NEW AMERICA
CYBERSECURITY INITIATIVE
OPEN TECHNOLOGY INSTITUTE

ANDI WILSON, ROSS SCHULMAN, KEVIN BANKSTON, AND TREY HERR

BUGS IN THE SYSTEM

A Primer on the Software Vulnerability Ecosystem and its Policy Implications

JULY 2016

About the Authors

Andi Wilson is a policy analyst at New America's Open Technology Institute, where she researches and writes about the relationship between technology and policy. With a specific focus on cybersecurity, Andi is currently working on issues including encryption, vulnerabilities equities, surveillance, and internet freedom.

Ross Schulman is a co-director of the Cybersecurity Initiative and senior policy counsel at New America's Open Technology Institute, where he focuses on cybersecurity, encryption, surveillance, and Internet governance. Prior to joining OTI, Ross worked for Google in Mountain View, California. Ross has also worked at the Computer and Communications Industry Association, the Center for Democracy and Technology, and on Capitol Hill for Senators Wyden and Feingold.

Kevin Bankston is the Director of New America's Open Technology Institute, where he works in the public interest to promote policy and regulatory reforms to strengthen communities by supporting open communications networks, platforms, and technologies. He previously served as OTI's Policy Director.

Trey Herr is a fellow with the Belfer Center's Cyber Security Project at the Harvard Kennedy School. He focuses on trends in state developed malicious software, the structure of criminal markets for malware components, and the proliferation of malware. Trey is also a non-resident fellow with New America's Cybersecurity Initiative.

Acknowledgments

The authors would like to thank Chris Riley, Joe Hall, Katie Moussouris and our other external reviewers for their input and comments on an earlier version of this paper. This paper does not necessarily reflect their views. We would also like to thank Donna Wentworth for her many valuable contributions to the paper. As well, we appreciate the extensive help of New America's staff and fellows, especially Ian Wallace, Jordan McCarthy, Liz Woolery, Robert Morgus, and Robyn Greene.

About New America

New America is committed to renewing American politics, prosperity, and purpose in the Digital Age. We generate big ideas, bridge the gap between technology and policy, and curate broad public conversation. We combine the best of a policy research institute, technology laboratory, public forum, media platform, and a venture capital fund for ideas. We are a distinctive community of thinkers, writers, researchers, technologists, and community activists who believe deeply in the possibility of American renewal.

Find out more at **newamerica.org/our-story**.

About the Cybersecurity Initiative

The Internet has connected us. Yet the policies and debates that surround the security of our networks are too often disconnected, disjointed, and stuck in an unsuccessful status quo. This is what New America's Cybersecurity Initiative is designed to address. Working across our International Security program and the Open Technology Institute, we believe that it takes a wider network to face the multitude of diverse security issues. We engage across organizations, issue areas, professional fields, and business sectors. And through events, writing and research, our aim is to help improve cybersecurity in ways that work—for the countries, for companies and for individuals.

Our work is made possible through the generous support of the William and Flora Hewlett Foundation, the Arizona State University, Microsoft Corporation, Symantec Inc., The Home Depot, Endgame Inc., and Facebook.

About the Open Technology Institute

The Open Technology Institute (OTI) works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

Contents

EXECUTIVE SUMMARY

In recent years, a seemingly endless string of massive data breaches in both the private and public sectors have been front-page news. Whether the target is a company like Sony or a government agency like OPM, such breaches are very often made possible by a software vulnerability—a "bug" in the system—that was unknown or left unaddressed by the target or its software vendor.

The existence of such vulnerabilities—or "vulns" for short—is unavoidable. Software is complex and humans are fallible, so vulnerabilities are bound to occur. Much of cybersecurity can be reduced to a constant race between the software developers and security experts trying to discover and patch vulnerabilities, and the attackers seeking to uncover and exploit those vulnerabilities. The question for policymakers is, what can they do to help speed the discovery and patching of vulnerabilities so that our computer systems—and therefore our economic stability, our national security, and consumers' privacy—are safer? This paper is intended to be a primer on the vulnerability ecosystem for policymakers and advocates seeking to answer that question, describing what vulns are, who discovers them, who buys them, how and when they do (or don't) get patched, and why.

There is a wide range of actors seeking to discover security flaws in software, whether to fix them, exploit them, or sell them to someone else who will fix or exploit them. These bug-hunters range from independent researchers, to small academic teams or security firms, to large tech companies working to improve their products, or even governments—including our own government, and other much less rights-respecting states—seeking to use these flaws for law enforcement or intelligence investigations. After finding a vulnerability, the discoverer has three basic options: not disclosing the vulnerability to the public or the software vendor; fully disclosing the vuln to the public, which in some cases may be the best way to get it patched but in others may leave users of the software dangerously exposed; and partial or "responsible" disclosure to the vendor so that they can fix the bug before it becomes public. Partial disclosure is often preferred because it can sometimes take months for a vendor to fix their product, and even longer for all the affected users to update their software to patch the security hole.

Confusing the issue of disclosure is the fact that there is a range of laws—such as the Computer Fraud and Abuse Act, the Digital Millennium Copyright Act, and the Electronic Communications Privacy Act—that by their broad and vague terms arguably criminalize and create civil penalties for actions that security researchers routinely engage in while conducting legitimate security research. Unless reformed, these laws will continue to chill researchers' disclosure of critical vulnerabilities, for

fear that they will be sued or even thrown in jail.

Another disincentive to researchers' disclosure of vulnerabilities so that they can be patched is the existence of open markets for vulnerabilities, where researchers can often get top dollar from criminal networks or governments seeking to exploit those vulnerabilities, or from intermediary agents who buy from researchers and then resell to criminals and states. Companies have responded by creating innovative vulnerability reward programs (VRPs), including "bug bounty" programs where they pay rewards for bugs that are submitted. Some of these programs also seek to reduce the legal chill on researchers by promising not to sue those who submit through these programs. It is sometimes difficult for these programs to compete with the much more lucrative open market, but they give researchers who want to help improve cybersecurity—and perhaps get a little cash or recognition for their discovery—a legitimate avenue to pursue.

Researchers often have a range of incentives to disclose their discoveries to someone, whether to the vendor, the public, or a buyer on the market. Governments, on the other hand, often have an incentive to withhold the vulns they buy or discover. Although they may want to keep the public and their own systems safe from bad guys exploiting those vulnerabilities, they also want to make use of them for a variety of purposes, from law enforcement to foreign intelligence surveillance, and the longer they are secret and unpatched, the longer they are useful. Governments have to weigh the security value of disclosure versus the benefit of stockpiling and using vulnerabilities for their own purposes.

In conclusion, we offer five initial policy recommendations to ensure that more vulnerabilities are discovered and patched sooner: (1) The U.S. government should minimize its participation in the vulnerability market, since it is the largest buyer in a market that discourages researchers from disclosing vulns to be patched; (2) The U.S. government should establish strong, clear procedures for government disclosure of the vulnerabilities it buys or discovers, with a heavy presumption toward disclosure; (3) Congress should establish clear rules of the road for government hacking in order to better protect cybersecurity and civil liberties; (4) Government and industry should support bug bounty programs as an alternative to the vulnerabilities market and investigate other innovative ways to foster the disclosure and prompt patching of vulnerabilities; and (5) Congress should reform computer crime and copyright laws, and agencies should modify their application of such laws, to reduce the legal chill on legitimate security research.

> **Much of cybersecurity can be reduced to a constant race between the software developers and security experts trying to discover and patch vulnerabilities, and the attackers seeking to uncover and exploit those vulnerabilities.**

INTRODUCTION

In recent years, there have been a seemingly endless string of massive data breaches in both the private and public sectors, resulting in the theft of vast amounts of private data.[1] Whether the breach target is a major company like Sony,[2] Anthem,[3] or Ashley Madison,[4] or a government agency like the Office of Personnel Management,[5] the IRS,[6] or the Joint Chiefs of Staff,[7] such breaches are very often made possible by a software vulnerability—a "bug" in the system—that was unknown or left unaddressed by the target or its software vendor. Although some high-profile hacks involve previously unknown or "zero-day" vulnerabilities,[8] a recent study concluded that most hacking attacks in 2015 exploited known vulnerabilities that the targets had failed to address despite fixes having been available for months or even years.[9] Failures like these are so widespread that it's been said that there are two types of organizations: those who know that they have been hacked, and those who just haven't discovered it yet.

Of course, the existence of such vulnerabilities—or "vulns" for short—is unavoidable. Software is complex and humans are fallible, so vulnerabilities are bound to occur. Which raises the question: what policies will best ensure that those vulnerabilities are discovered, disclosed to the software maker, and fixed (or "patched") as soon as possible? Before we can answer that question, we must first understand the vulnerability ecosystem: what vulns are, who discovers them, who buys and sells information about them and why, what they are used for, and what laws and policies currently impact their discovery and/or use.

The need for such understanding has become even more pressing as policy issues related to software vulnerabilities are now front page news. In just the past few months, for example, the FBI has had to defend its purchase of an iPhone hacking tool and its subsequent decision not to disclose that tool to Apple or the White House;[10] Mozilla has gone to court to force the Justice Department to disclose a Firefox browser vulnerability that investigators exploited in a string of child pornography investigations;[11] the U.S. government has gone back to the drawing board on an international agreement intended to keep hacking tools out of the hands of repressive regimes;[12] the FCC and the FTC have teamed up to investigate why many smartphone vulnerabilities aren't patched until it's too late,[13] and Facebook has paid a $10,000 "bug bounty" to a 10-year-old child for discovering a vulnerability in its Instagram app.[14]

This paper is a primer to help policymakers better understand the vulnerability ecosystem and the range of policy questions that it raises. It explains how vulnerabilities are discovered, the ways in which they can be disclosed, and the incentives and disincentives for, and legal constraints on, the people who look for them. It examines how various groups, both public and private, interact with the marketplace that has evolved around information about vulnerabilities, and explores strategies for ensuring that they are quickly disclosed and fixed, thereby protecting economic stability, national security, and consumer privacy.

In the future, supported by the background laid out in this paper, we will more deeply explore specific policy questions around vulnerabilities, such as: Should the government ever stockpile the vulnerabilities it learns about for its own use, and if so, how should it decide which vulns to keep secret and which to disclose? How should we regulate the government's use of vulnerabilities, or the global vulnerability marketplace as a whole? How can we reform the laws that are currently discouraging security researchers from discovering and disclosing vulnerabilities, so that more vulns can be found and fixed faster?

These are all complex questions, which we'll get to in due time. But let's start with the basics: what exactly is a vulnerability?

WHAT ARE VULNERABILITIES?

Vulnerabilities are weaknesses in software that enable an attacker to compromise the integrity, availability, or confidentiality of the software, putting users and networks at risk.[15] Much of cybersecurity can be reduced to a constant race between the software developers and security experts trying to discover and patch vulnerabilities, and the attackers—criminals, states, hacktivists, or others—seeking to uncover and exploit those vulnerabilities. Attackers can use vulnerabilities to force critical programs to crash, to compel monitoring utilities to report and act on incorrect information, to extract authentication credentials and personal information from databases, or even to infiltrate and take operational control over entire networks.

> **Vulnerabilities are weaknesses in software that enable an attacker to compromise the integrity, availability, or confidentiality of the software, putting users and networks at risk.**

Vulnerabilities can be introduced into software in a variety of ways. The majority of vulnerabilities originate from honest mistakes: they are caused by simple typos in software code,[16] unforeseen interactions among complex subcomponents of a larger system, or a failure to protect a program against an unforeseen misuse.[17] Still others are actively introduced by software developers for later exploitation. These deliberate vulnerabilities are generally known as "backdoors."[18]

Definitions

Vulnerability: A feature or flaw in a piece of software which allows for unintended operations to be performed by a third party.

Exploit: Code written to take advantage of a vulnerability and demonstrated through a proof of concept. An exploit is a component of malware and allows it to propagate into and run routines on vulnerable computers.

Malware: A category of malicious code that includes hostile or intrusive software such as viruses, worms, Trojan horse programs, ransomware, spyware, adware, and scareware.

Zero-day: A vulnerability that has not yet been disclosed, either publicly or privately, to the vendor, and therefore the vendor has had "zero days" during which a fix could be developed. Publishing such a vulnerability is often referred to as "dropping" a zero-day.

Backdoor: A vulnerability deliberately introduced either by the vendor responsible for the software or a malicious actor with access to the code. Intended to be used later to compromise systems.

If vulnerabilities can be described as weaknesses in code, "exploits" are programs that seek to demonstrate those weaknesses or take advantage of them.[19] The former category of exploit—the proof of concept intended merely to illustrate a vulnerability—is a common tool of legitimate security researchers. The latter category of exploit—paired with software used for malicious purposes—is called "malware", and comes in a wide variety of types.[20] Some malware programs are used to extract potentially sensitive information about users, while others give external actors unfettered control over the affected system.[21] "Ransomware" is a type of malware that attackers use to lock users out of their computers and force them to pay in exchange for decrypting their files.[22] In an attack called "clickjacking,"[23] attackers hide malware in legitimate websites so that, when users click on infected links, the criminals can attack their computers.[24] Intruders can also use vulnerabilities to insert a "keylogger"[25] in a computer so they can record every keystroke, allowing them to steal the user's logins, passwords, and credit card information.[26]

Vulnerabilities that enable these types of attacks are clearly a boon for computer criminals, but as we explain below, they're also exploited by other parties—including governments[27]—and discovering them represents an opportunity of a different sort for security researchers.

WHO DISCOVERS VULNERABILITIES?

