them all. What it will do is look at these two important issues through the lens of two recent court cases to see how these issues have begun to play out in the legal system. Part I will expand on the issues of vulnerability disclosure and use by government and explore what implications those issues have on prosecutions by looking at the Playpen cases—where the FBI used a software vulnerability within the Firefox browser to hack into a website distributing child pornography. Part II will then explore the San Bernardino iPhone case, where the FBI attempted to force Apple into creating a backdoor into the iPhone's encryption and the case's relationship to the greater debate over government-mandated backdoors. Part III will explore recently enacted and proposed solutions to these conflicts, including the new VEP. Finally, Part IV will propose a hybrid solution that attempts to provide a balance between the competing interests involved.

---

18. DANIELLE KEHL ET AL., DOOMED TO REPEAT HISTORY? LESSONS FROM THE CRYPTO WARS OF THE 1990S 1 (June 2015), https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf.

19. *See, e.g.,* Joe Miller, *Google and Apple to Introduce Default Encryption*, BBC NEWS (Sept.19, 2014), https://www.bbc.com/news/technology-29276955.

20. James B. Comey, Director, FBI, Going Dark: Are Technology, Privacy, and Public Safety on a Collison Course?, Remarks to the Brookings Institution (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

21. *See* Tom McCarthy, *NSA Director Defends Plan to Maintain 'Backdoors' into Technology Companies*, GUARDIAN (Feb. 23, 2015, 3:12 PM), https://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies.

II. Vulnerability Disclosures, Government Stockpiles, and the Playpen Cases

The pursuit and exploitation of vulnerabilities have existed since the dawn of the modern era of computing. In 1988, the "Morris Worm" became the first publicized use of a computer worm (a program that copies itself from computer to computer), and it was able to infect about 6,000 of the 60,000 hosts linked to the then-nascent internet.[22] At the time, network administrators did little to protect their systems and gave little thought to online attacks.[23] The worm's architect, a Cornell graduate student named Robert Morris, had created the worm not out of malice, but rather intellectual curiosity, though that did not stop him from becoming the first person prosecuted under the Computer Fraud and Abuse Act (CFAA).[24]

The Morris Worm was a wakeup call to both industry and government that malicious actors could exploit software vulnerabilities to weaken or break computer networks. In November of 1988 the Defense Advanced Research Projects Agency (DARPA) and Carnegie Mellon University formed the Computer Emergency Response Team Coordination Center (CERT-CC), which continues to this day to alert "U.S. industry and computer users worldwide to potential threats to the security of their systems" and provide "information about how to avoid, minimize, or recover from the damage."[25] Private industry likewise saw the necessity of pursuing vulnerabilities, with Netscape launching the first bug bounty program in 1995.[26]

As more researchers began to hunt for vulnerabilities, experts began developing three general categories governing when and to whom a vulnerability should be revealed:

- Full disclosure—Full details are released [publicly] as soon as possible, often without vendor involvement

- Coordinated disclosure—Researcher and vendor work together so that the bug is fixed before the vulnerability is disclosed

---

22. *See Timeline of Computer History—1988*, Computer History Museum, http://www.computerhistory.org/timeline/1988/ (last visited Dec. 20, 2017).

23. *See* Timothy B. Lee, *How a Grad Student Trying to Build the First Botnet Brought the Internet to its Knees*, Wash. Post (Nov. 1, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/?utm_term=.fa24b99bbb89.

24. *See id.*

25. Byron Spice, *U.S. Department of Homeland Security Announces Partnership with Carnegie Mellon's CERT Coordination Center*, Carnegie Mellon U. (Sept. 15, 2003), https://www.cs.cmu.edu/news/us-department-homeland-security-announces-partnership-carnegie-mellons-cert-coordination-center.

26. *See* Esben Friis-Jensen, *The History of Bug Bounty Programs*, Cobalt (Apr. 10, 2014), https://blog.cobalt.io/the-history-of-bug-bounty-programs-50def4dcaab3.

- Private or Non-Disclosure—The vulnerability is released to a small group of people (not the vendor) or kept private[27]

Upon discovering a vulnerability, a researcher can choose to release its details on their own (full disclosure), work with the software's vendor to fix the problem before making it public, or can choose to keep the information to itself, the latter of which (unless the vulnerability is later discovered by the vendor) leaves users at risk. From these three basic categories developers and corporations have spun a diverse web of policies, each with unique requirements and timetables.[28]

A. *Vulnerabilities Equities Policy and Process*

From 1988 and onward the government remained involved in public-facing vulnerability disclosure via CERT-CC, but it would not be until 2008 that the national security apparatus began to give the issue any attention.[29] On January 8, 2008, President George W. Bush signed National Security Presidential Directive 54 (NSPD-54), which was intended to give direction for federal cybersecurity operations.[30] This order led to the development of the "Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process" (VEP), a policy detailed in a document dated February 16, 2010, which was only partially declassified to the public in January of 2016.[31] The 2010 VEP applied to vulnerabilities that were "newly discovered and not publicly known,"[32] and did not apply to vulnerabilities discovered in the course of open and unclassified research.[33] The policy noted that "the discovery of vulnerabilities 'may present competing equities for [US government] offensive and defensive mission interests,' "[34] and thus "actions taken in response to knowledge of a specific vulnerability must be coordinated to ensure the needs of each of these 'equities' are addressed."[35] When a government entity identifies a vulnerability, the entity is tasked with reporting it to the "Executive Secretariat," a position assigned to the National Security Agency

27. Brad Antoniewicz, *Approaches to Vulnerability Disclosure*, OPEN SECURITY RES. (June 24, 2014), http://blog.opensecurityresearch.com/2014/06/approaches-to-vulnerability-disclosure.html.

28. *See id.*

29. SCHWARTZ & KNAKE, *supra* note 4, at 4.

30. *See* National Security Presidential Directive, NSPD-54 (Jan. 8, 2008), https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf.

31. *See EFF v. NSA, ODNI—Vulnerabilities FOIA*, EFF, https://www.eff.org/cases/eff-v-nsa-odni-vulnerabilities-foia (last visited Dec. 20, 2017).

