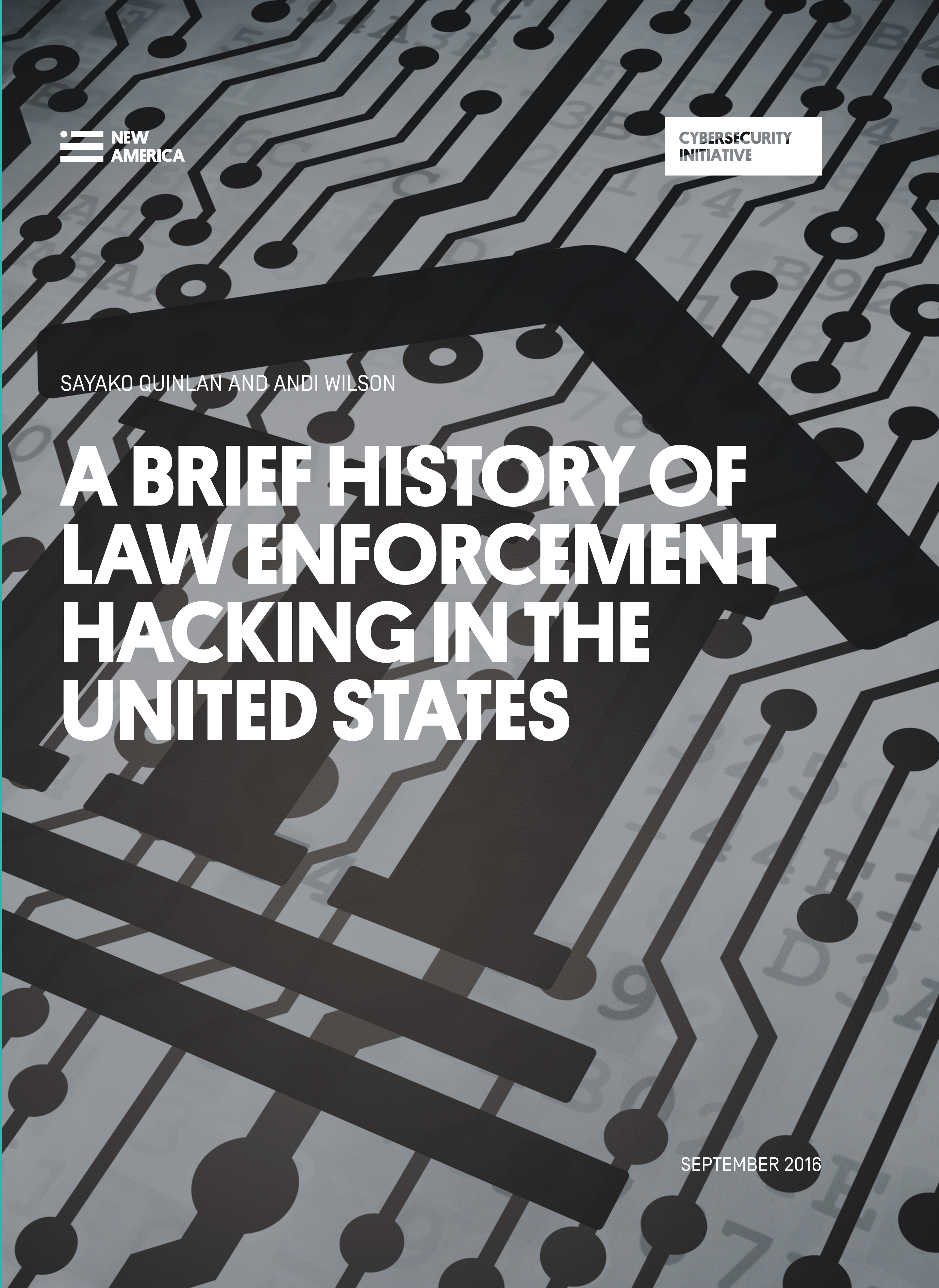

NEW
AMERICA

CYBERSECURITY
INITIATIVE

SAYAKO QUINLAN AND ANDI WILSON

A BRIEF HISTORY OF LAW ENFORCEMENT HACKING IN THE UNITED STATES

SEPTEMBER 2016

About the Authors

Sayako Quinlan is a former intern at New America's Cybersecurity Initiative, where she researched incidents around government hacking and the landscape for cyber capacity building. She is a junior at Georgetown University's School of Foreign Service, majoring in Science, Technology, and International Affairs with a concentration in Business Growth and Development. She is pursuing a career in cybersecurity.

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.