In the early days of the internet, security was considered to be a mostly theoretical problem and wasn't a top priority for software vendors—until the Morris Worm of 1998.[28] Coded by a grad student motivated more by curiosity than malice, this early example of malware was the first to have such a widespread impact—it infected 10 percent of all internet-connected computers at the time—that it made national news and resulted in the first conviction under the Computer Fraud and Abuse Act of 1986.[29]

In the intervening decades, the computer security community and industry has exploded. Today, there are countless information security companies or companies with their own information security divisions, public and private research institutions, and expert and amateur independent researchers hunting for software vulnerabilities. Whether motivated by money, prestige, curiosity, or a desire for a more secure digital environment, those who discover vulns—whom we will call "discoverers"—can be roughly categorized into four groups:

1. **Independent agents** (whether professional security researchers, academics, or amateurs), such as the independent researcher Space Rogue,[30] formerly of the renowned security group Lopht,[31] and Charlie Miller who discovered vulnerabilities in the Jeep Grand Cherokee.[32]
2. **Small teams** (mostly academic labs and small security firms), such as the University of Toronto's Citizen Lab[33] or security research company Rapid7;[34]
3. **Larger teams** within major technology companies (like Google[35] or Microsoft[36]);
4. **Governments** (including branches within law enforcement and intelligence organizations, like the FBI[37]and the NSA[38] in the U.S. and the GCHQ[39] in the U.K., that cultivate expertise in vulnerability discovery, defense, and deployment).

Although companies and governments are the well-funded powerhouses conducting security research, individuals and smaller actors also play a critical role, whether bringing to light vulnerabilities

> **There are countless information security companies or companies with their own information security divisions, public and private research institutions, and expert and amateur independent researchers hunting for software vulnerabilities.**

through independent security audits;[40] penetration testing or "pen testing"[41] which is an attack on a computer system or network to search for weaknesses; hacking competitions, where people compete to find vulnerabilities;[42] or so-called bug bounty programs, through which organizations offer financial rewards to the researchers who find and disclose vulnerabilities.[43]

Regardless of method or motivation, finding a vulnerability often requires a great deal of skill, effort, and time. Some vulnerabilities are much easier to find than others, while some vulnerabilities remain undiscovered for years or decades. The infamous Heartbleed bug, for example, was not discovered for over two years,[44] and the FREAK bug discovered last year was over a decade old.[45]

Of course, not everyone looking for vulnerabilities is doing so to secure and defend systems. Not only are there criminals seeking to exploit vulnerabilities to steal valuable information, there are also governments—both allies and enemies, rights-respecting and rights-repressing—seeking to exploit vulnerabilities for their own purposes, including damaging opponents' vulnerable infrastructure and conducting surveillance. Furthermore, there are people seeking to discover vulnerabilities simply so they can sell them, regardless of whether their discovery will be used to patch the vulnerability or exploit it.[46]

Hats and "Hackers"

While the current usage tends to focus on criminal activities, the term "hacker" has a much broader and less tainted meaning. It simply refers to an expert in a given system or systems—especially an expert in computers and programming—who is driven by curiosity and a desire for information to figure out how things work, especially by experimenting to find the ways that systems can unexpectedly fail or can be used in unforeseen ways. Whether a hacker is "good" or "bad" depends on the metaphorical "hat" they're wearing, much like in old Western movies.

White Hat Hackers test the security of computer systems for legal purposes, usually with authorization and usually to find vulnerabilities in these networks and help to secure them against malicious use. White Hats can work for vendors, or work as independent security researchers, testing the vulnerabilities they find and reporting them so that they can be patched.

Black Hat Hackers use their skills for destructive purposes, breaking into systems for malicious reasons. Black Hats often work for or sell vulnerabilities directly to criminal organizations or repressive governments. The goal is to make money, to disrupt systems, or to destroy or steal confidential data.

Gray Hat Hackers are somewhere in between Black Hats and White Hats. Although they hack into systems without authorization, they are more often motivated by mere curiosity or an activist cause rather than malice. They may also offer to disclose the vulnerability that they found to the system's administrators, and to fix it, for a fee (which for some looks and feels a lot like blackmail). Gray Hats often claim that they only sell vulnerabilities to "good actors," like intermediaries who engage with legitimate governments or vendors. However, the difference between good and bad actors in this context is often ambiguous, and there is always a possibility that vulnerabilities will be resold to bad actors.

WHAT ARE EXPLOITS AND HOW ARE THEY USED?

Exploits are small software programs written to take advantage of a vulnerability. While exploits are necessary to build malware, they are not malware in and of themselves. When security researchers find a vulnerability, for instance, they may write a "proof-of-concept" exploit to demonstrate that the flaw exists so that it can be patched. For the malicious hacker, however, an exploit can serve as the means to deploy malware.

Anything that can hold or transmit data can be used to propagate malware. For example, an attacker could use an email attachment, compromised website, or USB memory stick to distribute malware. Or an attacker could use an exploit developed to take advantage of a vulnerability in a common piece of software, such as a web browser. In that case, the exploit allows the hacker to open the door for the injection of a piece of malicious code in Internet Explorer, but does not achieve anything malicious by itself.

Just as security research has evolved from the early days of the internet, so too have the uses and market for exploits. Once they were simply objects of curiosity or tools for mischief, but exploits today are in-demand commodities with with quoted prices rising into the hundreds of thousands of dollars.[47] Increasingly, security freelancers and companies such as Hacking Team[48] and Vupen[49] are discovering and selling vulnerabilities and exploits to a wide range of government actors across the world, both savory and unsavory.[50] In addition to such gray market sales to militaries, spies, and police, there is also a growing black market for sales to criminals and criminal networks.[51] Through these rapidly developing markets, buyers can purchase individual exploits and payloads—the components of malware delivered via the exploit that actually execute a malicious activity[52]—as well as "exploit kits," a combination of components that are packaged together and then sold or rented to customers.

In contrast to those who are selling such hacking tools, there is a growing community of security researchers eager to disclose the vulnerabilities that they discover, whether to the software vendor or the public, so that they will be patched.

HOW ARE VULNERABILITIES DISCLOSED SO THEY CAN BE PATCHED?

To disclose a vulnerability is to share information about its existence or exploitation with another actor. Since vulnerabilities allow systems to be manipulated by third parties, they expose software users to security risks, and often quite serious ones. For this reason, there is pressure on those who discover vulnerabilities to disclose them in ways that will get them patched quickly while minimizing exposure of the vulns to those who might exploit them before they are patched. Not everyone who finds a vulnerability has the same interests, and not everyone agrees on the most responsible way to handle vulnerability disclosure, but someone who discovers a vuln basically has three paths to choose from: non-disclosure, full disclosure, or partial disclosure.[53]

Non-disclosure means that the security researcher does not report the vulnerability to the company that wrote the software nor to the general public. This path is most common among researchers who work in-house at organizations that develop exploits for their own use, like the intelligence community, or for sale, such as the exploit brokers Vupen.[54] The fewer people that know about a vulnerability, the fewer people can defend themselves against its exploitation, and the more valuable it will be for buyers like criminal groups or government agencies.

Full disclosure is publicly sharing some or all of the details about a vulnerability and how it works, without first informing the vendor.[55] This kind of disclosure can help pressure companies into fixing the flaws in their software to avoid damage to their reputation or revenue. Leading security expert Bruce Schneier, a fellow at Harvard University’s Berkman Center for Internet & Society, argues that “public scrutiny is the only reliable way to improve security, while secrecy only makes us less secure.”[56] If a researcher publishes a blog post disclosing information about a vulnerability, for example, the disclosure can motivate the vendor to fix it, and it gives users the chance to stop using the software until it is fixed.[57]

However, on the other side of the argument are people like Scott Culp, founder of Microsoft’s Security Response Center.[58] Culp has compared full disclosure to “arming the enemy,” and called on the security research community to stop “shouting fire in the middle of a crowded movie house.”[59] While full disclosure can draw attention to a problem, and enhance a researcher’s reputation, it can also provide attackers with a cost-free stream of new vulnerabilities for use in developing and deploying malware.[60]

Since the benefit of full disclosure is a matter of hot debate in the security research community, some have proposed forms of partial disclosure as an alternative. Sometimes called "responsible disclosure," partial disclosure is a compromise between the coercive power and cautionary effect of public disclosure and the risks and insecurity of non-disclosure. Researchers inform the vendor of the existence of a vulnerability and grant the company a window of time to develop and issue a patch.[61] Key practical and ethical concerns when it comes to responsible disclosure include the question of what constitutes an appropriate length of time before disclosure, and whether the researcher should opt for full disclosure if the company is unresponsive or doesn't fix the vulnerability in a timely manner.

Whether partial or full disclosure is more effective in keeping software secure depends on the nature of the vulnerability and the characteristics of the software vendor. For example, partial disclosure poses unique challenges when addressing flaws in open source software, software that is openly and collaboratively developed. Such software is often created and maintained by small informal groups of volunteers, working via public message boards and widely viewable code repositories, who may not have the time or resources to patch it. In such cases, not only could it be difficult to prevent the partial disclosure from leaking to the public—the software is itself being developed in public—but a full disclosure may be the only way to mobilize the resources necessary to address the vulnerability. This is an area where there is relatively little precedent and a workable set of procedures are still being developed.[62]

There are several other scenarios where partial disclosure may be insufficient to address the threat, further complicating the question of whether to fully or partially disclose a vulnerability. For example, partial disclosure may be impossible when software has been "abandoned" by its original developers, or the original developer is unknown or has gone out of business, such that there is no obvious single party to disclose to. Partial disclosure is also a risky option when attackers may already have discovered the vulnerability and begun exploiting it. Without full disclosure, users won't get any warning and can't protect themselves by ceasing to use the vulnerable software, instead they will remain at risk for weeks or months until the company fixes the flaw. Finally, partial disclosure presumes that there is a vendor on the other side who is willing to engage and fix a vulnerability both quickly and quietly. In some cases, a company may be unwilling or simply unable to engage with security researchers or issue a fix in a timely way. In such cases, the discoverer may have no other option other than to release information about the vulnerability to the public, or at least threaten to in order to force prompt action.

> **States and criminals are often willing to pay a great deal more for a vulnerability they can exploit than vendors are willing to or capable of paying.**

Each of these paths has tradeoffs, and how a discoverer chooses to disclose a vulnerability depends on their desired outcome. A researcher who is motivated by the desire to build her reputation and contribute to security might opt for partial or full disclosure with the goal of getting the vulnerability patched.[63] Discoverers who choose this route may even get a financial reward, either directly from the vendor or indirectly through a third party.[64] These rewards programs will be discussed later in this paper. However, a discoverer who is primarily seeking financial compensation may have less incentive to disclose a vulnerability to the vendor when it could be sold for a much higher price on the open market. States and criminals are often willing to pay a great deal more for a vulnerability they can exploit than vendors are willing to or capable of paying.

HOW ARE VULNERABILITIES PATCHED (OR NOT)?

When the company or group that is responsible for securing a piece of software learns about a vulnerability, that vuln is no longer a "zero-day," a vulnerability that has just been discovered and therefore theoretically has had zero days to be patched. Once that vendor knows about the vulnerability, it hopefully will work to eliminate it by patching the software with fixes or work-arounds that negate the threat.[65] However, vendors are more likely to prioritize the patching of newer "flagship" products than older ones, and older systems that are still in use but rarely patched or updated are an ongoing cybersecurity challenge. For example, hundreds of millions of computers around the world—including many computers belonging to the federal government!—were still running the Windows XP operating system in 2014 when Microsoft stopped providing security updates for that software.[66]

Sometimes developing a patch can take months, during which users are still at risk.[67] Furthermore, creating the patch is only half the battle. It also has to be distributed, which can be even harder. For one thing, many users will fail to install the patch. Indeed, most of the major attacks over the past few years have targeted known vulnerabilities for which a patch existed that many users nevertheless failed to install.[68] This is why some vendors such as Apple and Google are designing their mobile operating systems to be automatically updated rather than relying on action by the user.[69] Microsoft has also announced that its Windows 10 operating system will continuously and automatically update on a rolling basis going forward (instead of having new versions every few years).[70] However, automatic updates are only as useful as the vendor providing them, and unfortunately updates can be delayed in many cases, particularly in complex ecosystems like that of Android where carriers, handset manufacturers, and Google all must work together to distribute patches.[71] Concern about delayed security updates in the mobile computing environment has become serious enough to prompt a joint FTC-FCC investigation into the issue.[72]

Corporate vendors aren't the only ones that have to develop and issues patches. Open source projects often are not housed at any one company but instead are made up of volunteers from around the world. The software they write and maintain may be used by many large corporations and within complex systems yet lack any centralized or well-resourced capacity to securely receive vulnerability reports and privately develop and ship security patches. For example, recent vulnerabilities in the open-source security software OpenSSL put two-thirds of Web users at risk, allowing criminals or other bad actors to steal passwords, private cryptographic keys, and other sensitive user data.[73] Because the software is open source, the patching efforts had to be completed in secret between a group of companies that used the software, mostly connected by a group of developers who all knew each other previously.[74] The challenge for the community and maintainers of such complex open-source systems is developing and distributing patches before it becomes widely known that a vulnerability exists.

WHICH LAWS DISCOURAGE SECURITY RESEARCH AND VULNERABILITY DISCLOSURE?

As we've already described, the question of whether and how to disclose a given vulnerability to the appropriate vendor is already a complex one. Making the calculus even more complicated is another, even more personal factor: legal risk. In some cases, laws aimed at stopping malicious hacking and digital copyright infringement have had the unintended consequence of chilling legitimate security research.[75] In particular, laws like the Computer Fraud and Abuse Act[76] and the Digital Millennium Copyright Act,[77] though designed to meet the challenges of the digital age, have been used to bring civil or criminal charges against legitimate researchers or individuals using techniques widely used by legitimate researchers.[78] As a result, they discourage research that could uncover new vulnerabilities and chill researchers' disclosure of the vulns they do discover, which in turn undermines cybersecurity by leaving vulnerabilities unpatched.

This dangerous chill on security research and vulnerability disclosure is so acute that a broad coalition of academic security researchers has joined with civil society to call for legal reform. Noting that critical research into the safety of internet-connected cars, voting machines and medical devices is threatened by continuing legal ambiguity, they have called on Congress to reform three specific laws to ensure that they do not prohibit research intended to improve the security of digital devices or of our nation's internet systems and infrastructure.[79] Those three laws, along with one international agreement that also threatens legitimate security research, are described below.