32. COMMERCIAL AND GOVERNMENT INFORMATION TECHNOLOGY AND INDUSTRIAL CONTROL PRODUCT OR SYSTEM VULNERABILITIES EQUITIES POLICY AND PROCESS 5 (Feb. 16, 2010), https://www.eff.org/document/vulnerabilities-equities-process-january-2016.

33. *Id.* at 4.

34. *Id.* at 2.

35. *Id.*

Information Assurance Directorate.[36] The Executive Secretariat facilitates the flow of information about the new vulnerability to VEP "Points of Contact" within a number of government agencies.[37] If these agencies believe they have an equity at stake in the vulnerability, they will then take part, via subject matter experts assigned by each agency, in a multiagency discussion regarding the vulnerability, which will then lead to a recommendation to an Equities Review Board[38] (another multiagency body).[39]

The 2010 VEP report, and the secret process it created, began to come to light in 2014 after the public exposure of a major encryption vulnerability. In April of that year, computer security researchers revealed that a major security vulnerability, which they named "Heartbleed," existed within the OpenSSL software that many websites used to encrypt traffic.[40] The vulnerability exploited the connection process between a computer and an encrypted website, allowing hackers to bleed off data (including passwords and usernames) from what should have been secure systems.[41] News reports began to circulate that the NSA had been aware of the vulnerability for two years, based on unnamed sources who claimed the vulnerability had become a "basic part of the agency's toolkit for stealing account passwords and other common tasks."[42] The controversy led the Obama Administration to publicize the existence of the VEP, admitting that "building up a huge stockpile of undisclosed vulnerabilities while leaving the Internet vulnerable and the American people unprotected would not be in our national security interest."[43] They even provided a list of questions typically asked when considering the withholding of a vulnerability:

- How much is the vulnerable system used in the core internet infrastructure, in other critical infrastructure systems, in the U.S. economy, and/or in national security systems?

- Does the vulnerability, if left unpatched, impose significant risk?

---

36. *Id.* at 3–5.
37. *Id.* at 3.
38. *Id.* at 3–4.
39. *Id.* at 7.
40. Kim Zetter, *Has the NSA Been Using the Heartbleed Bug as an Internet Peephole?*, WIRED (Apr. 10, 2014, 6:30 AM), https://www.wired.com/2014/04/nsa-heartbleed/.
41. *Id.*
42. Kim Zetter, *Report: NSA Exploited Heartbleed to Siphon Passwords for Two Years*, WIRED (Apr. 11, 2014, 4:57 PM), https://www.wired.com/2014/04/nsa-exploited-heartbleed-two-years/.
43. Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, WHITE HOUSE BLOG (Apr. 28, 2014, 3:00 PM), https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

- How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
- How likely is it that we would know if someone else was exploiting it?
- How badly do we need the intelligence we think we can get from exploiting the vulnerability?
- Are there other ways we can get it?
- Could we utilize the vulnerability for a short period of time before we disclose it?
- How likely is it that someone else will discover the vulnerability?
- Can the vulnerability be patched or otherwise mitigated?[44]

The White House further stated that the process was "biased toward responsibly disclosing the vulnerability."[45] They did not, however, release the 2010 VEP document, which was released only after a FOIA request and legal battle between the Electronic Frontier Foundation (EFF), the NSA, and the Office of the Director of National Intelligence (ODNI).[46]

In 2016, the danger of vulnerability stockpiles became painfully clear, as a major security breach by a hacker organization called the "Shadow Brokers" released NSA-held vulnerabilities across the internet.[47] The Shadow Brokers released several different caches of NSA exploits, which targeted network routers, email servers, and the Windows operating system.[48] The Microsoft exploits were mainly older vulnerabilities, many of which had already been patched, though they would still be of use against unpatched systems.[49] The leak of these tools threw the NSA into turmoil, as the agency struggled to rebuild its arsenal while investigating the source of the leaked

44. *Id.*
45. *Id.*
46. *EFF v. NSA, ODNI—Vulnerabilities, FOIA*, *supra* note 31.
47. *See* Schneier, *supra* note 15.
48. *Id.*
49. Tim Cushing, *Latest Exploit Dump by Shadow Brokers Contains Easy-to-Use Windows Exploits, Most Already Patched by Microsoft*, TECHDIRT (Apr. 17, 2017, 3:22 AM), https://www.techdirt.com/articles/20170416/08190937159/latest-exploit-dump-shadow-brokers-contains-easy-to-use-windows-exploits-most-already-patched-microsoft.shtml.

materials.[50] Then, in May of 2017, one of the vulnerabilities included in the Shadow Broker's leaks was used to launch "WannaCry," a massive, world-wide cyber-attack.[51] The vulnerability was used to spread "ransomware," a type of malicious software, which held computers hostage until their owners paid the hackers to release them.[52] In a further blow to the NSA, researchers found signs that the attack was launched by North Korean hackers, using the NSA's own tools, though there was no evidence of North Korean involvement in the original theft of the hacking tools.[53] The incident prompted Microsoft to publicly criticize government stockpiling of vulnerabilities, comparing the leak of the NSA tools to the theft of Tomahawk cruise missiles.[54]

B. *The Playpen Cases: Vulnerability Disclosure and Criminal Investigations*

While the national security side of vulnerability disclosures has received the bulk of public and press attention, the issue of government-held vulnerabilities has also appeared in a series of criminal cases tied to a 2015 FBI operation to shut down a child pornography distribution website named Playpen. First created in August of 2014, the site had 60,000 member accounts within a month, booming to 215,000 accounts by 2015.[55] Acting on a tip from a foreign law enforcement agency, the FBI began to investigate Playpen and eventually secured a warrant to seize control of the site's server. With the server under their control, the FBI allowed the site to continue operation for almost two weeks, between February 20th and March 4th, 2015, before finally taking it down. During that period the FBI received a second warrant authorizing it to send malware (called a "Network Investiga-

50. See Scott Shane et al., *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core*, N.Y. TIMES (Nov. 12, 2017), https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.

51. *See* Ian Sherr, *WannaCry Ransomware: Everything You Need to Know*, CNET (May 19, 2017, 12:29 PM), https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/.

52. *See* Nicole Perlroth & David E. Sanger, *In Computer Attacks, Clues Point to Frequent Culprit: North Korea*, N.Y. TIMES (May 15, 2017), https://www.nytimes.com/2017/05/15/us/nsa-hacking-shadow-brokers.html.