Acknowledgments

The authors appreciate the help and support of New America's staff, especially Emefa Agawu, Ethan Walker, Kayla Cross, Rob Morgus, Laura Bate, Ian Wallace, Robyn Greene, Alison Yost, Kevin Bankston, and Ross Schulman.

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 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**.

Contents

INTRODUCTION

Hacking by law enforcement has been front page news since the FBI purchased a tool to bypass the security of an encrypted iPhone while investigating the San Bernardino shooting. However, this type of hacking is nothing new: it has been over fifteen years since the first known case of police intrusion into a computer as part of an investigation.[1] While it is uncertain when this behavior began, we are sure that, as of 1999, that the government had begun to use technological skills to access private digital networks and material in the process of investigating crimes.[2] Hacking methods can be as simple as using a USB drive to install a malicious program, or tricking users into opening a phishing email, and as complex as tools that rely on previously unknown or "zero-day" vulnerabilities to allow a hacker to bypass the sophisticated security functions of a mobile phone's operating system.

Despite being a key tactic for law enforcement since the turn of the century, hacking didn't become a major topic of public discussion until the San Bernardino iPhone hack.[3] That case received such widespread media coverage that even the general public was talking about the ways that law enforcement could, or could not, access the devices that we all carry in our pockets. But the repercussions of investigative hacking are unclear, and important questions must be asked when evaluating policy options to address the issue: what procedural and substantive standards must be met when the government seeks authorization to hack? Under what legal authority can this type of hacking be authorized? Could the hack damage the targeted device or infect untargeted devices? How can the privacy of third parties be protected when investigating a single individual? Should law enforcement be able to target only specific individuals, or everyone that visits a particular website or uses a particular service? How should law enforcement minimize the collection of data that isn't relevant to their investigation? These are all critical questions, yet law enforcement has taken very few steps to provide clear information about their procedures, tools, or tactics when it comes to their hacking activities.[4]

Understanding the history of government hacking is important in order to engage more people in the on-going policy discussion. This paper focuses on a selection of illustrative historical cases, with the understanding that due to the secret nature of government investigations, we can only know a fraction of the hacking that has taken place. This overview highlights major trends in investigative hacking and will hopefully foster more inquiries into these practices by policymakers and the public.

HACKING THE MOB WITH KEYLOGGERS

The first known case of hacking by U.S. law enforcement was in an investigation into the Italian-American mafia. In January 1999, the FBI searched the New Jersey property of Nicodemo Scarfo, who was under suspicion of running an illegal gambling business. When agents downloaded the contents of Scarfo's computer, one file was encrypted, using a program called "Pretty Good Privacy" or PGP.[5] Agents believed this to be the file containing the bookmaking information that would have incriminated Scarfo, but it was not enough evidence to arrest him.[6]

A few months after the initial search, in the spring of 1999, the FBI secured a warrant to secretly install a Key Logger System (KLS) – technology that, as the name would suggest, had the ability to record what was typed into Scarfo's computer. The FBI hoped the tool would help retrieve the password to Scarfo's PGP key.

On May 10, 1999, after securing the key logging warrant, FBI agents snuck onto Scarfo's property and installed the technology onto his computer. After 14 days, the keylogger had collected the necessary data to decrypt his bookmaking file,[7] and Scarfo was arrested and charged. But in a two-year pretrial court fight, Scarfo challenged the legality of using the key logging software, claiming that the tool was akin to wiretapping and that the FBI had not obtained the proper warrant for its use.[8] In August 2001, the judge ordered the FBI to provide more information on exactly how the keylogging software worked. They responded by filing a memorandum claiming that the technology was classified, and that revealing specifics would make the keylogger useless in future cases.[9] The judge ultimately rejected the defense's argument to have that specific evidence excluded and, in March 2002, Scarfo pleaded guilty.[10]

During the Scarfo trial MSNBC reported on a new key logging software named "Magic Lantern" that the FBI could deliver remotely over email (unlike the keylogger used in the Scarfo case which had to be physically installed on the suspect's computer).[11] Technology that could be installed remotely was a new development, and showed a significant advancement in the hacking strategies used by U.S. law enforcement. Although there are no publicly available warrants that describe law enforcement deploying Magic Lantern, there was a case in 2007 of two ecstasy manufacturers using PGP, in which law enforcement used a keylogger that may have been remotely installed.[12] In that same year, an even newer forensic hacking tool, called CIPAV, started grabbing headlines.