Computer Fraud and Abuse Act (CFAA)

The CFAA, at 18 U.S.C. §1030, is the primary federal anti-hacking law. Both security researchers and malicious attackers work to penetrate computers or networks; the difference between the two groups is what motivates them and what they do with the information they discover. The CFAA's strict, broad, vague prohibitions on unauthorized or excessive access to computer systems, coupled with severe legal penalties for violators, can prevent people from conducting research and testing, even tests that are aimed at identifying and eliminating vulnerabilities that put systems and users at risk. The CFAA is especially chilling to the extent that some prosecutors and civil litigants have applied it in cases where the accused didn't break into any system but instead merely violated a website's terms of service or an employer/employee contract.[80] Depending on the provision of the law at issue, those convicted under the CFAA for a first-time offense can face extensive fines and up to ten years in prison, which makes the law especially chilling. And even if a researcher is confident that the government won't prosecute, there is always the risk of a lawsuit: civil litigants can and often do sue under the CFAA over conduct that the Justice Department wouldn't prosecute but that arguably violates this broadly-written law.[81]

Digital Millennium Copyright Act (DMCA)

Under the "anti-circumvention" provisions of the DMCA, at 17 U.S.C. § 1201, it is unlawful to break a protection measure put in place to prevent a person from accessing copyrighted material. The law is aimed at stopping people from doing things like making bootleg copies of copy-protected DVDs. But in the 17 years since its passage, there have been fears that the law is susceptible to abuse by companies that don't want people tampering with their products, even in ways that have nothing to do with copyright infringement.[82] Due to the possibility of both criminal prosecution and civil suits, this law can chill security research and testing that involves breaking copy protection measures, even when the research is aimed at identifying and eliminating vulnerabilities, and even when that conduct is a legitimate fair use of the copyrighted work (such as reverse engineering) and isn't infringing. This section is still controversial today, and a group of researchers sued in July 2016 to challenge its constitutionality.[83] Researchers convicted under the DMCA for a first offense can face a fine up to $500,000 and/or a prison term of up to five years.

Electronic Communications Privacy Act (ECPA)

ECPA is the federal law aimed at protecting the privacy of electronic communications like your email. However, one provision, 18 U.S.C. §2701, prohibits access to private communications stored by a communications service provider without or in excess of authorization in terms very similar to those of the CFAA. This is aimed at protecting your privacy, but like the CFAA, ECPA's terms are broad and vague, and there is no exception that would protect legitimate security research. A first offense can lead to fines and up to five years in prison, and even in cases where there was no malicious intent, researchers could face up to a year in prison. More worrisome, some prosecutors have tried to use violation of ECPA as a penalty enhancer for CFAA violations—basically seeking a serious increase in penalties by double-counting the exact same conduct (which also doubly chills that conduct).[84]

Wassenaar Arrangement on Export Controls

The Wassenaar Arrangement is an international agreement between 41 countries which is focused on promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies.[85] Dual-use means that the technology can be used for both civilian and military purposes, and Wassenaar attempts to ensure that "states of concern" are prevented from acquiring these potentially dangerous tools. In 2013 the arrangement was updated to include controls on intrusion software, including exploits that bad guys use to break into systems.[86] The problem is that legitimate security researchers, such as penetration testers hired by a company to identify weaknesses in its systems, use the exact same tools.[87] Therefore, although the new provisions of the Arrangement are well-meaning— focused on keeping hacking software out of the hands of repressive regimes—the details, particularly in the way it was proposed to be implemented in American law, would have criminalized much of the work of security research.

The Department of Commerce has withdrawn its proposed implementation in the face of critical public comment,[88] and the State Department has indicated its intention to renegotiate the language of the Arrangement.[89] However, it remains to be seen how the Wassenaar Arrangement may ultimately apply to—and chill—critical cybersecurity work.

WHAT IS THE VULNERABILITIES MARKET?

Vulnerabilities are bought and sold, rented and traded, just like any other commodity—sometimes between companies with legal contracts and sometimes between anonymous hackers through internet forums. The market is a key component of the vulnerabilities ecosystem, and is comprised of a variety of different players that all interact and affect the broader picture. Mapping this ecosystem helps us to understand the incentives that drive discoverers either to disclose vulnerabilities to the vendor to be patched, or to sell them to the highest bidder. So who buys, and who sells vulnerabilities?

Earlier in the paper we discussed the four categories of discoverers: independent agents, small teams, larger teams within major technology companies, and governments. These groups find vulnerabilities and, sometimes, sell them on the market. Since we have already described these sellers, we can better understand the market by looking at to whom they are selling.

Prices for Vulnerabilities

What is a Google Chrome vulnerability worth?

Google pays: $500 - $15,000[90]

Google offered Vupen: $60,000[91]

Black Market pays: $80,000 - $200,000[92]

What is an iOS 9 vulnerability worth?

Zerodium has committed to pay: $1,000,000[93]

Governments

Governments are one of the key drivers of the vulnerabilities market, but their interaction with it is opaque. Analyzing whether these purchases are part of the purely criminal "black market", or the more legally ambiguous "gray market", is challenging because of the diversity of countries involved in the transactions. For example the company Hacking Team, which was itself the target of a massive data breach in the summer of 2015,[94] was revealed to have sold its products to a wide range of state actors. The released data shows that the company sold products to the United States military, and the Drug Enforcement Agency—these could be considered sales on the gray market.[95] But it also has sold its wares to Nigeria, Bahrain, Ethiopia, Sudan and Pakistan—countries whose governments are much less likely to respect human rights and could be considered part of the black market.[96] Some of these countries are currently under sanctions, making sales to them not only ethically questionable but clear violations of international law.[97]

> **Although the most advanced states like the U.K., Russia, Israel, the United States, China, and France often develop and discover vulnerabilities without resorting to the market, they are also the richest purchasers and seek out high-value products.**

State buyers tend to have more capital to spend in the vulnerabilities market.[98] Although the most advanced states like the U.K., Russia, Israel, the United States, China, and France often develop and discover vulnerabilities without resorting to the market, they are also the richest purchasers and seek out high-value products like zero-days and advanced hacking tools used to target other states or individuals. These buyers have been shown to often work through intermediaries like Gamma Group,[99] Vupen,[100] Hacking Team,[101] and ReVuln[102] (Netragard[103] and Endgame[104] sold exploits in the past, but both have announced that they will no longer do so) rather than buying directly from individual researchers.

Less advanced states like Ethiopia, Jordan, Kazakhstan, Saudi Arabia, Turkey, and Malaysia[105] are more likely to buy surveillance tools from intermediaries, versus expensive zero-days. For example, FinFisher—created and sold by Gamma International—is a surveillance tool used for remote monitoring and keylogging that the seller claimed could even listen in on a target's Skype calls in real time.[106] The tool has turned up in dozens of countries, and WikiLeaks documents have cited governments ranging from Pakistan to Belgium as confirmed buyers.[107] It is largely this market that the Wassenaar Arrangement's export controls[108] aim to affect, with the intention of stifling the flow of surveillance tools and intrusion software to repressive governments. While this may be a promising means to stem the sale of exploits in the government market, there are also genuine concerns about whether the export control rules as constructed unnecessarily stifle legitimate security research.[109]

Criminal Actors

The black market for vulnerabilities, once a varied landscape of ad hoc networks of individuals motivated by ego, notoriety, and (of course) money, has evolved into a mature market of highly organized groups, often including traditional criminal actors like drug cartels, mafias, and terrorist cells.[110] According to security expert Marc Goodman, 80 percent of black hat hackers are now affiliated with organized crime.[111] Dealings in this much larger, and slightly more public, black market take place through a variety of channels. Some are made through direct transactions with vulnerability discoverers, others through less reputable intermediaries,[112] and some using a network of web forums like Agora, Darkode, and Abraxas, functioning much like the clandestine online bazaars through which drugs and other illicit paraphernalia are sold.[113] Sellers in this market gain reputation by word of mouth but there are also more formalized rating and feedback systems used to identify which sellers have reliable and high-quality products. The buyers in this market are often less well-resourced than governments, and tend to be looking for the minimum investment necessary to achieve their goals.

Unlike governments, who usually buy tools used to attack, defend, or collect information on targets, many tools sold to criminal actors aim to make a profit for the groups using them.

Criminal actors are often focused more on acquiring non-zero day vulnerabilities that can be used on older or unpatched systems, because they are less expensive and the exploitation of them could impact more users, as well as on purchasing less sophisticated (and therefore more affordable) malware. These markets also offer services not directly based in vulnerabilities, such as the rental of botnets—networks of computers that have been "hijacked" through the use of an exploit and are afterward controlled remotely—to send spam or engage in Distributed Denial of Service attacks on websites.[114] These networks are much less interesting to government purchasers, because they don't provide the surveillance or intrusion functions those buyers seek. By contrast, criminal groups are seeking impact on a large scale with minimal investment, but do not aim to collect massive amounts of intelligence in the same way as governments. Other products that are prevalent in the black market are malware-as-a-service models, point-and-click tools, and easy-to-find online tutorials that allow less technically-inclined actors to make use of vulnerabilities and expand the market to include many more types of participants.[115]

Unlike governments, who usually buy tools used to attack, defend, or collect information on targets, many tools sold to criminal actors aim to make a profit for the groups using them. These buyers generally cannot afford zero-days, but instead purchase malware programs and/or exploit kits used to deliver that malware onto a machine.[116] Those programs can steal personal information, extort money from victims by using ransom or scareware,[117] redirect users to phishing sites, use your computer as a secret server to broadcast pornography files, or execute many other functions to support or fund criminal activity.[118]

Intermediaries

There is also a range of intermediary groups in the vulnerability ecosystem. As mentioned above, companies like Gamma Group,[119] Vupen,[120] Hacking Team,[121] ReVuln,[122] Netragard,[123] and Endgame fall into this category, though there are many others. They are viewed by some as part of the gray market, but in multiple cases they have also been accused of engaging with the black market of criminal actors and repressive governments. There are also individuals who serve as intermediaries, brokering sales between finders and high-income buyers for record fees.[124]

Intermediaries are both buyers and sellers, purchasing working exploits and integrating them into existing payloads and propagation tools to sell to government intelligence and law enforcement agencies. Intermediaries, when they act as buyers, have much larger budgets to work with—often paying out huge bounties to discoverers with the intention of selling them for even higher fees to buyers with deeper pockets.[125] These actors often also discover or build their own products for sale or rent to customers. These include some of the most notorious spyware that has been discovered in the wild by security researchers and tied to these intermediaries. Companies like Trovicor (formerly part of Siemens)[126] and Amesys[127] sell these proprietary tools to government clients, including oppressive regimes like Bahrain, Libya, and Syria.

The role of intermediaries, and whether or how they should be regulated is a contentious topic among experts in the field. Some companies, like Netragard,[128] limited their sales to a certain list of countries in an attempt to maintain a level of legitimacy. Others, like Vupen, are less specific about who they are willing to sell to,[129] and their tools have turned up in the possession of questionable governments. Adriel Desautels, who runs Netragard, says he knows of “greedy and irresponsible” people who “will sell to anybody,” to the extent that some exploits might be sold to two governments who oppose each other. “If I take a gun and ship it overseas to some guy in the Middle East and he uses it to go after American troops—it’s the same concept.” said Desautels[130] Some critics go even further, with the ACLU’s Chris Soghoian calling Vupen a “modern-day merchant of death,” selling “the bullets for cyberwar.”[131]

Like governments, the participation of intermediaries in the vulnerabilities market helps drive the prices up significantly, especially when the clients of these companies are willing to pay hundreds of thousands of dollars for top-quality products. Their participation helps to maintain the huge disparity between what vulnerability discoverers can get paid on the gray or black market, and what the other major market participant—software companies—can afford to pay to help fix their own products.

Software Vendors

Software vendors seeking vulnerabilities in their own products so that they can be patched face a significant challenge: outside researchers that discover those vulnerabilities, instead of disclosing to the vendor, can often make a substantial profit by selling the same information to the black or gray markets. Dan Geer, a computer security analyst and risk management specialist, said that “[F] or a good long while, you could do vulnerability finding as a hobby and get paid in bragging rights, but finding vulnerabilities got to be too hard to do as a hobby in your spare time—you needed to work it like a job and get paid like a job.”[132] In response to competition from buyers in the vulnerability market, vendors have begun to create vulnerability rewards programs (VRPs), also known as bug bounties,[133] which pay out fees to researchers for the vulnerabilities that they disclose. Many software vendors recognize VRPs as a financially efficient means to help find vulnerabilities their own security teams have missed, draw increased attention to their products, facilitate coordination with security researchers, and provide financially driven researchers with an alternative to selling on the black market.[134] Along with the individual bounties, discoverers who are highly successful at finding and reporting these flaws to vendors may even be offered full employment at these companies.[135]

VRPs aim to shift the cultural narrative from one that casts security researchers as universally malicious hackers or criminals, to one that recognizes that researchers may provide an invaluable service to companies—and consumers—by helping to make software more secure.[136] Along with big VRPs from Microsoft,[137] Facebook,[138] Yahoo!,[139] and Google,[140] there are also bounty intermediaries, like the Zero Day Initiative[141] and HackerOne,[142] that purchase information about vulnerabilities. These intermediaries provide a portal for reporting vulnerabilities to companies, streamlining reporting from a diverse group of researchers, establishing reputations for individual researchers, and paying out bounties to people who discover vulnerabilities worth rewarding.[143] High-profile hacking competitions are another tool used to capture the capacity of security researchers and encourage them to test widely used software. For example, the 2015 Pwn2Own challenge paid out $442,000 in bounties for critical bugs in all four major internet browsers, as well as in Windows, Adobe Flash, and Adobe Reader.[144]

A downside of VRPs and bug-finding competitions is that, although they provide researchers with an alternative to selling information about vulnerabilities on the black market, where they generally are not able to compete dollar-for-dollar.[145] Unfortunately, discoverers looking for maximum payoff may have to sell to buyers who aren’t looking to patch the bug, and the longer a vulnerability stays secret, and unpatched, the longer it retains its value for those who wish to exploit it.[146] But for ethical hackers who don’t want to contribute to insecurity by selling on the open market but do want to get some meaningful recognition and compensation, bug bounty programs offer an important avenue for responsible disclosure. Bug-bounty programs also have other positive effects for companies, including creating a clearer structure for receiving and tracking vulnerability reports, and creating a healthier relationship with the security community. Consequently, the number of companies with bounty programs, and the number of researchers who participate in them, is exploding.[147] Hopefully, this is a sign that these programs are successfully convincing hackers who may have gone to the dark side to put on a white hat instead.