53. *Id.*

54. Brad Smith, *The Need For Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack*, MICROSOFT: MICROSOFT ON THE ISSUES (May 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/?tduid=(29c8620bd207948d693e858a037b4a00)(256380)(2459594)(nOD_rLJHOac-QBTAt391V._e5aR84aLD.Q)()#sm.001c8i11317l0f3vs2f1cm2qoliu3?ranMID=24542&ranEAID=nOD%2FrLJHOac&ranSiteID=nOD_rLJHOac-QBTAt391V._e5aR84aLD.Q.

55. Joseph Cox, *The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers*, MOTHERBOARD (Jan. 4, 2016, 4:00 PM), https://motherboard.vice.com/en_us/article/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

tion Technique" (NIT)) through the site to anyone who visited the site.[56] It is believed the NIT exploited a vulnerability in the code of the Firefox Browser, as bundled within the Tor Browser (a browser used to surf the web anonymously).[57] Any computer that visited Playpen would be infected with the NIT, which was able to search infected computers for identifying information, including the computers' IP addresses. [58] Once investigators obtained the IP addresses, they subpoenaed ISPs to learn the names and addresses of the individuals associated with the given IPs. They secured search warrants for those individuals and carried out numerous searches and seizures.[59] Overall, the Playpen investigation was a massive success, leading to 350 arrests, as well as the prosecution of 25 producers of child pornography, 51 hands-on abusers, and the identification or rescue of 55 children in the US alone.[60]

As the Playpen cases came to trial, however, questions began to arise about the NIT itself. Defendants and their attorneys wanted to know more about the malware that had been used to identify them. *United States v. Michaud*, No. 3:15-cr-05351RJB (W.D. Wash.), a case in the Western District of Washington, became a focal point of the issue, as the Defendant fought for the chance to examine the code of the NIT. Michaud, a former school district administration worker, was arrested after the NIT gave the FBI evidence that he had accessed the Playpen site.[61] In court, the Judge showed an inclination toward disclosure, commenting at one point that, "much of the details of this information is lost on me, I am afraid, the technical parts of it, but it comes down to a simple thing. . . . You say you caught me by the use of computer hacking, so how do you do it? How do you do it? A fair question."[62] After hearing arguments from both sides, the court had to admit it was trapped in a catch-22, noting, "the defendant has the right to review the full N.I.T. code, but the government does not have to produce it[.]"[63]

---

56. *The Playpen Cases: Frequently Asked Questions*, EFF, https://www.eff.org/pages/playpen-cases-frequently-asked-questions#whathappened (last visited Dec. 20, 2017).

57. *Id.*

58. *See 'Playpen' Creator Sentenced to 30 Years*, FBI (May 5, 2017), https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years.

59. *See id.*

60. *Id.*

61. *See* Cyrus Farivar, *Feds May Let Playpen Child Porn Suspect Go to Keep Concealing Their Source Code*, ARS TECHNICA (Jan. 9, 2017, 4:39 PM), https://arstechnica.com/tech-policy/2017/01/feds-may-let-playpen-child-porn-suspect-go-to-keep-concealing-their-source-code/.

62. Joseph Cox, *Transcript Shows Why a Judge Ordered the FBI to Reveal Its Mass Hacking Malware*, MOTHERBOARD (Feb. 24, 2016, 12:30 PM), https://motherboard.vice.com/en_us/article/transcript-shows-why-a-judge-ordered-the-fbi-to-reveal-mass-hacking-malware-playpen-jay-michaud.

63. Order on Procedural History and Case Status in Advance of May 25, 2016 Hearing at 5, United States v. Jay Michaud, No. 3:15-cr-05351RJB (W.D. Wash. May 18, 2016).

Michaud's defense highlighted the fact that in a similar 2013 case, the FBI had been extremely cooperative in revealing details on a different NIT.[64] After continued debate the District Court finally ruled that the evidence based on the NIT was inadmissible.[65] While the US Attorney pursued an appeal of that order with the Ninth Circuit, the FBI classified "portions of the tool, the exploits used in connection with the tool, and some of the operational aspects of the tool."[66] In December of 2016 the government dropped the appeal citing "further review within the Department of Justice [of] the Court's order and the record in the case."[67] Finally, in March of 2017 the government dismissed the indictment, stating it had to "choose between disclosure of classified information and dismissal of [the] indictment," and given that "disclosure is not currently an option," the case had to be dropped.[68]

Given that the NIT in question involved their product, Mozilla, the creators of the Firefox browser, sought to intervene in the *Michaud* case. Following the Court's first order compelling the government to provide the code of the NIT, Mozilla filed a motion to intervene or appear as amicus curiae in relation to the government's motion to reconsider.[69] Citing reason to believe the NIT's exploit involved "a previously unknown and potentially still active vulnerability" in Firefox, Mozilla argued the vulnerability could put the security of millions of users at risk, and they asked the court to order the government to disclose the vulnerability to it before turning it over to the defendant.[70] In their brief Mozilla also noted that the government had refused to tell it if the vulnerability in question had gone through the VEP.[71] In the end, the Court denied the motion, effectively telling Mozilla to seek answers from the government directly.[72] Unable to gain information about the vulnerability in their product via the courts, Mozilla chose to put its

64. Declaration of Matthew Miller at 4, United States v. Jay Michaud, No. 3:15-cr-05351RJB (W.D. Wash. May 9, 2016).

65. Order Denying Dismissal and Excluding Evidence at 1, United States v. Jay Michaud, No. 3:15-cr-05351RJB (W.D. Wash. May 25, 2016).

66. Government's Response to Defendant's Motion to Compel at 22 n.8, United States v. Gerald Andrew Darby, No. 2:16cr36 (E.D. Va. June 16, 2016).

67. Motion of the United States for Voluntary Dismissal of its Appeal at 3-4, United States v. Michaud, No. 16-30163 (9th Cir. Dec. 23, 2016).

68. Government's Unopposed Motion to Dismiss Indictment Without Prejudice at 2, United States v. Jay Michaud, No. 3:15-cr-05351RJB (W.D. Wash. Mar. 3, 2017).