HACKING A BOMB THREAT WITH CIPAV

On May 30, 2007, a handwritten bomb threat was discovered on the campus of Timberline High School in Washington state. The school was evacuated, but no bomb was found. On June 4th, an e-mail to the school warned that the school district would go offline and that day, the Lacey School District computer network was hit with a Denial-of-Service attack that brought down their computer network.[13] Over the next three days, the school received several bomb threats sent by e-mail from different accounts, all of which were traced to a hacked server based in Italy. At the same time, a MySpace account was created under the name "timberlinebombinfo" and added 33 Timberline students as friends. After each threat, the students were evacuated, but a bomb was never discovered.[14] Because the perpetrator was using a proxy server to obscure their true location, law enforcement could not simply request the user's information from MySpace – they had to get more high tech.

On June 12, the FBI secured a search warrant allowing them to use a Computer and Internet Protocol Address Verifier (CIPAV). In the search warrant affidavit, law enforcement stated that CIPAV would collect the suspect's computer Internet Protocol (IP) address, Media Access Control (MAC) address, operating system information, what internet browser they were using, their computer username, registered computer name, and internet history.[15] After sending this information back to the FBI, CIPAV would monitor the electronic communication activity—but not the content of the communications—of the computer for 60 days.[16] When a computer accesses a website, the computer sends information about itself to the website over the network to inform the website how a web page should display to the user. CIPAV exploits this function by diverting the information that the computer sends to an FBI server.[17]

The FBI deployed CIPAV by impersonating an Associate Press reporter and messaging the "timberlinebombinfo" MySpace account.[18] The message contained a link to a fake news article which, when clicked, allowed CIPAV to access the computer and send its information to an FBI server.[19] At this point, CIPAV remained on the suspect's computer to record its electronic communications for the next 60 days.[20]

The spyware was successful in revealing the true location of the computer that sent the bomb threats, and the FBI arrested a 15-year-old Timberline student who pleaded guilty to three charges related to the incident.[21] Based on public records, we know that the FBI has sought search warrants and Foreign Intelligence Surveillance Court orders to use CIPAV in at least eight criminal investigations since 2005, including cases that dealt with the impersonation of an FBI agent and the hacking of NASA's Jet Propulsion Laboratories.[22] As early as 2002, however, an internal memo was circulated warning law enforcement that overuse of this technique could result in exclusion of important evidence in court. This means that CIPAV has been popular for a long time, and much more so than the public records illustrate.

THE COURT PUSHES BACK ON A HACK

In March 2013, the FBI approached Magistrate Judge of the Southern District of Texas Stephen Smith with a warrant request to locate unidentified persons who had hacked into an email account belonging to a resident of the district. The victim had discovered that the hacker(s) had created an almost identical fake email address and tried to use it to wire money from victim's bank into a foreign account.[23]

The warrant requested authorization to install software onto the computer that was used to create the email address in order to identify the user, but in this case the FBI did not know where the computer they sought was located. The search warrant application did not clarify how the software would be deployed, although the judge speculated that it would be by contacting the fake email address.[24] However, the document did specify that the software would collect the computer's IP address, internet history, saved usernames and passwords, documents, chat messages, and other correspondence. The FBI would also record when the computer was in use, catalog which applications were running, monitor the computer's physical location, and periodically take photographs from the target computer's camera.[25]

Judge Smith rejected the warrant request. It could not be verified that the computer was in his district, a prerequisite to his being able to issue the warrant under Rule 41 of the Federal Rules of Criminal Procedure, and he also raised concerns that the requested search would violate the Fourth Amendment's protection against unreasonable search and seizure.[26] In addition, the judge denied the FBI's request to exploit the infected computer's camera to conduct video surveillance. Warrant requests for video surveillance require that the FBI prove that other less intrusive means of obtaining the sought evidence are either ineffective or infeasible. The FBI must also demonstrate that agents will employ measures to limit the video feed to only that which records the criminal act or identifies potential suspects. In this case, the FBI failed to meet either of these requirements.[27]

However, Judge Smith's denial of the warrant request is not binding in other cases. The government continues to seek, and obtain, warrants for such investigative hacking,[28] while also seeking changes to the federal rule on which Smith based his opinion.[29]

HACKING THE ONION ROUTER

Tor, short for The Onion Router,[30] is a network that disguises the identity of users by transmitting their internet traffic through a series of encrypted nodes. The computers that act as relays serve as "layers" (hence the name onion) of protection, ensuring that a user's original Internet Protocol address is masked so that they can browse anonymously. In addition to allowing anonymous browsing, Tor enables "hidden services", which allow for the anonymous publication of websites that aren't indexed by web searches, and hides their geographic location behind layers of routing.[31] Users can take advantage of the Tor technology in a variety of ways; the simplest is to use the Tor Browser, a version of Mozilla's open source Firefox web browser that integrates Tor functionality.[32]