WHY GOVERNMENTS DO (OR DON'T) DISCLOSE THE VULNERABILITIES THEY FIND OR BUY

When governments purchase vulnerabilities on the market they have the same three options for disclosure as independent researchers: non-disclosure, full disclosure, and partial disclosure. However, their set of interests is very different from those of independent researchers. Security researchers or academics might seek the credibility or notoriety that could come from full disclosure; or they may want compensation or professional recognition through legal bug bounties or other vulnerability rewards programs; or they may want the bigger financial rewards of the black or gray market. Governments are not seeking any of these things.

Governments have a set of unique incentives to keep information about vulnerabilities secret.[148] They may want to keep the public and their own systems safe from bad guys exploiting those vulnerabilities, by disclosing them and ensuring they are patched. At the same time, they may want to use the vulnerabilities themselves, whether to conduct law enforcement or foreign intelligence surveillance, or even for offensive purposes—for example, the Stuxnet virus developed by the U.S. and Israel to disable Iran's uranium enrichment facilities relied on four zero-day vulnerabilities in the Microsoft Windows operating system.[149] Therefore, governments have to weigh the security value of disclosure versus the value that could come from stockpiling and using vulnerabilities for their own purposes. As we discuss below, any governmental process for making such decisions—in the U.S., the government calls it the "vulnerability equities process"[150]—ideally will be clearly and publicly defined, will involve a wide range of stakeholders, and will be strongly weighted in favor of disclosure.

CONCLUSION: WHAT POLICIES WILL FOSTER THE DISCOVERY, DISCLOSURE, AND PATCHING OF VULNERABILITIES

Now that we know what vulnerabilities and exploits are, who buys and who sells them, what types of laws can chill researchers and what kind of vulnerability reward programs can motivate them, it's worth asking the natural next question: what policies might better ensure that more vulnerabilities are discovered, disclosed, and patched faster? How can we better align incentives to ensure that more researchers are sharing the vulnerabilities they find with the people who can fix them, rather than selling them to those who want to exploit them?

> **There are a number of opportunities that policymakers have to influence the flow of vulnerabilities and thereby make the digital ecosystem much safer.**

There are a number of opportunities that policymakers have to influence the flow of vulnerabilities and thereby make the digital ecosystem much safer for all of us. In particular, here are five policy recommendations to start the conversation, initial recommendations that we'll explore in more depth in future publications.

1. The U.S. government should minimize its participation in the zero-day market.

The ever-expanding market for previously undiscovered vulnerabilities is perhaps the single largest disincentive to disclosing a vulnerability to a vendor so that it can be patched. Many researchers are already paid directly for their work, or would have ethical qualms selling vulns for offensive use rather than working to get them fixed. But others will ask themselves: Why disclose a vulnerability for no financial reward or for a relatively small bug bounty when it can be sold on the open market—a market that unfortunately caters not just to democratic nations' intelligence and law enforcement communities but to a wide range of spies, criminals, and repressive regimes—for much more money?

The U.S. government is in a unique position to significantly shrink this market simply by not participating, as it is one of the largest buyers—indeed, probably the single largest buyer—in that market.[151] The U.S. government is also in a unique position to be able to forego the market by relying on and growing its own technical expertise, at the NSA and other agencies, to discover vulnerabilities and develop exploits itself rather than fostering a dangerous gray market in vulnerabilities that ultimately makes us all less safe.[152] Therefore, we recommend that U.S. policymakers—and the U.S. Congress in particular—begin investigating the extent of U.S. participation in the vulnerability market, and weigh the benefits that flow from that participation versus the very real costs of participating in and facilitating such a market. Based on such investigation, the government should establish clear policies for when (if at all) the government buys vulnerabilities from third parties, with a goal of reducing or even eliminating our reliance on and support for the zero-day market.

> **The government should establish clear policies for when (if at all) the government buys vulnerabilities from third parties, with a goal of reducing or even eliminating our reliance on and support for the zero-day market.**

Dan Geer, chief security officer at the CIA's venture firm In-Q-Tel, has suggested a more radical and controversial solution that would have the government maximize rather than minimize its participation in the market.[153] Geer suggests that the best use of U.S. government resources would be to corner the market in vulnerabilities, paying top dollar for all the zero-days it can find and disclosing them so they can be fixed. The consequent increase in the price of zero-days would price many bad guys out of the market while also growing the population of people hunting for new vulnerabilities to be patched. As Geer admits, however, the effectiveness of this strategy would turn on how common vulnerabilities are. If zero-days are relatively rare, this strategy could succeed, but if they are relatively plentiful, such an approach likely wouldn't scale. So again, we recommend further investigation of the market by policymakers so they can better decide whether and how the U.S. should participate in the market as a zero-day buyer. If the U.S. government is going to buy zero-days at all, however, it will also need a strong, clear process for timely disclosure of those vulnerabilities to the vendors who can fix them.

2. The U.S. government should establish strong, clear procedures for government disclosure of the vulnerabilities it buys or discovers.

Whether it buys them or discovers them itself, the U.S. government has a responsibility to ensure that vulnerabilities that put users and companies in the U.S. at risk are disclosed and patched as soon as possible. That conclusion is shared by a wide range of stakeholders, from the President's own hand-picked Review Group on Intelligence and Communications Technologies,[154] to political scientists like Joseph Nye,[155] to tech companies like Microsoft,[156] to digital rights advocates like the Electronic Frontier Foundation (EFF).[157]

In the Spring of 2014, the White House announced it was "re-invigorat[ing]" an interagency process first established 2010 in order to decide when the government should disclose vulnerabilities, a so-called "vulnerability equities process" (VEP) intended to weigh the costs and benefits of holding on to a vulnerability for offensive or investigative use versus disclosing it so that it can be patched.[158] The White House claims that the vast majority of vulnerabilities that go through the process end up being disclosed,[159] but many questions remain about whether all vulnerabilities actually go through the process, how many vulnerabilities have actually been disclosed under the process and how many have been withheld for how long, which agencies meaningfully participate in the process, who makes the ultimate decisions, and how exactly those decisions are made.[160] Indeed, there are so many questions that EFF has sued the NSA and the Director of National Intelligence under the Freedom of Information Act to obtain more information.[161]

These questions about when the government does and does not disclose vulnerabilities can and should be answered. First, they should be answered by the Executive Branch, which should be as transparent as possible about the processes, standards, and results of its vulnerability equities process—transparent not only to the American people but to Congress, which should investigate the issue. Second and ultimately, though, these questions should be answered by Congress itself, after such an investigation, in the form of a statutorily codified process that is heavily weighted toward disclosure and that the agencies are required by law to follow. The issue of vulnerability disclosure is too important, and the incentives of the intelligence community and especially the law enforcement community are too skewed on the side of stockpiling vulnerabilities, to leave such decisions solely to the Executive Branch.

The Executive Branch shouldn't wait for Congressional action to reform and vigorously implement its existing VEP, however. As top former White House cybersecurity officials have recommended, the President can and should issue an executive order formalizing and requiring compliance with the current VEP, and strengthening transparency, oversight and accountability of the process.[162] Amongst the former officials' recommended reforms is a prohibition against agencies' entering into nondisclosure agreements when they buy vulnerabilities or exploits, and a requirement that they instead buy exclusive rights to the vulnerabilities so they are not further resold to other parties. That way the information or tool can go into the VEP to be reviewed for disclosure, and agencies cannot contract their way around complying with the process.[163] Notably, such a rule would have prevented the recent scenario where the FBI failed to submit to the VEP an Apple iPhone exploit it had purchased because it had not also purchased rights to the underlying vulnerability that made the exploit possible.[164]

3. Congress should establish clear rules of the road for government hacking in order to protect cybersecurity in addition to civil liberties.

Government use of vulnerabilities to surreptitiously and remotely hack into computers as part of criminal investigations is a growing practice, so much so that the Justice Department has sought updates to the federal rule concerning search warrants—Federal Rule of Criminal Procedure 41—to routinize the practice.[165] Yet for an investigative technique that has been common for at least fifteen years,[166] practically nothing is known about how often law enforcement engages in such "network

> **Government hacking is just as invasive if not more invasive than government wiretapping, and raises a wide variety of unique security and civil liberties risks.**

investigative techniques" or "remote access searches" as they are euphemistically called, or how they do it; indeed, law enforcement agencies have recently been fighting in court to avoid having to disclose details about how they have been breaking into suspects' computers.[167] And it's not just the public who's left in the dark: courts themselves, including the courts that routinely sign off on secret warrants to authorize such hacking despite vague, unclear, or misleading language in the government's warrant applications, don't seem to understand what they are authorizing.[168]

> **The status quo needs to change. Especially considering that government hacking may result in a less secure digital environment.**

This state of affairs is all the more worrisome because government hacking is just as invasive if not more invasive than government wiretapping, and raises a wide variety of unique security and civil liberties risks, including the risk that the malware used by the government may spread to innocent people's computers, lead to unintended damage, or the creation of new vulnerabilities.[169] Yet unlike wiretapping, a practice that Congress has specifically authorized and tightly regulated with many special additional constraints that aren't applied to regular search warrants, there is no such Congressional authorization nor statutory rules of the road to ensure that the government's ability to hack isn't abused.

The status quo needs to change. Especially considering that government hacking may result in a less secure digital environment—whether by perpetuating old vulnerabilities that the government chooses to exploit rather than disclose, or by unintentionally damaging systems or creating new vulnerabilities[170]—it's time for Congress step in. Rather than allowing the Rule 41 changes to automatically go into effect in December 2016, which is what will happen if Congress does not take action, it should press pause on those changes and take this opportunity to educate itself on the issue, demand answers from the government about its hacking practices, and—if it chooses to allow government hacking at all—craft legislation to regulate the practice just as it has previously done for uniquely invasive search and seizure practices like wiretapping.

4. Government and industry should support bug bounty programs as an alternative to the zero-day market and investigate other innovative ways to foster the disclosure and prompt patching of vulnerabilities.

Every company that produces software should have a clear process for outside researchers to disclose vulnerabilities—and if they're smart they will also offer Vulnerability Reward Programs (VRPs) or "bug bounty" programs to reward the people who discover those vulnerabilities. Whether the reward comes in the form of "thanks, t-shirts, or [simply] cold hard cash," providing a clear path for vulns to be disclosed and for disclosures to be rewarded is a must if companies want to provide a meaningful alternative to selling vulns on the open market.[171] Though unlikely to ever be able to compete dollar-for-dollar with governments and organized criminals, these programs provide an outlet for researchers who have ethical or legal qualms with simply selling to the highest bidder, want to build a legitimate reputation as a security expert, or just want to help improve digital security.

We encourage companies to get even more creative about the financial and non-financial incentives they can offer to bug discoverers. For example, some security researchers have suggested that in order for the "defensive" market of companies looking to discover and patch bugs to better be able to keep up with the "offensive" market serving governments and criminals, it should offer bounties not only for the vulnerabilities themselves but for tools and techniques that help them find vulnerabilities more efficiently. The government should also also get creative about how it can better foster such programs—for example through tax incentives or small grants—and about how it can help increase both the flow of vulnerability information to vendors and increase vendors' responsiveness to that information.[172] The recent launch by the Commerce Department's National Telecommunications and Information Administration (NTIA) of a multistakeholder process to come up with best practices in this area for both researchers and vendors is a positive sign,[173] as is the FCC and FTC's investigation into the security update practices of mobile device manufacturers to ensure that mobile device vulnerabilities are being patched in a timely manner.[174]

One last key feature of a robust bug bounty program is a pledge by the vendor not to sue those who disclose vulnerabilities in compliance with their program's rules for reasonable disclosure. Many researchers are rightly concerned about potential legal action under overbroad or ambiguous computer crime and copyright laws, and those concerns may chill them from disclosing at all.[175] Thankfully, such pledges are becoming increasingly common.[176] However, company pledges can only go so far in reassuring researchers, especially when it comes to criminal statutes where prosecution by the government[177] is just as much a risk as a lawsuit by the company.[178] Reform of the law itself will be necessary to fully address this problem.

5. Congress should reform computer crime and copyright laws, and agencies should modify their application of such laws, to reduce the legal chill on legitimate security research.

Improving cybersecurity entails supporting and encouraging security research. Policymakers looking to move the cybersecurity needle could start by reforming a number of laws that subject independent security researchers to legal threat, as a broad coalition of academic researchers and civil society experts have urged.[179] There are already some bills introduced in Congress, such as Aaron's Law, that would reform the Computer Fraud and Abuse Act (CFAA) to reduce the legal chill on security researchers.[180] This proposed law would eliminate criminal liability for terms of service violations and reduce the currently disproportionate penalties for crimes that caused little to no economic harm.[181] However, the Justice Department need not wait for Congress to help protect security researchers; as that same coalition of experts and researchers has urged, it could issue public guidance to prosecutors now to emphasize the importance of cybersecurity research and to narrow and clarify the scope of conduct that it will and won't prosecute under CFAA, as well as under the similar unauthorized access provisions in the Electronic Communications Privacy Act (ECPA).

Researchers and their allies in civil society have been also advocating for updates to the Digital Millennium Copyright Act (DMCA) for very similar reasons.[182] That law prohibits skirting any technological measure that protects copyrighted material, but can create civil and criminal liability for security researchers even if their research isn't infringing. In October 2015, the Librarian of Congress responded to some of these criticisms by granting an exemption from the DMCA anti-circumvention law for a few types of security research.[183] While this is a good first step, many commentators, including this paper's authors, are concerned that the new exemptions are still drawn too narrowly and that important security research may still be stifled under the new rules, and would prefer to see Congress codify such exemptions in the law. Congress should also use its oversight authority to ensure that State Department renegotiation and Commerce Department implementation of the Wassenaar agreement restricting the export of intrusion tools leads to a final rule that adequately protects legitimate cybersecurity-related activities.

Notes

[1] See e.g., "Verizon's 2016 Data Breach Investiations Report", Verizon Enterprise, April 2016, available at http://news.verizonenterprise.com/2016/04/2016-data-breach-report-info/ (accessed July 24, 2016); "Gemalto Releases Findings of First Half 2015 Breach Level Index," Gemalto, September 9, 2015, http://www.gemalto.com/press/Pages/Gemalto-Releases-Findings-of-First-Half-2015-Breach-Level-Index.aspx (accessed July 24, 2016).