69. Mozilla's Motion to Intervene or Appear as Amicus Curiae in Relation to Government's Motion for Reconsideration of Court's Order on the Third Motion to Compel, United States v. Jay Michaud, No. 3:15-cr-05351RJB (W.D. Wash. May 11, 2016).

70. *Id.* at 1.

71. *Id.* at 7 n. 9.

72. *See* Seung Lee, *FBI Doesn't Have to Give Mozilla Details On Bug It Used to Bust a Child Porn Ring*, NEWSWEEK (May 18, 2016, 6:22 PM), http://www.newsweek.com/fbi-doesnt-have-give-mozilla-details-bug-it-used-bust-child-porn-ring-461325.

weight behind efforts to reform the VEP and create legislation to guide the process.[73]

The issues that arose in *Michaud* illustrate how government uses of software vulnerabilities can stretch beyond national security and how the secretive way the government has chosen to deal with vulnerabilities can cost it convictions in criminal cases. Whenever vulnerabilities are exploited to gain evidence in a criminal case, the government runs the risk of hitting the same wall it did in *Michaud*. Defendants will argue that information about the vulnerability is material to their defense, leaving the government to "disclose or dismiss."[74] This opens the door to a version of what is called "graymail" in national security prosecutions—a situation where a potential criminal defendant threatens to expose sensitive classified information if they are prosecuted.[75] Though the exact decision-making process behind the choice has yet to come to light, when the government refuses to release information on a vulnerability, they are making a choice: secrecy over law enforcement.

III. Making New Vulnerabilities—Backdoors and San Bernardino

For decades the government has sought to create vulnerabilities where there once were none—all in the name of national security. These software "backdoors"—intentional weaknesses in a piece of technology or software—are designed to allow authorities to bypass security features.[76] The recent boom in encryption capabilities has led some in the government to call for controls on just how secure a developer can make their product, lest they prevent law enforcement from gaining access.[77] While discussions of encryption are not always directly connected to discussions of vulnerability disclosure, history and recent events show that many of the same issues arise in the context of backdoors.

The first major battle over encryption backdoors came in the 1990s, a period that has come to be known in technology policy circles as the "Cryp-

73. *See* Denelle Dixon, *Improving Internet Security Through Vulnerability Disclosure*, Mozilla Blog (May 17, 2017), https://blog.mozilla.org/blog/2017/05/17/improving-internet-security-vulnerability-disclosure/.

74. Susan Hennessey & Nicholas Weaver, *A Judicial Framework for Evaluating Network Investigative Techniques*, Lawfare (July 28, 2016, 10:17 AM), https://lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques.

75. Arjun Chandran, Note, *The Classified Information Procedures Act in the Age of Terrorism: Remodeling CIPA in an Offense-Specific Manner*, 64 Duke L.J. 1411, 1415 (2015).

76. *See* Lisa A. Hayes, *Strong Encryption Wins Again, Time to End the Debate on Government Backdoors*, CDT (Mar. 29, 2016), https://cdt.org/blog/strong-encryption-wins-again-time-to-end-the-debate-on-government-backdoors/.

77. *See, e.g.*, Comey, *supra* note 20.

to Wars."[78] In 1993, with personal computers and the internet proliferating at an ever-increasing rate, the Clinton administration announced the creation of the "Clipper Chip," a microchip intended to be inserted into consumer telephones.[79] The chip was promised to provide consumers with secure encrypted communications while preserving government access to unencrypted versions of those communications.[80] The chip worked by requiring two separate cryptographic keys to decrypt any communication, a style of system known as "key escrow."[81] These keys would be held by two separate government agencies, the National Institute of Standards and Technology (NIST) and the Treasury Department, who would only release those keys to law enforcement with "lawful authorization."[82] Industry groups moved quickly to criticize the proposal, as did civil liberties organizations. While the proposal did not require industry to include the chips in their devices, many in industry saw the move as the first step toward greater restrictions on encryption in the future.[83] By 1994, public opinion was against the chip as well, with a CNN/TIME poll finding 80% of Americans opposed.[84] The chip was finally killed when, later that year, a computer scientist was able to demonstrate that with a "brute force" attack, a user could override the technology that allowed law enforcement to surveil communications using the chip—making the backdoor useless.[85] For the time being, it seemed, encryption was protected.

The current debate over encryption and government backdoors is part of the greater debate over government surveillance launched by Edward Snowden's 2013 exposure of expansive NSA surveillance programs. The reaction by the tech industry was almost immediate—in 2014 Google and Apple both introduced default encryption in their smartphone operating systems.[86] At the same time, law enforcement and intelligence agencies began to once again broach the subject of limitations on encryption. In an October 16, 2014 speech at the Brookings Institute, then FBI Director James Comey spoke about such limits, saying that the FBI often had "the legal authority to intercept and access communications and information pursuant to court orders," but "often lacked the technical ability to do so."[87] He went on to say that the FBI needed "assistance and cooperation from companies to comply with lawful court orders," and that the private sector needed to "take a step back," pause, and "consider changing course" when it came to ever-

78. KEHL ET AL., *supra* note 18, at 1.
79. *Id.* at 5.
80. *Id.*
81. *See id.*
82. *Id.*
83. *Id.* at 6.
84. *Id.* at 8.
85. *Id.*
86. Miller, *supra* note 19.
87. Comey, *supra* note 20.

increasing encryption.[88] A few months later, then NSA Director Mike Rogers, in a question-and-answer session with technology policy experts, supported the creation of built-in government access, saying backdoors would not "fatally compromise encryption" or limit international markets for US products (two major concerns of backdoor opponents).[89] Despite such high-level discussions, it would take a tragic mass shooting to bring the debate into the public consciousness.