Users of Tor and these hidden websites have long been targets of law enforcement hacking, even though many Tor users are law-abiding advocates, journalists, and human rights defenders trying to evade surveillance and censorship by repressive governments, or just average citizens trying to protect their privacy.[33] But Tor also appeals to criminal users,[34] and there are several known cases of the FBI targeting Tor websites or users in criminal investigations. For example, "Operation Onymous" was a coordinated effort between multiple international law enforcement agencies that targeted hidden websites selling drugs and other contraband, including Topix, Black Market, and Silk Road 2.0.[35] Although it is unclear what technology was used to infiltrate these organizations, the sheer number of Tor-hosted sites affected raised concerns about whether unknown vulnerabilities in Tor might have been exploited, as well as concerns that innocent Tor users had been compromised. When asked, a representative from Europol responded "This is something we want to keep for ourselves," he said. "The way we do this, we can't share with the whole world, because we want to do it again and again and again."[36]

The FBI has also targeted various organizations and individuals accused of facilitating the distribution of child pornography using Tor hidden service sites.[37] In 2012, the FBI was accused of exploiting a vulnerability in the Firefox browser to target Tor users who were connecting to sites hosted by Freedom Hosting, a web hosting service that operated within the Tor network and allegedly hosted child porn websites.[38] The malware was used to target the specific version of Firefox that makes up the basis of the Tor Browser Bundle, and included malware that would expose the user's real IP address.[39] The technology's behavior and the fact that the servers receiving the exposed IP addresses appeared to be based in Northern Virginia is consistent with what we know about CIPAV, a tool that was touched on earlier in the the paper. The targeting of Freedom Hosting users was of particular concern because it impacted countless users of legitimate Freedom Hosting-hosted services such as the private Tormail email service.[40]

Most recently, and at the largest scale we know of so far, the FBI infiltrated the child pornography website Playpen as part of an investigation called Operation Pacifier.[41] In the beginning of the investigation, the FBI struggled to identify who was running or using the website because, like some other known child pornography sites, it was using Tor. But in December 2014, a foreign law enforcement agency tipped off the FBI about an IP address associated with Playpen. After a month of investigation, FBI agents located, and, with a warrant, seized the North Carolina server that had hosted the website.[42] The FBI copied the contents of the server onto its own server in Virginia and became the host of Playpen, continuing to serve child pornography to the site's visitors.[43] On February 2nd, 2015, the FBI successfully applied for a search warrant to utilize a "network investigative technique" (NIT) to circumvent the anonymity of the Tor browser and identify the users on Playpen.[44] The NIT, although called a technique, is simply the latest version of the same type of surveillance software that the FBI has used since at least 2002 to investigate other crimes ranging from computer hacking to bomb threats.[45]

In this case, the malware was embedded in several of Playpen's forums that covered particular child pornography themes.[46] The NIT caused computers that accessed those Playpen forums to send their location and operating information to an FBI computer.[47] From February 20th to March 4th, the FBI hosted Playpen and collected over 1,300 "true" computer addresses that resulted in 137 individuals in the United States being charged for crimes related to child pornography.[48] The FBI's investigation did not only target computers in the United States, however. Remote searches under Operation Pacifier extended to Greece, Chile, Denmark, Colombia, and Austria.[49]

In the transcript from a January 2016 Playpen hearing in Washington state, the defense attorney questioned the legality of the search warrant that was issued to the FBI.[50] What authority did a judge in the Eastern District of Virginia have to approve a search that was executed thousands miles away on a computer in Washington state? On top of that, how could one search warrant legally have been carried out across multiple state lines (and even national borders) and be used to arrest over 100 individuals?[51] Defense attorneys in the Playpen cases have asked the government to reveal the technology behind the Playpen spyware, but the government has refused to share much information. Even Mozilla, the company associated with the Firefox browser, was not able to force the FBI to reveal the web browser security flaw it had exploited, even though the company argued that the exploit threatened its customers' security.[52] In response to the FBI's non-disclosure, or arguments that the FBI violated Rule 41, judges have thrown out the evidence obtained by the hacking tool in Playpen cases in Washington, Oklahoma, and Massachusetts.[53] However, in a Playpen case prosecuted in the same district where the warrant was issued, a judge ruled that the defendant was not entitled to the the spyware's source code and had no expectation of privacy online.[54] These conflicting rulings bring us back to the questions raised at the beginning of this paper – questions that the courts and Congress have yet to sort out.