[2] Dawn Chiemeilewski and Arik Hesseldahl, "Sony Pictures Knew of Gaps in Computer Network Before Hack Attack," Re/code, December 12, 2014, http://www.recode.net/2014/12/12/11633774/sony-pictures-knew-of-gaps-in-computer-network-before-hack-attack (accessed July 24, 2016).

[3] Clint Boulton, "Experts on the Anthem Hack: SurfWatch Lab's Adam Meyer," Wall Street Journal, February 5, 2015, http://blogs.wsj.com/cio/2015/02/05/experts-on-the-anthem-hack-surfwatch-labs-adam-meyer/ (accessed July 24, 2016).

[4] Dan Goodin, "Once Seen As Bulletproof, 11 million+ Ashley Madison Passwords Already Cracked," ArsTechnica, September 10, 2015, http://arstechnica.com/security/2015/09/once-seen-as-bulletproof-11-million-ashley-madison-passwords-already-cracked/ (accessed July 24, 2016).

[5] Sean Gallagher, "EPIC Fail—How OPM Hackers Tapped the Mother Lode of Espionage Data," ArsTechnica, June 21, 2015, http://arstechnica.com/security/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/ (accessed July 24, 2016).

[6] Keith Collins, "A Rare Detailed Look Inside the IRS's Massive Data Breach, via a Security Expert Who Was a Victim," Quartz, August 27, 2015, http://qz.com/445233/inside-the-irss-massive-data-breach/ (accessed July 24, 2016).

[7] Jason Hong, "Human Weakness in Cybersecurity," Slate, August 12, 2015, http://www.slate.com/articles/technology/future_tense/2015/08/joint_chiefs_of_staff_email_hack_the_dangers_of_spear_phishing.html (accessed July 24, 2016).

[8] See, e.g., Arik Hesseldahl, "Here's What Helped Sony's Hackers Break In: Zero-Day Vulnerability," Re/code, January 20, 2015, https://recode.net/2015/01/20/heres-what-helped-sonys-hackers-break-in-zero-day-vulnerability (accessed July 24, 2016).

[9] Verizon Enterprise, "Verizon's 2016 Data Breach Investigations Report."

[10] Ellen Nakashima, "Comey Defends FBI's Purchase of iPhone Hacking Tool," Washington Post, May 11, 2016, https://www.washingtonpost.com/world/national-security/comey-defends-fbis-purchase-of-iphone-hacking-tool/2016/05/11/ce7eae54-1616-11e6-924d-838753295f9a_story.html?postshare=2391463017543104&tid=ss_tw (accessed July 24, 2016).

[11] Joseph Cox, "Mozilla Urges FBI to Disclose Potential Firefox Security Vulnerability," Motherboard, May 12, 2016, http://motherboard.vice.com/read/mozilla-urges-fbi-to-disclose-firefox-security-vulnerability (accessed July 24, 2016).

[12] Katie Bo Williams, "Obama Administration to Renegotiate Rules for Intrusion Software," The Hill, February 29, 2016, http://thehill.com/policy/cybersecurity/271204-obama-administration-to-renegotiate-international-anti-hacking-regs (accessed July 24, 2016).

[13] David Shepardson, "U.S. Investigates Security of Mobile Devices," Reuters, May 9, 2016, http://www.reuters.com/article/us-wireless-inquiry-regulators-idUSKCN0Y022E (accessed July 24, 2016).

[14] Andrii Degler, "10-Year-Old Gets $10,000 Bounty For Finding Instagram Vulnerability," ArsTechnica, May 4, 2016, http://arstechnica.com/security/2016/05/facebook-schoolboy-bug-bounty-justin-bieber-instragram-hack/ (accessed July 24, 2016).

[15] "Software Vulnerability Management at Microsoft," Microsoft, http://www.microsoft.com/en-us/download/details.aspx?id=4372 (accessed July 24, 2016).

[16] See, e.g., Gregg Keizer, "Single Code Typo Triggers Massive internet Explorer Hack Attacks," itBusiness, August 4, 2009, http://www.itbusiness.ca/news/ single-code-typo-triggers-massive-internet-explorerhack-attacks/13806 (accessed July 24, 2016); "Apple's SSL/TLS bug," ImperialViolet, February 22, 2014, https://www.imperialviolet.org/2014/02/22/applebug.html (accessed July 24, 2016).

[17] See, e.g., Matthew Prince, "Deep Inside a DNS Amplification DDoS Attack," Cloudflare Blog, October 30, 2012, https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/ (accessed July 24, 2016).

[18] Chris Wysopal, Chris Eng, and Tyler Shields. "Static Detection of Application Backdoors." DuD Datenschutz Und Datensicherheit, March 24, 2010: 149-55, available at http://www.veracode.com/sites/default/files/Resources/Whitepapers/static-detection-of-backdoors-1.0.pdf (accessed July 24, 2016).

[19] “What Does Exploit Mean?” PC Tools by Symantec, http://www.pctools.com/security-news/what-does-exploit-mean/ (accessed May 25, 2016); Rustell Yatrin, “Proof-of-Concept Exploit Sharing Is On The Rise,” Information Week, May 5, 2016, http://www.darkreading.com/vulnerabilities-and-threats/proof-of-concept-exploit-sharing-is-on-the-rise/d/d-id/1325413 (accessed July 24, 2016); Maria Korolov, “60% of Enterprise Phones Still Vulnerable to QSEE Exploit,” CSO, May 19, 2016, http://www.csoonline.com/article/3072472/android/60-of-enterprise-phones-still-vulnerable-to-qsee-exploit.html (accessed July 24, 2016).

[20] “The Exploit Malware Family,” Microsoft Malware Protection Center, https://www.microsoft.com/security/portal/mmpc/threat/exploits.aspx (accessed July 24, 2016); Camilo Gutiérrez Amaya, “Myths About Malware: An Exploit is the Same As Malware,” WeLiveSecurity, October 21, 2014, http://www.welivesecurity.com/2014/10/21/myths-about-malware-exploit-is-the-same-as-malware/ (accessed July 24, 2016).

[21] “Severity Levels,” Qualys, https://qualysguard.qualys.com/qwebhelp/fo_help/knowledgebase/vulnerability_levels.htm (accessed July 24, 2016);

“Types of Security Vulnerabilities,” Mac Developer Library, February 11, 2014, https://developer.apple.com/library/mac/documentation/Security/Conceptual/SecureCodingGuide/Articles/TypesSecVuln.html (accessed July 24, 2016);

“OWASP Top 10-2013: The Ten Most Critical Application Security Risks,” Open Web Application Security Project, http://owasptop10.googlecode.com/files/OWASP Top 10 - 2013.pdf (accessed July 24, 2016).

[22] See e.g., Seung Lee, “Your Money Or Your Data: Ransomware Viruses Reach Epidemic Proportions,” Newsweek, May 10, 2016, http://www.newsweek.com/money-or-data-ransomware-viruses-epidemic-proportions-457588 (accessed July 24, 2016); Chris Franciscani, “Ransomware Hackers Blackmail U.S. Police Departments,” NBC News, April 26, 2016, http://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746 (accessed July 24, 2016); Andrew Dalton, “Ransomware Hackers Get Their Money, Then Ask For More,” Endgaget, May 24, 2016, http://www.engadget.com/2016/05/24/ransomware-hackers-get-paid-ask-for-more/ (accessed July 24, 2016).

[23] “Clickjacking,” Open Web Application Security Project, December 1, 2015, https://www.owasp.org/index.php/Clickjacking (accessed July 24, 2016).

[24] See e.g., Marshall Honorof, “Clickjack Attack Infects Nearly One Million Computers,” Yahoo News, May 17, 2016, https://www.yahoo.com/tech/clickjack-attack-infects-nearly-one-150450744.html (accessed July 24, 2016); Jacob Siegal, “Half a Billion Android Devices Are Impacted By the Latest Evolution of Mobile Malware,” BGR, March 4, 2016, http://bgr.com/2016/03/04/android-malware-accessibility-clickjacking/ (accessed July 24, 2016).

[25] “Security Intelligence Definitions,” Trendmicro, https://www.trendmicro.com/vinfo/us/security/definition/ (accessed July 24, 2016);

[26] See e.g., Lucian Constantin, “Attack Campaign Uses Keylogger to Hijack Key Business Email Accounts,” CIO, March 17, 2016, http://www.cio.com/article/3045536/attack-campaign-uses-keylogger-to-hijack-key-business-email-accounts.html (accessed July 24, 2016); Joan Goodchild, “How Keylogging Malware Steals Your Information,” CSO, July 15, 2013, http://www.csoonline.com/article/2112405/social-networking-security/how-keylogging-malware-steals-your-information--includes-video-.html (accessed July 24, 2016).

[27] Joshua Kopstein, “U.S. Government is Now the Biggest Buyer of Malware, Reuters Reports,” The Verge, May 10, 2013, http://www.theverge.com/2013/5/10/4319278/us-government-hacking-threatens-cybersecurity-former-officials-say (accessed July 24, 2016); See e.g. Ellen Nakishima, “This is How the Government is Catching People Who Use Child Porn Sites,” Washington Post, January 21, 2016, https://www.washingtonpost.com/world/national-security/how-the-government-is-using-malware-to-ensnare-child-porn-users/2016/01/21/fb8ab5f8-bec0-11e5-83d4-42e3bceea902_story.html (accessed July 24, 2016); Glyn Moody, “German Police Can Now Use Spying Malware to Monitor Suspects,” Ars Technica, February 24, 2016, http://arstechnica.co.uk/tech-policy/2016/02/german-police-can-now-use-spying-malware-to-monitor-suspects/ (accessed accessed July 24, 2016); Seth Rosenblatt, “Russian Government Gathers Intelligence with Malware: Report,” CNet, October 28, 2014, http://www.cnet.com/news/russian-government-gathers-intelligence-with-malware-report/ (accessed July 24, 2016); Adrienne Lafrance, “Hacking and the Future of Warfare,” The Atlantic, June 12, 2015, http://www.theatlantic.com/technology/archive/2015/06/hacking-and-the-future-of-warfare/395723/ (accessed July 24, 2016); Jennifer Valentino-Devries and Danny Yadron, “Cataloging the World’s Cyberforces,” Wall Street Journal, October 11, 2015, http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710 (accessed July 24, 2016).

[28] Timothy B. Lee, “How a Grad Student Trying to Build the First Botnet Brought the internet to Its Knees,”

Washington Post, November 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/ (accessed July 24, 2016).

29 Serge Malenkovich, "Morris Worm Turns 25," Kaspersky Lab Daily, November 4, 2013, https://blog.kaspersky.com/morris-worm-turns-25/3065/ (accessed July 24, 2016).

30 Space Rogue, "Bio," http://www.spacerogue.net/wordpress/?page_id=49 (accessed July 24, 2016).

31 Craig Timberg, "A Disaster Foretold—And Ignored," Washington Post, June 22, 2015, http://www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/ (accessed July 24, 2016)

32 Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me In It," WIRED, July 21, 2015 https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (accessed July 24, 2016). Charlie Miller, then an independent researcher, has since been recruited by Uber.

33 Citizen Lab, "About," https://citizenlab.org/about/ (accessed July 24, 2016).

34 Rapid7, "Our Company," https://www.rapid7.com/company (accessed April 27, 2016).

35 Chris Evans, "Announcing Project Zero," Google Online Security Blog, July 15, 2014, http://googleonlinesecurity.blogspot.com/2014/07/announcing-project-zero.html (accessed July 24, 2016).

36 "Microsoft Security Response Center," Microsoft TechNet, https://technet.microsoft.com/en-us/Library/Dn440717.aspx (accessed July 24, 2016).

37 Jennifer Valentino-Devries and Danny Yadron, "FBI Taps Hacker Tactic to Spy on Suspects," Wall Street Journal, Aug 3, 2013, http://www.wsj.com/articles/SB10001424127887323997004578641993388259674 (accessed July 24, 2016).

38 Speigel Staff, "Inside TAO: Documents Reveal Top NSA Hacking Unit," Speigel Online International, December 29, 2013, http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html (accessed July 24, 2016).

39 Glenn Greenwald, "Hacking Online Polls And Other Ways British Spies Seek To Control the Internet", The Intercept, July 14, 2014, https://theintercept.com/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet/ (accessed July 24, 2016).

40 "Definition: Security Audit," Tech Target, http://searchcio.techtarget.com/definition/security-audit (accessed July 24, 2016).

41 "Penetration Testing Overview," Core Security, http://www.coresecurity.com/penetration-testing-overview (accessed July 24, 2016).

42 Dan Goodin, "All Four Major Browsers Take a Stomping at pwn2own Hacking Competition," Ars Technica, March 20, 2015, http://arstechnica.com/security/2015/03/all-four-major-browsers-take-a-stomping-at-pwn2own-hacking-competition/ (accessed July 24, 2016); Parker Higgins and Ranga Krishnan, "DEFCON Router Hacking Contest Reveals 15 Major Vulnerabilities," Electronic Frontier Foundation, October 7, 2014, https://www.eff.org/deeplinks/2014/08/def-con-router-hacking-contest-success-fun-learning-and-profit-many (accessed July 24, 2016); Lucian Constantin, "15 New Vulnerabilities Reported During Router Hacking Contest," Computer World, August 12, 2014, http://www.computerworld.com/article/2491141/malware-vulnerabilities/15-new-vulnerabilities-reported-during-router-hacking-contest.html (accessed July 24, 2016).

43 In 2015 Facebook paid out $936,000 to 210 researchers, who submitted a total of 526 valid reports. "2015 Highlights: Less Low-Hanging Fruit," Facebook, February 9, 2016, https://www.facebook.com/notes/facebook-bug-bounty/2015-highlights-less-low-hanging-fruit/1225168744164016 (accessed July 24, 2016); In the same year, Google paid out more than $2 million to over 300 researchers. This includes a new rewards program for the Android operating system, which was started in June. "Google Security Rewards - 2015 Year in Review," Google Security Blog, January 28, 2016, https://security.googleblog.com/2016/01/google-security-rewards-2015-year-in.html (accessed July 24, 2016). In 2015 and early 2016, organizations launching new bug bounty programs have included Tesla, United Airlines, Dropbox, the Tor Project, MIT, and Uber, though it is worth noting that not all of these programs pay out rewards in cash. Right now United Airlines is offering travel miles to discoverers, and General Motors launched a Vulnerability Submission Program that, so far, has made no mention or rewards for discoverers—other than the ability to report a vulnerability without threat of being sued by the company.