A. *Apple, the FBI, and San Bernardino*

On December 2, 2015, a married couple, Syed Rizwan Farook and Tashfeen Malik, attacked a holiday party in San Bernardino, California, killing 14 people. Farook and Malik were killed by the police after a high-speed chase.[90] Amongst the evidence collected by the FBI in the aftermath of the shooting was Farook's employer-issued iPhone, which had been locked with a numeric passcode.[91] One of the iPhone's built-in security features, an auto-erase function, had also been enabled, which would destroy the encryption key after 10 failed attempts to unlock the device, rendering the information on the phone forever inaccessible.[92] In an effort to recover any information that could be on the phone, the FBI sought a court order to compel Apple to create for it a custom piece of software to circumvent the phone's security.[93] The program would reboot the phone while bypassing or disabling the auto-erase function, allowing the FBI to then use another program to rapidly guess the passcode.[94] A federal magistrate granted the order, though Apple appealed, beginning a very public legal battle between the company and the government.[95] In its motion to vacate the order, Apple rebuked the government's claim that this was a one-time request, and argued that they believed the backdoor the order would create was "too dangerous to build."[96] Indeed,

88. *Id.*

89. McCarthy, *supra* note 21.

90. Richard Winton, *We May Never Know Why the San Bernardino Terrorists Targeted a Christmas Party. Here's What We Do Know*, L.A. TIMES (Dec. 2, 2016, 7:55 AM), http://www.latimes.com/local/lanow/la-me-san-bernardino-attack-20161202-story.html.

91. Government's Ex Parte Application for Order Compelling Apple Inc. to Assist Agents in Search; Memorandum of Points and Authorities at 1-2, In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451M (C.D. Cal. Feb. 16, 2016).

92. *Id.* at 3.

93. *See id*.

94. *See id.*

95. *See* Tracey Lien et al., *Court Order in San Bernardino Case Could Force Apple to Jeopardize Phone Security*, L.A. TIMES (Feb. 17, 2016, 1:54 PM), http://www.latimes.com/local/lanow/la-me-ln-apple-san-bernardino-security-20160217-story.html; Jonathan Chew, *This is Apple's Next Move in Its Fight With the FBI*, FORTUNE, (March 2, 2016), http://fortune.com/2016/03/02/apple-appeal-fbi-iphone.

96. *See* Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, And Opposition to Government's Motion to Compel Assistance at 2, In the Matter

at the same time the government was seeking Apple's assistance in the San Bernardino case, it was also attempting to get the company to unlock at least nine other iPhones in unrelated cases.[97] Apple's CEO Tim Cook signaled that the company intended to fight the issue for as long as it could, and expressed concern that the order was an overreach of government power that would undermine "the very freedoms and liberty" that the government was meant to protect.[98] In response, the government filed a motion to compel, in which it accused Apple of opposing the order as a publicity stunt.[99] Despite these heated words, a little over a month after Apple filed its appeal, the government dropped the issue entirely.[100] The FBI, in cooperation with a third party, had been able to circumvent the iPhone's security and thus no longer needed the order. In a statement the US Attorney, Eileen Decker, was emphatic that the "decision to conclude the litigation was based solely on the fact that, with the assistance of a third party, we are now able to unlock that iPhone without compromising any information in the phone."[101] It was later revealed that the FBI had paid a computer security expert $900,000 to crack the phone's encryption.[102] In April of 2016 the FBI released a further statement where they said they would not submit the vulnerability used to access the phone to the VEP, because it had been discovered by a third party, and the FBI had not purchased "the rights to technical details about how the method functions, or the nature and extent of any vulnerability upon which the method may rely in order to operate."[103] Later attempts by the media to force the FBI to release more detailed information about the vulnerability finally failed in October of 2017, when a federal judge dismissed

---

of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451M (C.D. Cal. Feb. 25, 2016).

97. Eric Lichtblau & Joseph Goldstein, *Apple Faces U.S. Demand to Unlock 9 More iPhones*, N.Y. TIMES (Feb. 23, 2016), https://www.nytimes.com/2016/02/24/technology/justice-department-wants-apple-to-unlock-nine-more-iphones.html?rref=collection%2Fnewseventcollection%2Fapple-fbi-case.

98. *See* Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter/.

99. Kate Knibbs, *Feds Say Apple's Stand Against the FBI Is Just a PR Stunt*, GIZMODO (Feb. 19, 2016, 2:42 PM), https://gizmodo.com/the-doj-is-going-in-hard-on-apple-about-unlocking-that-1760141290.

100. Government's Status Report at 1-2, In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451M (C.D. Cal. Mar. 28, 2016).

101. Joel Rubin et al., *FBI Unlocks San Bernardino Shooter's iPhone and Ends Legal Battle with Apple, for Now*, L.A. TIMES (Mar. 28, 2016, 10:39 PM), http://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html.

102. Matt Novak, *The FBI Paid $900,000 to Unlock the San Bernardino Terrorist's iPhone*, GIZMODO (May 8, 2017, 8:00 AM), https://gizmodo.com/the-fbi-paid-900-000-to-unlock-the-san-bernardino-kill-1795010203.

103. Don Reisinger, *FBI: Sorry, But We're Keeping the iPhone Crack Secret*, FORTUNE (Apr. 27, 2016), http://fortune.com/2016/04/27/fbi-apple-iphone-crack/.

the FOIA lawsuit, upholding the FBI's claim that revealing the identity of the vendor could lead to that entity being attacked and could lead to the unauthorized disclosure of the vulnerability, damaging national security.[104]

The San Bernardino case illuminates not only the debate over backdoors but also the limits of the VEP. Unlike the issues surrounding WannaCry or Heartbleed, where the vulnerabilities remained mostly secret until exploited by bad actors or exposed by whistleblowers, this vulnerability was publicly known and clearly effective—at least effective enough for the government to drop their case against Apple once it became available. Yet, despite knowing there was a potentially dangerous and exploitable error in the iPhone's encryption software, the FBI was able to stop the vulnerability from even entering the VEP.

IV. Proposed Solutions—The New VEP, Legislation, and Beyond

Given the myriad of competing interests and agendas involved in the debate over vulnerability disclosure (as well as the debate over government backdoors), any proposal to move the conversation forward faces a difficult fight. Any solution has to appease both government agencies looking to preserve investigative and tactical capabilities and companies seeking to protect their products and customers. Given how central computer systems are to the functioning of society, vulnerabilities will remain dangerous and valuable for the foreseeable future, making any resolution that even partially satisfies the parties involved something worth pursuing. In recent years there have been proposals from many corners, including the Executive Branch, Congress, and technology policy advocates from both civil society and industry, and an evaluation of these proposals is vital in any attempt to plot a future course.