> **When asked, a representative from Europol responded "This is something we want to keep for ourselves," he said. "The way we do this, we can't share with the whole world, because we want to do it again and again and again."**

HACKING THE SAN BERNARDINO IPHONE

On December 2, 2015, Syed Rizwan Farook and Tashfeen Malik attacked a holiday party at Farook's office in San Bernardino, California. The two individuals killed 14 people before being killed themselves in a shootout with law enforcement.[55] In an attempt to conceal information from law enforcement, the perpetrators erased and smashed their mobile phones and computer hard drives.[56] Left undestroyed was an iPhone 5C that was issued to Farook as a work phone by the city of San Bernardino.[57] Farook's iPhone had an encryption-enforced security feature set to erase all data from the hard drive after 10 failed attempts to key in a passcode, ensuring that any attempt by the FBI to try all possible passcode combinations (a method known as "brute forcing" the passcode) risked loss of potential evidence.[58] Sometimes law enforcement is able to access iPhone data, even from a locked device, when that data has been automatically backed up to Apple's iCloud servers. However in the hours after the shooting, the FBI inadvisedly asked a San Bernardino county technician to reset Farook's iCloud password, preventing the phone from backing up any new information.[59] Because of this mistake, only data from six week before the attack was recoverable. This left the FBI with only one option — find a way to hack the physical device.

In February 2016, the FBI obtained an order from a judge that required Apple to help law enforcement circumvent its software's auto-erase and passcode delay functions by modifying the operating system on Farook's phone.[60] Apple released a statement that it planned to appeal the order, arguing that the U.S. government was asking the company to put customers at risk by weakening the security of the iPhone.[61] This only intensified the debate on backdoors and encryption. Apple said that to comply with the FBI's request, the company would need to create a new version of the phone's operating system (iOS) that would allow law enforcement to break into the iPhone — a move that Apple stated would "undeniably create a backdoor."[62]

In response, many major tech companies, including Google, Facebook, Twitter, Yahoo, and Ebay, as well as advocacy groups, academics, and technical experts filed briefs in support of Apple's appeal.[63] This resulted in much debate about whether a company could or should be legally required to circumvent the security of their own product, and whether a concession from Apple would create legal precedent to undermine other technology in the future.[64] However, on the eve of court arguments, the Justice Department dropped its request for a court order compelling assistance from Apple: a third party had come forward and successfully helped law enforcement unlock the phone.[65] The FBI reportedly paid approximately $1 million for the hack.[66]

The San Bernardino iPhone hack is a public confirmation of the FBI's long-reported practice of purchasing hacking tools.[67] However, in a briefing with reporters, the FBI Director expressed a desire to "use the tool to help in other investigations,"[68] and the FBI refused to disclose any information to Apple about vulnerabilities in its iOS software. It also refused to submit the tool to the interagency government process—the so-called "Vulnerability Equities Process"—that decides when the government should disclose the vulnerabilities it buys or discovers.[69] And, contradicting the FBI's earlier claims that this was only about a single phone, local law enforcement agencies across the country have been requesting assistance to hack phones in their own cases.[70]

THE FUTURE OF HACKING

In April 2016, the Supreme Court submitted to Congress revisions to Rule 41 of the Federal Rules of Criminal Procedure, which regulates search warrants. These revisions aim to address the difficulties law enforcement faces when conducting investigations where suspects have used anonymizing technology.[71] Such technology includes the Tor browser service used in Playpen, or proxy servers like the one utilized by the student from Timberline High School. Two significant changes were introduced in these revisions: they allow a judge from any district with jurisdiction over the crime to authorize a warrant when the search involves a device using anonymizing technology, and they permit the FBI to use one warrant to search compromised computers when the investigation involves devices located in five or more districts.[72] If Congress does not pass a bill rejecting the proposed amendments by December 1st, 2016, they will automatically go into effect.[73] These revisions will certainly make it easier for the government to hack lawfully, even though we know that law enforcement has been hacking for more that 15 years without this authorization.

It is clear that from 1999 to 2016, U.S. law enforcement's hacking capabilities dramatically expanded.[74] It began with something as simple as physical installation of spyware onto a single computer,[75] and has evolved into the ability to infect thousands of computers from one FBI server.[76] But just as the technology used to hack computers has progressed, so has the technology that helps to limit law enforcement access to user data. Encryption and anonymization technology are stronger than ever before, and so law enforcement has become more reliant on the use of vulnerabilities—security flaws in software and hardware—to access information on their targets. The FBI has been reluctant to share the functions of their hacking technology, or the vulnerabilities they exploit, allowing them to repeatedly use tools like CIPAV and the tool used to hack Syed Rizwan Farook's iPhone.[77] This behavior raises the question of whether or not law enforcement leaves citizens' communications, data, and systems insecure by refusing to disclose information that would allow companies to patch their products and protect their users. The history of technology used in government hacking has been a back and forth between investigators and those they investigate, each trying to use the newest software or system in order to achieve their goals.