44 Alex Fitzpatrick, "Heartbleeding Out: internet Security Bug Even Worse Than First Believed," Time, April 11, 2014, http://time.com/59390/heartbleed-internet-security-routers/ (accessed July 24, 2016).

45 Craig Timberg, "'FREAK' Flaw Undermines Security for Apple and Google Users, Researchers Discover,"

Washington Post, https://www.washingtonpost.com/news/the-switch/wp/2015/03/03/freak-flaw-undermines-security-for-apple-and-google-users-researchers-discover/ (accessed July 24, 2016).

46 Sebastian Anthony, "The First Rule of Zero-Days Is No One Talks about Zero-Days (So We'll Explain)," Ars Technica, October 20, 2015, http://arstechnica.com/security/2015/10/the-rise-of-the-zero-day-market/ (accessed July 24, 2016).

47 Andy Greenberg, "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploit," Forbes, March 23, 2012, http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/#2715e4857a0b59367f060335 (accessed July 24, 2016).

48 Kim Zetter, "Hacking Team Leak Shows How Secretive Zero Day Exploit Sales Work," Wired, July 24, 2015, http://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/ (accessed July 24, 2016).

49 "Vupen Security: The Golden Boys of Malware," Insider Surveillance, December 4, 2014, https://insidersurveillance.com/vupen-security-the-golden-boys-of-malware/ (accessed July 24, 2016).

50 Danielle Walker, "NSA Sought Services of French Security Firm, Zeroday Seller Vupen," SC Magazine, September 18, 2013, http://www.scmagazine.com/nsa-sought-services-of-french-security-firm-zeroday-seller-vupen/article/312266 (accessed July 24, 2016);

David Fidler, "Zero-Sum Game: The Global Market for Software Exploits," Arms Control Law, July 18, 2013, http://armscontrollaw.com/2013/07/18/zero-sum-game-the-global-market-for-software-exploits/ (accessed July 24, 2016).

51 Ryan Gallagher, "Cyberwar's Gray Market," Slate, January 16, 2013, http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html (accessed July 24, 2016).

52 "Definition - What Does Payload Mean?" Technopedia, https://www.techopedia.com/definition/5381/payload (accessed July 24, 2016).

53 Andrew Cencini, Kevin Yu, and Tony Chan. "Software Vulnerabilities: Full-, Responsible-, and Non-Disclosure," University of Washington, December 7, 2005, available at http://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/software_vulnerabilities_by_cencini_yu_chan.pdf (accessed July 24, 2016).

54 Stephen A. Shepherd, "Vulnerability Disclosure: How Do We Define Responsible Disclosure?" SANS GIAC SEC Practical, (April 2003): 6, available at https://www.sans.org/reading-room/whitepapers/threats/defineresponsible-disclosure-932 (accessed July 24, 2016).

55 In a public forum such as a web posting or a semi-public resource like the electronic mailing list Bugtraq. Archives for this mailing list can be found at http://www.securityfocus.com/archive/1 (accessed July 24, 2016).

56 Bruce Schneier, "Schneier: Full Disclosure of Security Vulnerabilities a Damned Good Idea," CSO Online, January 9, 2007, http://www.csoonline.com/article/2121803/application-security/schneier--fulldisclosure-of-security-vulnerabilities-a--damnedgood-idea-.html (accessed July 24, 2016).

57 Shepherd, 7.

58 "Microsoft Security Response Center," Microsoft TechNet.

59 Scott Culp, "It's Time to End Information Anarchy," Microsoft TechNet, October 2001, Archived at http://www.angelfire.com/ky/microsfot/timeToEnd.html (accessed July 24, 2016).

60 Shepherd, 8.

61 Cencini, Yu, and Chan, 6.

62 Russell Brandom, "How Do You Fix Two-Thirds of the Web in Secret?" The Verge, April 10, 2014, http://www.theverge.com/2014/4/10/5601576/how-do-you-fix-two-thirds-of-the-web-in-secret (accessed July 24, 2016).

63 Researchers can gain notoriety, which can even lead to job offers. see e.g., Joseph Menn and Heather Somerville, "Uber Hires Two Security Researchers to Improve Car Technology", Reuters, August 28, 2015, http://www.reuters.com/article/2015/08/28/ubertech-security-idUSL1N1131T120150828 (accessed accessed July 24, 2016).

64 See, e.g., Hacker One, https://hackerone.com/ (accessed July 24, 2016) .

65 In some contexts "patches" may also refer to software updates that add new features or make other changes to the software, but in the security context, we use the term specifically to refer to those that eliminate security vulnerabilities. Tim Fisher, "Patch: Definition of a Patch or Hot Fix," About Tech, http://pcsupport.about.com/od/termsp/g/patch-fix.htm (accessed July 24, 2016).

66 Shaun Waterman, “Microsoft XP’s cybersecurity problem”, Politico, April 7, 2014, avialable at http://www.politico.com/story/2014/04/microsoft-xp-cybersecurity-problem-105451 (accessed July 24, 2016);

Craig Timberg and Ellen Nakashima, “Government Computers Running Windows XP Will Be Vulnerable to Hackers After April 8,” Washington Post, March 16, 2014, https://www.washingtonpost.com/business/technology/government-computers-running-windows-xp-will-be-vulnerable-to-hackers-after-april-8/2014/03/16/9a9c8c7c-a553-11e3-a5fa-55f0c77bf39c_story.html (accessed July 24, 2016).

67 “2015 State of Vulnerability Risk Management,” NopSec, June 2015: 3, available at http://info.nopsec.com/rs/736-UGK-525/images/NopSec_StateofVulnRisk_WhitePaper_2015.pdf shows that average time from report to patch is 176 days (accessed July 24, 2016).

68 “Microsoft Security Intelligence Report: July-December 2014,” Microsoft, available at https://www.microsoft.com/security/sir/archive/ (accessed July 24, 2016);

“internet Security Threat Report 10,” Symantec, available at https://www.symantec.com/security_response/publications/threatreport.jsp (accessed July 24, 2016);

Peter Mell, Tiffany Bergeron, and David Henning, “Creating a Patch and Vulnerability Management Program,” National Institute of Standards and Technology (NIST), November, 2005, http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf (accessed July 24, 2016).

69 For example, Google has been moving more and more of the security related software on Android into “Google Play Services” that they can update more quickly. Alex Dobie, “The Genius of Google Play Services, Tackling Android Fragmentation, Malware, and Forking in One Fell Swoop,” Android Central, June 24, 2015, http://www.androidcentral.com/genius-google-play-services (accessed July 24, 2016).

70 Steven J. Vaughan-Nichols , “Windows 10 Automatic Updates: Get Over It,” ZDnet, August 3, 2015, http://www.zdnet.com/article/windows-10-automatic-updates-get-over-it/ (accessed July 24, 2016).

71 Casey Johnston, “The Checkered, Slow History of Android Handset Updates”, Ars Technica, December 21, 2012, http://arstechnica.com/gadgets/2012/12/the-checkered-slow-history-of-android-handset-updates/ (accessed July 24, 2016).

72 Todd Shields, “Apple, Google, and Mobile Carriers Asked About Security Fixes,” Bloomberg, May 9, 2016, http://www.bloomberg.com/news/articles/2016-05-09/apple-google-and-wireless-carriers-asked-by-u-s-about-security (accessed July 24, 2016).

73 Andy Greenberg, “The 5 Most Dangerous Software Bugs of 2014,” Wired, December 29, 2014, http://www.wired.com/2014/12/most-dangerous-software-bugs-2014/ (accessed July 24, 2016).

74 Danny Yadron, “After Heartbleed Bug, a Race to Plug internet Hole”, Wall Street Journal, April 9, 2014, http://www.wsj.com/articles/SB10001424052702303873604579491350251315132 (accessed July 24, 2016).

75 Ross Schulman, “Forget Information Sharing: If Congress is Worried About Cybersecurity, it Should Start by Changing These Three Laws,” Slate, October 15, 2015,

http://www.slate.com/articles/technology/future_tense/2015/10/congress_should_change_these_three_laws_to_protect_cybersecurity.html (accessed July 24, 2016); Trey Ford, Marcia Hofmann, and Kevin Bankston, “The Big Chill: Legal Landmines that Stifle Security Research and How to Disarm Them,” [presentation, Black Hat USA 2014, Los Vegas, NV, August 6, 2014] available at https://www.youtube.com/watch?v=8UUIFyr-85Q (accessed July 24, 2016).

76 “The Computer Fraud and Abuse Act Hampers Security Research,” Electronic Frontier Foundation, https://www.eff.org/files/filenode/cfaa-security-researchers.pdf (accessed July 24, 2016);

Robyn Greene, “Addressing Computer Crime: Whitehouse Amendment No. 2626 Undermines Cybersecurity and Over-Penalizes Vague Legal Violations,” New America’s Open Technology Institute, August 15, 2015, https://www.newamerica.org/oti/wrong-approach-for-addressing-computer-crime-whitehouse-amendment-no-2626/ (accessed July 24, 2016).

77 Edward Felten, “The Chilling Effects of the DMCA,” Slate, March 25, 2013, http://www.slate.com/articles/technology/future_tense/2013/03/dmca_chilling_effects_how_copyright_law_hurts_security_research.html (accessed July 24, 2016); “Unintended Consequences: Fifteen Years under the DMCA,” Electronic Frontier Foundation, March 2013, https://www.eff.org/pages/unintended-consequences-fifteen-years-under-dmca (accessed July 24, 2016).

78 See, e.g..Kim Zetter, “AT&T Hacker ‘Weev’ Sentenced to 3.5 Years in Prison,” Wired, March 18, 2013, http://www.wired.com/2013/03/att-hacker-gets-3-years/ (accessed July 24, 2016); Jamie Williams, “Keys Case Spotlights Flaws of Computer Hacking Law,” Electronic Frontier Foundation, January 12, 2016, https://www.eff.

org/deeplinks/2016/01/keys-case-spotlights-flaws-computer-hacking-law (accessed July 24, 2016); Orin Kerr, “The Criminal Charges Against Aaron Swartz (Part 1: The Law),” The Volokh Conspiracy, January 14, 2013, http://volokh.com/2013/01/14/aaron-swartz-charges/ (accessed July 24, 2016).

[79] “Statement on Legal Impediments to Cybersecurity Research,” May 1, 2015, available at http://www.ischool.berkeley.edu/files/cybersecurity-statement-rev9.pdf (accessed July 24, 2016).

[80] See e.g. United States v. Drew, 259 F.R.D. 449 (C.D. Cal., 2008) (prosecution of woman for using a fake name on Myspace in violation of that site’s Terms of Use); Marcia Hoffman and Rainey Reitman, “Rebooting Computer Crime Law Part 1: No Prison Time for Violating Terms of Service”, Electronic Frontier Foundation, February 4, 2013, https://www.eff.org/deeplinks/2013/01/rebooting-computer-crime-law-part-1-no-prison-time-for-violating-terms-of-service (accessed July 24, 2016); Esha Bhandari and Rachel Goodman, “ACLU Challenges Computer Crimes Law That is Thwarting Research on Discrimination Online”, ACLU Free Future, June 29, 2016, https://www.aclu.org/blog/free-future/aclu-challenges-computer-crimes-law-thwarting-research-discrimination-online (accessed July 24, 2016).

[81] “Legal Threats Against Security Researchers,” Attrition.org: Security Community Errata, June 18, 2016, http://attrition.org/errata/legal_threats/ (accessed July 24, 2016).

[82] Dan Goodin, “Lawyers Threaten Researcher Over Key-Cloning Bug in High-Security Lock,” Wired, May 5, 2015, http://arstechnica.com/security/2015/05/lawyers-threaten-researcher-over-key-cloning-bug-in-high-security-lock/ (accessed July 24, 2016); Cyberlaw Clinic, “Petition of a Coalition of Medical Device Researchers for Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies,” Berkman Center for Internet and Society, September 17, 2014, available at https://www.eff.org/files/2014/11/04/medical_device_research_coalition_petition.pdf (accessed July 24, 2016); Kit Walsh, “Jeep Hack Shows Why the DMCA Must Get Out of the Way of Vehicle Security Research,” Electronic Frontier Foundation, July 21, 2015, https://www.eff.org/deeplinks/2015/07/jeep-hack-shows-why-dmca-must-get-out-way-vehicle-security-research (accessed July 24, 2016).

[83] “EFF Lawsuit Takes on DMCA Section 1201: Research and Technology Restrictions Violate the First Amendment,” Electronic Frontier Foundation, July 21, 2016, https://www.eff.org/press/releases/eff-lawsuit-takes-dmca-section-1201-research-and-technology-restrictions-violate (accessed July 24, 2016).

[84] See, e.g., Marcia Hofmann, “Court Rejects Argument That All First-Time Email Hacking Offenses Are Felonies,” Electronic Frontier Foundation, April 21, 2011, https://www.eff.org/deeplinks/2011/04/court-rejects-argument-that-all-first-time-email (accessed Juy 25, 2016).

[85] “About Us, The Wassenaar Arrangement,” http://www.wassenaar.org/about-us/ (accessed July 24, 2016).

[86] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, List of Dual-Use Goods, 89 (2013), http://www.wassenaar.org/wp-content/uploads/2016/07/WA-LIST-15-1-CORR-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf (accessed July 24, 2016); “A Guide to the Wassenaar Arrangement”, New America’s Open Technology Institute, December 9, 2013, http://www.newamerica.org/oti/blog/a-guide-to-the-wassenaar-arrangement/.

[87] Alastair Stevenson, “A Tiny Change to This Obscure Arms Dealing Agreement Could Kill the Cyber Security Industry,” Business Insider, July 22, 2015, http://www.businessinsider.com/the-wassenaar-arrangement-cyber-weapons-proposal-will-kill-international-security-research-2015-7 (accessed July 24, 2016).