A. *A New VEP*

As part of the fallout from the Heartbleed incident, some security researchers raised the alarm about the need for public disclosure of vulnerabilities discovered by the government. After reviewing various government operations that exploited vulnerabilities, it became clear to them the government was sitting on a worrisome stockpile—why else would the government be willing to "burn" four zero-day vulnerabilities in a single mission, as was done in the Stuxnet attack, a joint US/Israeli cyber assault on the Iranian nuclear program?[105] Once used, zero-day vulnerabilities would most likely become public and, therefore, patched in short order, so it seemed unlikely the government would expend them so readily if its stock-

104. *See* Associated Press v. FBI, 265 F. Supp. 3d 82, 94 (D.D.C. 2017).
105. *See* Schneier, *supra* note 1.

pile was extremely limited.[106] Yet the government denied the existence of any stockpile and maintained that not disclosing a vulnerability was the exception, not the rule for the government.[107] In an interview with *Wired*, National Security Council cybersecurity coordinator Michael Daniel avoided directly answering the question of whether that default rule extended to zero-day vulnerabilities discovered by third parties, saying that if the government thought it was a significant threat, it would move to get the vulnerability patched.[108]

In 2017, in the wake of the 2010 VEP document's release and in response to the WannaCry attack, voices in civil society and the technology industry launched another round of calls for further action on vulnerabilities. Industry players like Mozilla[109] and Microsoft,[110] both of which had seen the negative aspects of government use of vulnerabilities, cited the WannaCry attack as impetus for changes in policy. Microsoft went as far as to call for a "Digital Geneva Convention" that would bind world governments to report vulnerabilities.[111] Similar calls for reform came from civil society groups like EFF, which pushed for Congressional action (discussed further below).[112] In October of 2017 the White House Cybersecurity Coordinator Rob Joyce announced that the White House was preparing to release new information on the VEP, leading to the release of an updated VEP on November 15, 2017.[113]

The updated VEP provides greater detail on the considerations that go into cases where law enforcement or intelligence interests override the benefits of disclosure. The new policy includes a series of "core considerations" that are supplied to help decision makers "weigh the benefits to U.S. national security and national interest" when deciding whether or not to disclose or rescript knowledge of a vulnerability. These considerations are:

---

106. *See id.*

107. Kim Zetter, *U.S. Gov Insists It Doesn't Stockpile Zero-Day Exploits to Hack Enemies*, WIRED (Nov. 17, 2014, 6:30 AM), https://www.wired.com/2014/11/michael-daniel-no-zero-day-stockpile/.

108. *Se id.*

109. *See* Denelle Dixon, *WannaCry is a Cry for VEP Reform*, MOZILLA BLOG (May 15, 2017), https://blog.mozilla.org/blog/2017/05/15/wannacry-cry-vep-reform/.

110. Smith, *supra* note 54.

111. Brad Smith, *The Need for a Digital Geneva Convention*, MICROSOFT: MICROSOFT ON THE ISSUES (Feb. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001gnysbhjsod01z7q11hvz0xg2d.

112. *See, e.g.*, Andrew Crocker & Kate Tummarello, *Congress' Imperfect Start to Addressing Vulnerabilities*, EFF (May 24, 2017), https://www.eff.org/deeplinks/2017/05/congress-imperfect-start-addressing-vulnerabilities.

113. 2017 VEP, *supra* note 17; Michelle Richardson & Mike Godwin, *What the White House Needs to Disclose About Its Process for Revealing Cybersecurity Vulnerabilities*, JUST SECURITY (Nov. 2, 2017), https://www.justsecurity.org/46647/white-house-disclose-process-revealing-cybersecurity-vulnerabilities/.

PART I—DEFENSIVE EQUITY CONSIDERATIONS

1. A. Threat Considerations

- Where is the product used? How widely is it used?
- How broad is the range of products or versions affected?
- Are threat actors likely to exploit this vulnerability, if it were known to them?

1. B. Vulnerability Considerations

- What access must a threat actor possess to exploit this vulnerability?
- Is exploitation of this vulnerability alone sufficient to cause harm?
- How likely is it that threat actors will discover or acquire knowledge of this vulnerability?

1. C. Impact Considerations

- How much do users rely on the security of the product?
- How severe is the vulnerability? What are the potential consequences of the exploitation of this vulnerability?
- What access or benefit does a threat actor gain by exploiting this vulnerability?
- What is the likelihood that adversaries will reverse engineer a patch, discover the vulnerability and use it against unpatched systems?
- Will enough USG [United States Government] information systems, U.S. businesses and/or consumers actually install the patch to offset the harm to security caused by educating attackers about the vulnerability?

1. D. Mitigation Considerations

- Can the product be configured to mitigate this vulnerability? Do other mechanisms exist to mitigate the risks from this vulnerability?
- Are impacts of this vulnerability mitigated by existing best - practice guidance, standard configurations, or security practices?
- If the vulnerability is disclosed, how likely is it that the vendor or another entity will develop and release a patch or update that effectively mitigates it?
- If a patch or update is released, how likely is it to be applied to vulnerable systems? How soon? What percentage of vulnerable

systems will remain forever unpatched or unpatched for more than a year after the patch is released?

- Can exploitation of this vulnerability by threat actors be detected by USG or other members of the defensive community?

PART 2—INTELLIGENCE, LAW ENFORCEMENT, AND OPERATIONAL EQUITY CONSIDERATIONS

2. A. Operational Value Considerations

- Can this vulnerability be exploited to support intelligence collection, cyber operations, or law enforcement evidence collection?
- What is the demonstrated value of this vulnerability for intelligence collection, cyber operations, and/or law enforcement evidence collection?
- What is its potential (future) value?
- What is the operational effectiveness of this vulnerability?

2. B. Operational Impact Considerations

- Does exploitation of this vulnerability provide specialized operational value against cyber threat actors or their operations? Against high-priority National Intelligence Priorities Framework (NIPF) or military targets? For protection of warfighters or civilians?
- Do alternative means exist to realize the operational benefits of exploiting this vulnerability?
- Would disclosing this vulnerability reveal any intelligence sources or methods?

PART 3—COMMERCIAL EQUITY CONSIDERATIONS

- If USG knowledge of this vulnerability were to be revealed, what risks could that pose for USG relationships with industry?