The United States is at a fork in the road, and we must consider what role law enforcement hacking should play in criminal investigations. With the imminent changes to Rule 41, the power to push back against forensic hacking resides in the courts and in Congress. At the same time, more and more crimes have a technological component and investigators will have to address these challenges. So where do we stand? If Congress allows the changes to Rule 41 to take effect, judges will be responsible for determining when a warrant for hacking is appropriate, as they have done in other cases for centuries. If Congress decides to examine the issue further, they could either deem the practice too dangerous to continue at all, or institute new rules of the road for hacking that reflect the unique situation it presents. In any case, the next five years will be an exciting tour through the intersection of criminal justice and modern technology. This paper provides a historical overview of some of the most publicly known cases of investigative hacking in order to help further this urgent and important discussion.

Notes

1. Kim Zetter, "Everything We Know About How the FBI Hacks People," *Wired*, May 5, 2016, https://www.wired.com/2016/05/history-fbis-hacking.

2. Declan McCullagh, "FBI Hacks Alleged Mobster," *Wired*, December 6, 2000, http://www.wired.com/2000/12/fbi-hacks-alleged-mobster/.

3. "Story so Far: Apple-FBI Battle over San Bernardino Terror Attack Investigation – All the Details," *Los Angeles Times*, February 19, 2016, http://www.latimes.com/business/technology/la-fi-tn-apple-fbi-20160219-htmlstory.html.

4. Zetter, "Everything We Know About How the FBI Hacks People."

5. PGP designates two separate series of jumbled letters, numbers, and characters as the "public key" and "private key" for a user. A combination between the sender's private key and the recipient's public key encrypts the content, and the combination of the sender's public key and the recipient's private key decrypts the content. To encrypt and decrypt one's own files, the user utilizes one's own public and private keys. The actual texts of the two keys are too long and obscure to memorize. Philip Zimmermann, "Preface," PGP Source Code and Internals, (Massachusetts: MIT Press, 1995) available at https://www.philzimmermann.com/EN/essays/index.html.; Affidavit of Randall Murch 3-4 , United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. Dec. 26, 2001), available at http://www.epic.org/crypto/scarfo/murch_aff.pdf. [hereinafter Murch Aff.]; "Surveillance Self-Defense: An Introduction to Public Key Cryptography and PGP," Electronic Frontier Foundation, November 7, 2014, https://ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp.

6. Richard Willing, "Case Tests Legality of FBI's PC Surveillance," *USA Today*, July 31, 2001, http://usatoday30.usatoday.com/tech/news/2001-07-30-pc-snooping.htm.

7. Murch Aff. 10-11.

8. George Anastasia, "Scarfo's High-Tech Case Ends with Plea," *The Inquirer*, March 1, 2002, http://articles.philly.com/2002-03-01/news/25342831_1_guilty-plea-nicodemo-little-nicky-scarfo-mob-boss.

9. John Schwartz, "U.S. Refuses to Disclose PC Tracking," *The New York Times*, August 25, 2001, http://www.nytimes.com/2001/08/25/technology/25CODE.html?pagewanted=all.

10. Anastasia, "Scarfo's High-Tech Case Ends with Plea."

11. Bob Sullivan, "FBI Software Cracks Encryption Wall," *MSNBC.com*, November 20, 2001, http://www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall/#.V2wwfvkrLct.

12. United States of America v. Mark Stephen Forrester, Opinion, 05-50410 (9th Ct. App. 2007) http://caselaw.findlaw.com/us-9th-circuit/1144425.html; Declan McCullagh, "Feds use keylogger to thwart PGP, Hushmail," *CNET*, July 20, 2007, http://www.cnet.com/news/feds-use-keylogger-to-thwart-pgp-hushmail.

13. A Denial-of-Service (DOS) attack is when an intruder prevents legitimate users from accessing a network or website. DOS attacks are typically done by overflooding a system with computer traffic. US-CERT, "Understanding Denial-of-Service Attacks," Department of Homeland Security, February 6th, 2013, https://www.us-cert.gov/ncas/tips/ST04-015; Kevin Poulsen, "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats," *Wired*, July 18, 2007, http://archive.wired.com/politics/law/news/2007/07/fbi_spyware?currentPage=all.

14. Declan McCullagh, "FBI Remotely Installs Spyware to Trace Bomb Threat," *CNET*, July 18, 2007, http://www.cnet.com/news/fbi-remotely-installs-spyware-to-trace-bomb-threat.