[88] See, e.g., Access Now, Center for Democracy & Technology, Collin Anderson, Electronic Frontier Foundation, Human Rights Watch, and New America’s Open Technology Institute, “Comments to the U.S. Department of Commerce on Implementation of 2013 Wassenaar Arrangement Plenary Agreements,” July 20th, 2015, available at https://static.newamerica.org/attachments/4409-comments-on-wassenaar-implementation/JointWassenaarComments-FINAL.66518daf50e54d1c96f16e64b967f718.pdf (accessed July 24, 2016); Neil Martin and Tim Willis, “Google, the Wassenaar Arrangement, and Vulnerability Research”, Google Security Blog, July 20, 2015, https://security.googleblog.com/2015/07/google-wassenaar-arrangement-and.html (accessed July 24, 2016).

[89] Katie Bo Williams, “House Oversight Presses Kerry to Renegotiate Cyber Controls,” The Hill, February 8, 2016, http://thehill.com/policy/cybersecurity/268641-house-oversight-presses-kerry-to-renegotiate-hacking-export-agreement (accessed July 24, 2016).

[90] “Chrome Reward Program Rules,” Google Application Security, https://www.google.com/about/appsecurity/chrome-rewards/ (accessed July 24, 2016).

[91] Andy Greenberg, “The Zero-Day Salesmen,”

Forbes, March 28, 2012, http://www.forbes.com/global/2012/0409/technology-hackers-security-government-zero-day-salesmen.html (accessed July 24, 2016).

92 Greenberg, "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits."

93 Andy Greenberg, "Spy Agency Contractor Puts Out a $1M Bounty for an iPhone Hack," Wired, September 21, 2015, http://www.wired.com/2015/09/spy-agency-contractor-puts-1m-bounty-iphone-hack/ (accessed July 24, 2016).

94 Andy Greenberg, "Hacking Team Breach Shows a Global Spy Firm Run Amok," Wired, July 6, 2015, https://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok (accessed July 24, 2016).

95 Cyrus Farivar, "DEA, U.S. Army Bought $1.2M Worth of Hacking Tools in Recent Years," Ars Technica, April 16, 2015, http://arstechnica.com/tech-policy/2015/04/dea-us-army-bought-1-2m-worth-of-hacking-tools-in-recent-years/ (accessed July 24, 2016).

96 Kim Zetter, "Hacking Team's Leak Helped Researchers Hunt Down a Zero-Day," Wired, January 13, 2016, https://www.wired.com/2016/01/hacking-team-leak-helps-kaspersky-researchers-find-zero-day-exploit/ (accessed July 24, 2016).

97Lorenzo Franceschi-Bicchierai, "WikiLeaks Exposes Countries That Use Controversial 'FinFisher' Surveillance Tech," Mashable, September 15, 2014, http://mashable.com/2014/09/15/wikileaks-finfisher-customers-surveillance/#Y7Y8fHkznOqk (accessed July 24, 2016); Dennis Fisher, "EU Lawmaker Wants Answers on Hacking Team Sales to Sanctioned Countries," Threat Post, July 7, 2015, https://threatpost.com/eu-lawmaker-wants-answers-on-hacking-team-sales-to-sanctioned-countries/113638/ (accessed July 24, 2016).

98 "Navy Solicitation for Common Vulnerability Exploit Products," available at https://www.eff.org/document/navy-soliciation-common-vulnerability-exploit-products (June 9, 2016); Nicole Perlroth and David E. Sanger, "Nations Buying as Hackers Sell Flaws in Computer Code," New York Times, July 13, 2013, http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?_r=0 (accessed July 24, 2016);

99 Violet Blue, "Top Gov't Spyware Company Hacked; Gamma's FinFisher Leaked," ZDNet, August 6, 2014, http://www.zdnet.com/article/top-govt-spyware-company-hacked-gammas-finfisher-leaked/ (accessed July 24, 2016).

100 Tim Cushing, "French Company That Sells Exploits To The NSA Sat On An internet Explorer Vulnerability For Three Years," Tech Dirt, August 1, 2014, https://www.techdirt.com/articles/20140725/11013528006/french-company-that-sells-exploits-to-nsa-sat-internet-explorer-vulnerability-three-years.shtml (accessed July 24, 2016).

101 Greenberg, "Hacking Team Breach Shows a Global Spy Firm Run Amok."

102 Dennis Fisher, "ReVuln Emerges as New Player in Vulnerability Sales Market," Tech Dirt, October 12, 2012, https://threatpost.com/revuln-emerges-new-player-vulnerability-sales-market-101212/77112/ (accessed July 24, 2016).

103 Brian Krebs, "Got $90,000? A Windows 0-Day Could Be Yours," Krebs on Security, May 31, 2016, http://krebsonsecurity.com/2016/05/got-90000-a-windows-0-day-could-be-yours/ (accessed July 24, 2016); Dan Goodin, "Firm stops selling exploits after delivering Flash 0-day to Hacking Team," Ars Technica, July 20, 2015, http://arstechnica.com/security/2015/07/firm-stops-selling-exploits-after-delivering-flash-0-day-to-hacking-team/ (accessed July 24, 2016).

104 Andy Greenberg, "Inside Endgame: A Second Act For The Blackwater Of Hacking," Forbes, February 12, 2014, http://www.forbes.com/sites/andygreenberg/2014/02/12/inside-endgame-a-new-direction-for-the-blackwater-of-hacking/#1325308052d9 (accessed July 24, 2016).

105 Charlie Osborne, "In Hacking Team's Wake, FinFisher Spyware Rises in Popularity with Government Users," ZDNet, October 9, 2015, http://www.zdnet.com/article/in-hacking-teams-wake-finfisher-spyware-rises-in-popularity-with-government-users/ (accessed July 24, 2016).

106 Amar Toor and Russell Brandom, "A Spy in the Machine: How a Brutal Government Used Cutting-Edge Spyware to Hijack One Activist's Life," The Verge, January 21, 2015, http://www.theverge.com/2015/1/21/7861645/finfisher-spyware-let-bahrain-government-hack-political-activist (accessed July 24, 2016).

107 Franceschi-Bicchierai, "WikiLeaks Exposes Countries That Use Controversial 'FinFisher' Surveillance Tech."

108 Access Now, Center for Democracy & Technology, Collin Anderson, Electronic Frontier Foundation, Human Rights Watch, and New America's Open Technology Institute, "Comments to the U.S. Department of Commerce on Implementation of 2013 Wassenaar Arrangement Plenary Agreements."

109 Ibid.

110 Lillian Ablon, Martin C. Libicki, Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," RAND National Security Research Division, March 25, 2014, page 39, available at http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf (accessed July 24, 2016).

111 Deloitte Insights, "Security Expert Marc Goodman on Cyber Crime," Wall Street Journal, ay 12, 2015, http://deloitte.wsj.com/cio/2015/05/12/security-expert-marc-goodman-on-cyber-crime/ (accessed July 24, 2016).

112 Greenberg, "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploit."

113 Andy Greenberg, "New Dark-web Market is Selling Zero Day Exploits to Hackers," Wired, April 17, 2015, https://www.wired.com/2015/04/therealdeal-zero-day-exploits/ (accessed July 24, 2016).

114 Nick Clayton, "Where to Rent a Botnet for $2 an Hour or Buy One for $700," Wall Street Journal, November 5, 2012, http://blogs.wsj.com/tech-europe/2012/11/05/where-to-rent-a-botnet-for-2-an-hour-or-buy-one-for-700/ (accessed July 25, 2016). A Distributed Denial of Service attack is a flood of traffic sent by a distributed botnet that effectively disables access to a given website. US-CERT, Understanding Denial of Service Attacks, Nov. 4, 2009, https://www.us-cert.gov/ncas/tips/ST04-015 (accessed July 24, 2016).

115 Ablon, Libicki, and Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar."

116 Ibid.

117 Rob Waugh, "Scareware: It's Back, and Now It's Even Scarier," We Live Security, August 21, 2014, http://www.welivesecurity.com/2014/08/21/scareware-back-now-scarier/ (accessed July 24, 2016).

118 Paul Gil, "Malware 101: Understanding the Secret Digital War of the internet," About Tech, http://netforbeginners.about.com/od/antivirusantispyware/a/malware101.htm (accessed July 24, 2016).

119 Blue, "Top Gov't Spyware Company Hacked; Gamma's FinFisher Leaked."

120 Tim Cushing, "French Company That Sells Exploits To The NSA Sat On An internet Explorer Vulnerability For Three Years," Tech Dirt, August 1, 2014, https://www.techdirt.com/articles/20140725/11013528006/french-company-that-sells-exploits-to-nsa-sat-internet-explorer-vulnerability-three-years.shtml (accessed July 24, 2016).

121 Greenberg, "Hacking Team Breach Shows a Global Spy Firm Run Amok."

122 Dennis Fisher, "ReVuln Emerges as New Player in Vulnerability Sales Market," Tech Dirt, October 12, 2012, https://threatpost.com/revuln-emerges-new-player-vulnerability-sales-market-101212/77112/ (accessed July 24, 2016).

123 Krebs, "Got $90,000? A Windows 0-Day Could Be Yours." Goodin, "Firm stops selling exploits after delivering Flash 0-day to Hacking Team."

124 See e.g., Jose Pagliery, "Meet Zerodium, the Company That Pays $1 Million for Apple Hacks," CNN Money, April 7, 2016, http://money.cnn.com/2016/04/07/technology/zerodium-apple-hacks/ (accessed July 24, 2016); Andy Greenberg, "Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees)," Forbes, March 21, 2012, http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/#68cf158c9448 (accessed July 24, 2016); Neal Ungerleider, "How Spies, Hackers, And the Government Bolster A Booming Software Exploit Market," Fast Company, May 1, 2013, http://www.fastcompany.com/3009156/the-code-war/how-spies-hackers-and-the-government-bolster-a-booming-software-exploit-market (accessed July 24, 2016).

125 Pagliery, "Meet Zerodium, the Company That Pays $1 Million for Apple Hacks."; Greenberg, "Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees)."; Neal Ungerleider, "How Spies, Hackers, And the Government Bolster A Booming Software Exploit Market," Fast Company, May 1, 2013, http://www.fastcompany.com/3009156/the-code-war/how-spies-hackers-and-the-government-bolster-a-booming-software-exploit-market (accessed July 24, 2016); Lucian Constantin, "Cost of a Windows Zero-Day Exploit? This One Goes for $90,000," CIO, June 1, 2016, http://www.cio.com/article/3077861/cost-of-a-windows-zero-day-exploit-this-one-goes-for-90000.html (accessed July 24, 2016).

126 "The Enimies of the internet: Trovicor," Reporters without Borders, http://surveillance.rsf.org/en/trovicor/ (accessed July 24, 2016); Vernon Silver and Ben Elgin, "Torture in Bahrain Becomes Routine With Help From Nokia Siemens," Bloomberg Markets, August 22, 2011, http://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking (accessed July 24, 2016); "Monitoring the Opposition: Siemens Allegedly Sold Surveillance Gear to Syria," Spiegel Online International, April 11, 2012, http://www.spiegel.de/international/

business/ard-reports-siemens-sold-surveillance-technology-to-syria-a-826860.html (accessed July 24, 2016).

127 "The Enimies of the internet: Amesys," Reporters without Borders, http://surveillance.rsf.org/en/amesys/ (accessed July 24, 2016); Paul Sonne and Margaret Coker, "Firms Aided Libyan Spies," Wall Street Journal, August 30, 2011, http://www.wsj.com/articles/SB10001424053111904199404576538721260166388 (accessed July 24, 2016).

128 Netragard only sold its products to buyers within the United States. Ungerleider, "How Spies, Hackers, and the Government Bolster A Booming Software Exploit Market."

129 Vupen sold its products to NATO governments and "NATO partners" - an undefined list of counties. Greenberg, "The Zero-Day Salesmen."

130 Gallagher, "Cyberwar's Gray Market."

131 Greenberg, "Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees)."

132 Tim Lisko, "Cybersecurity as Realpolitik by Dan Geer," Privacy Wonk, November 20, 2014, https://www.privacywonk.net/2014/11/cybersecurity-as-realpolitik-by-dan-geer.php (accessed July 24, 2016).

133 The first such program was created by Netscape in 1995 to find bugs in the beta versions of Netscape 2.0. "Netscape Announces Netscape Bugs Bounty with Release of Netscape Navigator 2.0 Beta," October 10, 1995, https://web.archive.org/web/19970501041756/www101.netscape.com/newsref/pr/newsrelease48.html (accessed July 24, 2016).

134 Matthew Finifter, Devdatta Akhawe, and David Wagner, "An Empirical Study of Vulnerability Rewards Programs," USENIX Security Symposium, August 2013, 273, available at https://0b4af6cdc2f0c5998459-c0245c5c937c5dedcca3f1764ecc9b2f.ssl.cf2.rackcdn.com/12309-sec13-paper_finifter.pdf (accessed July 24, 2016).

135 See e.g., "An Update on Our Bug Bounty Program," Facebook, August 2, 2013, https://www.facebook.com/notes/facebook-security/an-update-on-our-bug-bounty-program/10151508163265766/ (accessed July 24, 2016).

136 "Tipping Point Zero Day Initiative," http://www.zerodayinitiative.com/about/ (accessed July 24, 2016).

137 "Microsoft Bounty Programs," Microsoft TechNet, https://technet.microsoft.com/en-us/library/dn425036.aspx (accessed July 24, 2016).

138 "Facebook Security's Bug Bounty Program," Facebook, https://www.facebook.com/BugBounty (accessed July 24, 2016).

139 Sara Sorcher, "How Much is a Security Flaw Worth? An Inside Look Into Yahoo's Bug Bounty Program", Christian Science Monitor, May 16, 2016, http://www.csmonitor.com/World/Passcode/Security-culture/2016/0513/How-much-is-a-security-flaw-worth-An-inside-look-into-Yahoo-s-bug-bounty-program (accessed July 24, 2016).

140 "Google Vulnerability Reward Program (VRP) Rules," Google Application Security, https://www.google.com/about/appsecurity/reward-program/ (accessed July 24, 2016).

141 "Tipping Point Zero Day Initiative."

142 "About HackerOne," HackerOne, April 14th, 2015, https://hackerone.com/about (accessed July 24, 2016).