PART 4—INTERNATIONAL PARTNERSHIP EQUITY CONSIDERATIONS

- If USG knowledge of this vulnerability were to be revealed, what risks could that pose for USG international relations?[114]

This list is much more extensive than what was included in the White House's 2014 statement, and the new VEP has received positive, if re-

114. *Id.*

strained, reviews from groups like the ACLU.[115] The new policy still exempts vulnerabilities that are subject to non-disclosure agreements—which are common in cases dealing with third-party discovered vulnerabilities (as in the San Bernardino case).[116] Likewise, the Equities Review Board, while including civilian departments like the Departments of State, Treasury, and Commerce, excludes both the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC).[117] This is notable, given the FCC's role in regulating the nation's telecommunications infrastructure and the FTC's mission to protect privacy and data security.[118] Given the increasing attention paid to connected vehicles, the Department of Transportation would seem to be a natural fit for a permanent seat on the board as well.[119] Yet even with these criticisms, some of the changes to the VEP were close to those requested by civil society organizations,[120] though time will tell if the VEP can deliver the outcomes those organizations desire when put into practice.

B. *Congressional Fixes*

Both the previous VEP and its 2017 version are products of the executive branch. Yet after the WannaCry attack, Congress began to take interest in the process—starting with the "Protect our Ability to Counter Hacking Act" (PATCH Act).[121] The PATCH Act would codify the VEP process and the Equities Review Board (ERB).[122] Unlike the 2017 VEP, the act would put the Secretary of Homeland Security, rather than the Director of the NSA, in charge of the ERB, though it only gives seats to the Secretaries of State, Treasury, and Energy, as well as to representatives of the FTC, on an as-needed basis.[123] The PATCH Act would also place the ERB under yearly Congressional oversight, via a yearly report to the relevant committees, and require unclassified public versions of that report to be released. The

115. Jennifer Stisa Granick, *Trump's New Cybersecurity Rules Are Better Than Obama's*, ACLU: FREE FUTURE (Nov. 27, 2017, 9:45 AM), https://www.aclu.org/blog/privacy-technology/internet-privacy/trumps-new-cybersecurity-rules-are-better-obamas.

116. Andrew Crocker, *Time Will Tell if the New Vulnerable Is a Step Forward for Transparency*, EFF (Nov. 16, 2017), https://www.eff.org/deeplinks/2017/11/time-will-tell-if-new-vulnerabilities-equities-process-step-forward-transparency.

117. 2017 VEP, *supra* note 17, at 3.

118. *See* Granick, *supra* note 115.

119. *See* Rob Toews, *The Biggest Threat Facing Connected Autonomous Vehicles is Cybersecurity*, TECHCRUNCH (Aug. 25, 2016), https://techcrunch.com/2016/08/25/the-biggest-threat-facing-connected-autonomous-vehicles-is-cybersecurity/.

120. Richardson & Godwin, *supra* note 113.

121. Press Release, Office of Senator Brian Schatz, Bipartisan, Bicameral Lawmakers Introduce Bill to Enhance Cybersecurity, Promote Transparency (May 17, 2017), https://www.schatz.senate.gov/press-releases/bipartisan-bicameral-lawmakers-introduce-bill-to-enhance-cybersecurity-promote-transparency.

122. PATCH Act of 2017, S. 1157, 115th Cong. (2017).

123. *Id.* at § 2(c)(1)-(2).

PATCH Act also gained support from Mozilla, who found that the act included many of the key reforms to the VEP system that it had been pushing for.[124]

While civil society organizations and industry were encouraged by the introduction of the PATCH Act, they also had reservations. The EFF took exception to the exclusion from the VEP of classified vulnerabilities that are "inappropriately released to the public," which would allow the government to keep vulnerabilities like Heartbleed secret even after a public leak.[125] Further criticism was directed at the fact that, like the 2017 VEP, the PATCH Act also excluded third-party discovered vulnerabilities.[126] Despite the attention paid to the act by industry and advocates, the Act, though introduced in May of 2017, has yet to move any further through the legislative process.[127]

V. A Hybrid Solution to the Vulnerability Disclosure Issue

Given the flurry of activity and debate over vulnerability disclosures over the past few years, there are a number of viable solutions to the issue that could be attractive to industry, government, and advocates alike. However, given the diversity in thought among those groups, and the differing weight they give to considerations of national security, keeping private, governmental, and civil society actors engaged in active policy-making, it becomes difficult to create an effective final policy. A solid foundation for the new vulnerability disclosure schema can be found in the 2017 VEP and the PATCH Act. As discussed in Part III, both of these received a mix of praise and criticism from players in the technology policy world, and thus any new system derived from the PATCH Act or the 2017 VEP will be a creature of compromise.

The PATCH Act represents the most important aspect of any VEP reform—the codification of the process into law. Rather than depending on the Executive Branch to write its own rules for vulnerabilities, Congress needs to be involved. The PATCH Act's oversight requirements of yearly reports, including public reports, will ensure the process is kept under a watchful eye. A useful addition, first proposed in a 2016 paper by two former Obama Administration cybersecurity officers and included in the PATCH Act, is further oversight by the Inspector General of the given department charged with chairing the ERB, along with expanding the mission of the Privacy and Civil Liberties Oversight Board (PCLOB), which is already tasked with reviewing the actions of intelligence agencies, to include

124. Dixon, *supra* note 73.

125. *See* Crocker & Tummarello, *supra* note 112.

126. *Id.*

127. *Actions Overview S.1157 — 115th Congress (2017-2018)*, CONGRESS.GOV, https://www.congress.gov/bill/115th-congress/senate-bill/1157/actions?q=%7B%22search%22%3A%5B%22s+1157%22%5D%7D&r=1 (last visited Dec. 20, 2017).

oversight of the VEP.[128] Given the sensitive nature of the VEP's operations, oversight by a group like PCLOB allows for a level of operational secrecy while still ensuring independent oversight.

The 2017 VEP and the PATCH Act each structure the ERB differently, and a hybrid of the two is needed to better address current differences. The 2017 VEP's membership list should serve as the basis, as it includes important civilian departments like State, Treasury, and Commerce. Additionally, representatives from the FCC and FTC should be granted permanent seats on the board, given the missions and expertise of those agencies. The PATCH Act's transfer of the Executive Secretariat from the NSA to the Department of Homeland Security (DHS) is a vital change from the VEP, as DHS has significant experience and expertise in coordinated vulnerability disclosure programs (which evolved from the work of CERT-CC, mentioned above).[129] This also takes control of the board out of the hands of an agency dedicated to intelligence gathering and puts it into the hands of DHS, an agency tasked with a wider portfolio of interests.