15. McCullagh, "FBI Remotely Installs Spyware to Trace Bomb Threat"; An IP address is a series of four numbers (between 0-255) each separated by a period (ex: 200.15.73.189) that identifies a computer when it connects to a network or another computer. IP addresses can easily be spoofed or changed. A MAC address is a permanent identifier comprised of letters and numbers that labels the adapter that connects a computer or device via wifi or ethernet.
Application and Affidavit for Search Warrant, In the Matter of the Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Messages Delivered to That Account by the Government, 3.

16. Electronic communication, in this case, means any signal or information send over the internet with an originating IP address and a destination IP address. Common forms of electronic communication include instant messages and e-mail.
Application and Affidavit for Search Warrant, In the

Matter of the Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Messages Delivered to That Account by the Government, 2-3.

[17] Application and Affidavit for Search Warrant, In the Matter of the Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Messages Delivered to That Account by the Government, 12-14.

[18] Chris Grygiel, "FBI says agent impersonated AP reporter," *Associated Press*, November 7, 2014, **http://www.ap.org/Content/AP-In-The-News/2014/FBI-says-agent-impersonated-AP-reporter**.

[19] Elizabeth Chuck, "FBI Created Fake Seattle News Story to Catch Bomb Threat Suspect," *NBC News*, October 28, 2014, **http://www.nbcnews.com/news/us-news/fbi-created-fake-seattle-news-story-catch-bomb-threat-suspect-n235346.**

[20] Application and Affidavit for Search Warrant, In the Matter of the Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Messages Delivered to That Account by the Government, 13-14.

[21] Poulsen, "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats."

[22] Kevin Poulsen, "Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years," *Wired*, April 16, 2009, **https://www.wired.com/2009/04/fbi-spyware-pro**; Kevin Poulsen, "Get your FBI Spyware Documents Here," *Wired*, April 17, 2019, **https://www.wired.com/2009/04/get-your-fbi-sp**.

[23] In re Warrant to Search a Target Computer at Premises Unknown, 958 F.Supp.2d 753, 1 (S.D.Tex.2013), available at **https://s3.amazonaws.com/files.cloudprivacy.net/Order%20denying%20warrant.MJ%20Smith.042213.pdf**.

[24] In re: Warrant to Search a Target Computer at Premises Unknown, 3.

[25] Cyrus Farivar, "FBI Denied Permission to Spy on Hacker through His Webcam," *ArsTechnica*, April 24, 2013, **http://arstechnica.com/tech-policy/2013/04/fbi-denied-permission-to-spy-on-hacker-through-his-webcam**.

[26] Searches and seizures fall under Rule 41 of the Federal Rules of Criminal Procedure. Rule 41 outlines five situations based on territory that a judge of a district has the authority to issue a search warrant. Judge Smith stated that this case did not meet any of the requirements. The Fourth Amendment restricts law enforcement from overstepping their search capabilities. Judge Smith argued that accidentally hacking innocent computers would constitute as a violation of those computer users' rights. Marshall Honorof, "Why the FBI Can't Hack a Bank Hacker," *NBC News*, April 25, 2013, **http://www.nbcnews.com/id/51663535/ns/technology_and_science-tech_and_gadgets/t/why-fbi-cant-hack-bank-hacker/#.V1bgnvmDFHw**.

[27] In re: Warrant to Search a Target Computer at Premises Unknown, 11.

[28] Joseph Cox, "The FBI's 'Unprecedented' Hacking Campaign Targeted over a Thousand Computers," *Motherboard*, January 5, 2016, **http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers**.

[29] Robyn Greene, "Congress Must Pass the Stopping Mass Hacking Act," New America's Open Technology Institute, June 1, 2016, **http://www.newamerica.org/oti/blog/congress-must-pass-stopping-mass-hacking-act/**.

[30] The Tor Project, **https://www.torproject.org/**.

[31] Thorin Klosowski, "What Is Tor and Should I Use It?" *Lifehacker*, February 21, 2014, **https://lifehacker.com/what-is-tor-and-should-i-use-it-1527891029**.

[32] What is the Tor Browser?, The Tor Project, **https://www.torproject.org/projects/torbrowser.html.en**.

[33] "Who Uses Tor," The Tor Project, **https://www.torproject.org/about/torusers.html.en**.

[34] Jake Wallis Simons, "Guns, Drugs and Freedom: The Great Dark Net Debate," *The Telegraph*, September 17, 2014, **http://www.telegraph.co.uk/culture/books/11093317/Guns-drugs-and-freedom-the-great-dark-net-debate.html**.

[35] David Bisson, "Operation Onymous Challenges Tor To Strengthen Its Security," *The State of Security*, November 18, 2014, **http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/operation-onymous-challenges-tor-to-strengthen-its-security/**.