143 Since its inception in 2012, HackerOne reports paying out over $3.3 million for vulnerabilities.

144 Dan Goodin, "All Four Major Browsers Take a Stomping at pwn2own Hacking Competition," Ars Technica, March 20, 2015, http://arstechnica.com/security/2015/03/all-four-major-browsers-take-a-stomping-at-pwn2own-hacking-competition/ (accessed July 24, 2016).

145 Katie Moussouris, "New Markets: Putting a Bounty on Vulnerabilities." [presentation, Cybersecurity for a New America, Washington, DC, February 23, 2015] available at https://www.youtube.com/watch?v=U7vru9_ahGc (accessed July 24, 2016).

146 Katie Moussouris, "The Wolves of Vuln Street - The First System Dynamics Model of the oday Market," HackerOne, April 14th, 2015, https://hackerone.com/blog/the-wolves-of-vuln-street (accessed July 24, 2016).

147 "The Rapid Growth of the Bug Bounty Economy," HelpNet Security, https://www.helpnetsecurity.com/2015/08/03/the-rapid-growth-of-the-bug-bounty-economy (accessed July 24, 2016); Mike Lennon, "Bugcrowd Raises $15 Million to Expand Bug Bounty Business," Security Week, April 20, 2016,

http://www.securityweek.com/bugcrowd-raises-15-million-expand-bug-bounty-business (accessed July 24, 2016).

148 Chris Soghoian and Sonia Roubini, "Feds Refuse to Release Documents on "Zero-Day" Security Exploits," ACLU, March 3, 2015, https://www.aclu.org/blog/feds-refuse-release-documents-zero-day-security-exploits

(accessed July 24, 2016).

149 Ryan Naraine, “Stuxnet Attackers Used 4 Windows Zero-day Exploits, ZDNet, Sep. 14, 2010, http://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/ (accessed July 24, 2016)

150 Office of the Director of National Intelligence and National Security Agency, “Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process,” released under a Freedom of Information Act request filed by the Electronic Frontier Foundation, available at https://www.eff.org/document/vulnerabilities-equities-process-redactions; other documents detailing this process available at https://www.eff.org/cases/eff-v-nsa-odni-vulnerabilities-foia (accessed July 24, 2016).

151 Joseph Menn, “Special Report - U.S. Cyberwar Strategy Stokes Fear of Blowback,” Reuters, May 10, 2013, http://in.reuters.com/article/usa-cyberweapons-idINDEE9490AX20130510?type=economicNews (accessed July 24, 2016). (“the U.S. government…has become the biggest buyer in a burgeoning gray market where hackers and security firms sell tools for breaking into computers.”)

152 Ellen Nakishima, “Meet the Woman in Charge of the FBI’s Most Controversial High-Tech Tools,” Washington Post, December 8, 2015, https://www.washingtonpost.com/world/national-security/meet-the-woman-in-charge-of-the-fbis-most-contentious-high-tech-tools/2015/12/08/15adb35e-9860-11e5-8917-653b65c809eb_story.html (accessed July 24, 2016); Andrea Peterson, “The NSA Has Its Own Team of Elite Hackers,” Washington Post, August 29, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers/ (accessed July 24, 2016).

153 Dan Geer, “Cybersecurity as Realpolitik,” [presentation, Black Hat USA 2014, Los Vegas, NV, August 6, 2014] text available at http://geer.tinho.net/geer.blackhat.6viii14.txt (accessed July 24, 2016); video available at https://www.youtube.com/watch?v=nT-TGvYOBpI (accessed July 24, 2016); Sean Gallagher, “CIA’s Venture Firm Security Chief: U.S. Should Buy Zero-Days, Reveal Them,” Ars Technica, August 6, 2014, http://arstechnica.com/security/2014/08/cias-venture-firm-security-chief-us-should-buy-zero-days-reveal-them/ (accessed July 24, 2016).

154 Richard Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein and Peter Swire, “Liberty and Security in a Changing World: Report and Recommendations of the President’s Review Group on Intelligence and Communications Technologies,” December 13, 2013: 219-220, available at https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (accessed July 24, 2016); Richard Clarke and Peter Swire, “The NSA Shouldn’t Stockpile Web Glitches,” The Daily Beast, April 18, 2014, http://www.thedailybeast.com/articles/2014/04/18/the-nsa-shouldn-t-stockpile-web-glitches.html (accessed July 24, 2016).

155 Joseph S. Nye Jr., “The World Needs New Norms on Cyberwarfare,” Washington Post, October 1, 2015, https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-cybersecurity/2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html (accessed July 24, 2016). (“[I]f the United States unilaterally adopted a norm of responsible disclosure of zero-days to companies and the public after a limited period, it would destroy their value as weapons—simultaneously disarming ourselves, other countries and criminals….”)

156 Angela McKay, Jan Neutze, Paul Nicholas, and Kevin Sullivan, “International Cybersecurity Norm: Reducing Conflict in an internet-dependent World,” Microsoft, December 2014: 12, available at http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf (accessed July 24, 2016).

157 Andrew Crocker, “FBI Breaks into iPhone. We Have Some Questions.” Electronic Frontier Foundation, March 28, 2016, https://www.eff.org/deeplinks/2016/03/fbi-breaks-iphone-and-we-have-some-questions (accessed July 25, 2016); Nate Cadozo and Andrew Crocker, “Guess Who Wasn’t Invited to the CIA’s Hacker Jamboree?” Electronic Frontier Foundation, March 10, 2015, https://www.eff.org/deeplinks/2015/03/guess-who-wasnt-invited-cias-hacker-jamboree (accessed July 25, 2016).

158 Michael Daniel, “Heartbleed: Understanding When We Disclose Cyber Vulnerabilities,” The White House, April 28, 2014, https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities (accessed July 24, 2016); Kim Zetter, “U.S. Gov Insists It Doesn’t Stockpile Zero-Day Exploits to Hack Enemies,” Wired, November 17, 2014, https://www.wired.com/2014/11/michael-daniel-no-zero-day-stockpile/ (accessed July 24, 2016).

159 Ibid.

160 See, e.g., Bruce Schneier, “Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?” The Atlantic, May 19, 2014, http://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploit-them/371197/ (accessed July 24, 2016); and Andrew Crocker, “FAQ: Apple, the FBI, and Zero Days,” Electronic Frontier Foundation, April 14, 2016, https://www.eff.org/deeplinks/2016/04/will-apple-ever-

find-out-how-fbi-hacked-phone-faq (accessed July 24, 2016); Ellen Nakashima, "Comey Defends FBI's Purchase of iPhone Hacking Tool," Washington Post, May 11, 2016, https://www.washingtonpost.com/world/national-security/comey-defends-fbis-purchase-of-iphone-hacking-tool/2016/05/11/ce7eae54-1616-11e6-924d-838753295f9a_story.html (accessed July 24, 2016).

161 Electronic Frontier Foundation v. NSA, ODNI, - Vulnerabilities FOIA," https://www.eff.org/cases/eff-v-nsa-odni-vulnerabilities-foia, (accessed July 24, 2016).

162 Ari Schwartz and Rob Knake, " Government's Role in Vulnerability Disclosure," Belfer Center for Science and International Affairs, Harvard Kennedy School, June 2016, available at http://belfercenter.ksg.harvard.edu/files/vulnerability-disclosure-web-final3.pdf (accessed July 24, 2016).

163 Ibid., 15.

164 Nakashima, "Comey Defends FBI's Purchase of iPhone Hacking Tool."

165 Kevin Bankston, "Privacy Groups Including OTI Unite to Oppose Expansion of Government Hacking Authority," New America's Open Technology Institute, November 5, 2014, https://www.newamerica.org/oti/blog/privacy-groups-including-oti-unite-to-oppose-expansion-of-government-hacking-authority/ (accessed July 24, 2016); "Testimony of Kevin S. Bankston, On Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure" Judicial Conference Advisory Committee on Criminal Rules, November 5, 2014, available at http://akdev.preview.newamerica.org/downloads/OTI_Rule_41_Testimony_11-05-14_final.pdf (accessed July 24, 2016); "OTI to Congress: Block New Government Hacking Proposal," New America's Open Technology Institute, April 28, 2016, http://www.newamerica.org/oti/press-releases/oti-to-congress-block-new-government-hacking-proposal/ (accessed July 24, 2016); "Written Statement of the Center for Democracy & Technology," Judicial Conference Advisory Committee on Criminal Rules, October 24, 2014, available at https://cdt.org/files/2014/10/CDT-Rule41-Written-Statement-final-20141024.pdf (accessed July 24, 2016); "Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media," Judicial Conference Advisory Committee on Criminal Rules, October 14, 2014, available at https://www.aclu.org/files/assets/aclu_comment_on_remote_access_proposal.pdf (accessed July 24, 2016).

166 Kevin Poulson, "Documents: FBI Spyware has Been Snaring Extortionists, Hackers for Years," Wired, April 16, 2014, https://www.wired.com/2009/04/fbi-spyware-pro/ (accessed July 24, 2016).

167 Joseph Cox, "How a Child Porn Case Became a Battle Over Government Secrets," Motherboard, May 19, 2016, https://motherboard.vice.com/read/how-a-child-porn-case-became-a-battle-over-government-secrets-playpen-hack (accessed July 21, 2016); Gene Johnson, "DOJ's Refusal to Turn over Code Complicates Child Porn Cases," Associated Press, June 24, 2016, http://bigstory.ap.org/article/3234210ba0fb4730abff9df6b789dfdf/dojs-refusal-turn-over-code-complicates-child-porn-cases (accessed July 24, 2016).

168 Joseph Cox, "Judge in FBI Hacking Case Is Unclear on How FBI Hacking Works," Motherboard, January 27, 2016, http://motherboard.vice.com/read/judge-in-fbi-hacking-case-is-unclear-on-how-fbi-hacking-works (accessed July 24, 2016).

169 See full citation for congressional testimony and comments at 165.

170 Steven M. Belovin, Matt Blaze, and Susan Landau. "Insecure Surveillance: Technical Issues with Remote Computer Searches." IEEE Computer Society, 49, no. 3 (2016): 14-24, available at https://computingnow.computer.org/cms/Computer.org/ComputingNow/issues/2016/06/mco2016030014.pdf (accessed July 24, 2016).

171 Moussouris, "The Wolves of Vuln Street - The First System Dynamics Model of the oday Market."

172 Moussouris, "The Wolves of Vuln Street - The First System Dynamics Model of the oday Market."

173 "Multistakeholder Process: Cybersecurity Vulnerabilities," U.S. Department of Commerce National Telecommunications and Information Administration, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities (accessed July 24, 2016).

174 "FTC To Study Mobile Device Industry's Security Update Practices," U.S. Federal Trade Commission, May 9, 2016, https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices (accessed July 24, 2016).

175 Malena Carolo, "Influencers: Lawsuits to Prevent Reporting Vulnerabilities Will Chill Research," Christian Science Monitor, September 29, 2015, http://passcode.csmonitor.com/influencers-research (accessed July 24, 2016); "Legal Threats Against Security Researchers," Attrition.org: Security Community Errata, June 18, 2016, http://attrition.org/errata/legal_threats/ (accessed July 24, 2016).

176 See e.g., "PayPal Bug Bounty Program: Responsible

Disclosure Policy," PayPal, https://www.paypal.com/us/webapps/mpp/security-tools/reporting-security-issues#responsible-disclosure-policy (accessed June 21, 2016); "GoDaddy Responsible Disclosure Policy and Bug Bounty Program," GoDaddy, June 26, 2015, https://in.godaddy.com/hi/agreements/showdoc.aspx?pageid=16284 (accessed July 24, 2016); GitHub Security Bug Bounty: Rules," GitHub, https://bounty.github.com/#rules (accessed July 24, 2016); "BugCrowd: Tesla Motors," Bug Crowd, https://bugcrowd.com/tesla (accessed July 24, 2016).

177 See e.g., "Mitnick Released From Prison," Cnet, March 24, 2002, http://www.cnet.com/news/mitnick-released-from-prison/ (accessed July 24, 2016); Kim Zetter, "Whistle-Blower Faces FBI Probe," Wired, July 29, 2005, http://archive.wired.com/politics/security/news/2005/07/68356?currentPage=all (accessed July 24, 2016); Dissent Doe, "FBI Raids Dental Software Researcher Who Discovered Private Patient Data on Public Server," The Daily Dot, May 27, 2016, http://www.dailydot.com/politics/justin-shafer-fbi-raid/ (accessed July 24, 2016); Kim Zetter, "AT&T Hacker 'Weev' Sentenced to 3.5 Years in Prison," Wired, March 18, 2013, https://www.wired.com/2013/03/att-hacker-gets-3-years/ (accessed July 24, 2016); Kerr, "The Criminal Charges Against Aaron Swartz (Part 1: The Law)."

178 Corynne McSherry and Marcia Hofmann, "Sony v. Hotz: Sony Sends A Dangerous Message to Researchers—and Its Customers," Electronic Frontier Foundation, January 19, 2011, https://www.eff.org/deeplinks/2011/01/sony-v-hotz-sony-sends-dangerous-message (accessed July 24, 2016);

179 "Statement on Legal Impediments to Cybersecurity Research."

180 Aaron's Law Act of 2015, HR 1918, 114th Cong., available at https://www.congress.gov/bill/114th-congress/house-bill/1918 (accessed July 24, 2016).

181 Mark Jaycox, Kurt Opsahl, and Trevor Timm, "Aaron's Law Introduced: Now Is the Time to Reform the CFAA," Electronic Frontier Foundation, June 20, 2013, https://www.eff.org/deeplinks/2013/06/aarons-law-introduced-now-time-reform-cfaa (accessed July 24, 2016).

182 See, e.g., Steven M. Bellovin, Matt Blaze, Edward W. Felten, J. Alex Halderman, and Nadia Heninger, "Petition for Proposed Exemption Under 17 U.S.C. § 1201," available at http://copyright.gov/1201/2014/petitions/Bellovin_1201_Intial_Submission_2014.pdf (accessed July 24, 2016).

183 "Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65, 944 (Oct. 28, 2015) (amending 37 CFR 201) available at https://www.federalregister.gov/articles/2015/10/28/2015-27212/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control (accessed July 24, 2016).

NEW AMERICA