While it is not necessary to codify the exact criteria for evaluating vulnerabilities, the equity considerations found in the 2017 VEP should provide the base of the ERB's thought process. Those considerations touch on a wide swath of the issues the ERB will have to face, including:

- Details on the product in question—the extent of its use and who might exploit the vulnerability if it became known;
- How likely it is that other actors will discover the vulnerability and exploit it;
- The severity of the threat and the potential to mitigate the vulnerability;
- The value of the vulnerability as a law enforcement or intelligence tool; and
- The effect the revelation of US government knowledge of the vulnerability will have on US government relationships with industry and international relationships.

These are deeply important questions in any discussion of vulnerability disclosure and need to be part of any hybrid VEP/PATCH system.

Controls over any stockpiling of vulnerabilities will also be a necessary component of a hybrid solution. Both the 2017 VEP and the PATCH Act provide for periodic review of those vulnerabilities that are chosen to be kept secret—with the VEP adopting yearly review. Yet both the 2017 VEP and the PATCH Act allow the government to circumvent the VEP process

128. SCHWARTZ & KNAKE, *supra* note 4, at 16.

129. Dixon, *supra* note 73; Press Release, Office of Senator Brian Schatz, Bipartisan, Bicameral Lawmakers Introduce Bill to Enhance Cybersecurity, Promote Transparency (May 17, 2017), https://www.schatz.senate.gov/press-releases/bipartisan-bicameral-lawmakers-introduce-bill-to-enhance-cybersecurity-promote-transparency.

when the vulnerability is subject to a non-disclosure agreement (as in San Bernardino) or when the vulnerability's existence is made public via a leak of information (as in WannaCry). These provisions must be eliminated from the proposed hybrid solution. When a third party approaches the government with a vulnerability, the government should be compelled to run that vulnerability through the VEP. A strong VEP has the potential to increase confidence in the government's ability to responsibly handle vulnerabilities, and allowing it to be circumvented via non-disclosure agreements derails that progress. Likewise, once a vulnerability is made public via a leak or a cyber-attack, the ERB should move to release what information they have to any government agency working to repair the damage or reveal the vulnerability to private companies whose products are under threat. It is clear from the lessons of Heartbleed and WannaCry that continued government secrecy after a vulnerability becomes public does not end well for the government, especially in the court of public opinion.

Any move to reform vulnerability disclosures would be a complicated process involving many more interests and actors than those discussed above. But a hybrid of the 2017 VEP and the PATCH Act has the opportunity to bridge the gap between government and private interests, and allow for greater public confidence in the vulnerability disclosure process. While the PATCH Act has not made progress in the current Congress, the implementation of the new VEP gives supporters of vulnerability disclosure reform another opportunity to raise awareness of the issue and push for further changes.

C. *Other Considerations*

While not directly implicated in the VEP or PATCH Act, there are two additional areas of interest that could prove useful as leverage in a debate over vulnerability disclosure reform. The first is the use of vulnerabilities in criminal cases, as in the Playpen investigation. In *Michaud*, the government effectively decided that a set of software vulnerabilities were more important than the successful prosecution of defendants who had been found to be in possession of child pornography. In a 2016 article, Susan Hennessey, an expert in national security law and former NSA attorney, along with Nicholas Weaver, a computer security expert and UC Berkeley lecturer, proposed a new judicial framework for NITs that included *in camera* review of classified information.[130] Hennessey and Weaver's proposal is worthy of deeper investigation in a different discussion, but for the purposes of vulnerability disclosure reform, it presents an opportunity to clear up the issues surrounding NIT cases, retaining them as a viable law enforcement tool,

130. Hennessey & Weaver, *supra* note 74.

which could entice law enforcement agencies to support reforms to the VEP which they may otherwise not favor.[131]

The second area of potential leverage to build support for vulnerability disclosure is the reform of the laws that govern security research. Currently, third-party researchers, be they individual white hat hackers or university-sponsored teams of students, have the potential to run afoul of the CFAA, which has never been amended to give a good faith research exception to its prohibition on accessing a computer "without authorization."[132] Such a change would further open up the world of vulnerability research and give both companies and the government access to new sources of vulnerability discovery. Laws like the Digital Millennium Copyright Act (DMCA) also have the potential to derail good faith security research, when they bar circumventing things like access controls on devices, even by the owners of said devices.[133] Changes to these laws can help protect consumers and could even take some pressure off of the government to reveal every vulnerability–since there will be an army of researchers also looking for them.

CONCLUSION

In modern society, software vulnerabilities have become a fact of life. Data breaches, malware attacks, and the like have become common news stories, and often have real-world implications.[134] It is easy to understand why law enforcement and intelligence agencies would want to exploit these vulnerabilities for their own missions, but such actions will always come at a cost. The government's ability to hide vulnerabilities from developers is a threat not only to the security of American citizens, but the security of millions of users across the world. Reform of the vulnerability disclosure scheme is the best opportunity for the government to lead on this issue—and by bringing advocates and industry into the fold on designing a new system they can preserve national security utility without sacrificing the best interest of the public.

---

131. Given the complicated technological issues in play, in camera review of technological investigative techniques like an NIT would require input from technology experts to insure judges were given an impartial view on how the technique works. This could either occur at the time of review or as regular training for judges hearing criminal cases (at least at the Federal level, where law enforcement had the resources to use such techniques).

132. *See* CENTER FOR DEMOCRACY & TECHNOLOGY, "THE CYBER:" HARD QUESTIONS IN THE WORLD OF COMPUTER SECURITY RESEARCH 7-8, 12 (2017), https://cdt.org/files/2017/03/2017-03-23-Security-Research.pdf.

133. Joseph Lorenzo Hall, *"The Cyber" Part I: Legal Impediments to Security Research*, CDT (Mar. 31, 2017), https://cdt.org/blog/the-cyber-part-i-legal-impediments-to-security-research/.

134. Dan Goodin, *Why the Equifax Breach is Very Possibly the Worst Leak of Personal Info Ever*, ARS TECHNICA (Sept. 8, 2017, 2:09 AM), https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/.