[36] Andy Greenberg, "Global Web Crackdown Arrests 17, Seizes Hundreds Of Dark Net Domains," *Wired*, November 7, 2014, **https://www.wired.com/2014/11/operation-**

onymous-dark-web-arrests/.

37. Kevin Poulsen, "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack," *Wired*, September 13, 2013, https://www.wired.com/2013/09/freedom-hosting-fbi/.

38. Patrick Howell O'Neill, "An In-depth Guide to Freedom Hosting, the Engine of the Dark Net," *The Daily Dot*, August 4, 2013, http://www.dailydot.com/news/eric-marques-tor-freedom-hosting-child-porn-arrest/.

39. O'Neill, "An in-depth guide to Freedom Hosting, the engine of the Dark Net.

40. Joseph Cox, "FBI May Have Hacked Innocent TorMail Users," *Wired*, January 21, 2016, http://motherboard.vice.com/read/fbi-may-have-hacked-innocent-tormail-users.

41. Brad Heath, "FBI Ran Website Sharing Thousands of Child Porn Images," USA Today, January 21, 2016, http://www.usatoday.com/story/news/2016/01/21/fbi-ran-website-sharing-thousands-child-porn-images/79108346; Pierluigi Paganini, "Operation Pacifier, the FBI Massive Hacking Campaign to De-anonymize Tor Users," *Security Affairs*, August 2, 2016, http://securityaffairs.co/wordpress/49925/laws-and-regulations/operation-pacifier-hacking-campaign.html.

42. A server, in this case, is a computer connected to a network that serves other computers and devices. In the Matter of the Search of COMPUTERS THAT ACCESS upf45jv3bziuctml.onion, Case No. 1:15-SW-89, 21 (E.D.Va. 2016).

43. Brad Heath, "FBI Ran Website Sharing Thousands of Child Porn Images"; Paganini, "Operation Pacifier, the FBI Massive Hacking Campaign to De-anonymize Tor Users."

44. In the Matter of the Search of COMPUTERS THAT ACCESS upf45jv3bziuctml.onion, 1.

45. Kevin Poulsen, "Visit the Wrong Website, and the FBI Could End Up in Your Computer," *Wired*, August 5, 2014, https://www.wired.com/2014/08/operation_torpedo.

46. United States of America v. Jay Michaud, 69-70 (W.D. Wash. 2016), available at https://www.scribd.com/doc/297326719/Michaud-Playpen-Hearing-Transcript.

47. Like CIPAV, the NIT took advantage of the process that when a computer visits a website and the computer downloads instructions from the site to inform the computer how display a webpage. For Playpen, the FBI coded the NIT into the website's "instructions". Specifically, the NIT gathered the computer's actual IP address, operating system type, operating system username, hostname, and MAC address. A hostname is the name that shows up for a device when it connects to a network. In the Matter of the Search of COMPUTERS THAT ACCESS upf45jv3bziuctml.onion, 24-25.

48. Brad Heath, "FBI Ran Website Sharing Thousands of Child Porn Images."

49. Joseph Cox, "FBI's Mass Hack Hit 50 Computers in Austria," *Motherboard*, July 28, 2016, https://motherboard.vice.com/read/fbis-mass-hack-playpen-operation-pacifier-hit-50-computers-in-austria.

50. United States of America v. Jay Michaud, 13.

51. United States of America v. Jay Michaud, 13.

52. Mario Trujillo, "Judge Won't Force Government to Disclose Vulnerability to Mozilla," *The Hill*, May 17, 2016, http://thehill.com/policy/technology/280139-judge-wont-force-government-to-disclose-vulnerability-to-mozilla.

53. Bill Camarda, "Judge Tosses Evidence in FBI Tor Hacking Child Abuse Case," *Naked Security by Sophos*, May 27, 2016, https://nakedsecurity.sophos.com/2016/05/27/judge-tosses-evidence-in-fbi-tor-hacking-child-abuse-case.

54. United States of America v. Edward Joseph Matish, III, Opinion and Order, 9-40 (E.D. Va. 2016) https://www.eff.org/files/2016/06/23/matish_suppression_edva.pdf.

55. "Everything We Know about the San Bernardino Terror Attack Investigation So Far," *Los Angeles Times*, December 14, 2015, http://www.latimes.com/local/california/la-me-san-bernardino-shooting-terror-investigation-htmlstory.html.

56. Pierre Thomas and Jack Date, "San Bernardino Shooters Tried to Destroy Phones, Hard Drives, Sources Say," *ABC News*, December 3, 2015, http://abcnews.go.com/US/san-bernardino-shooters-destroy-phones-hard-drives-sources/story?id=35570286; "Source: Nothing Significant Found on San Bernardino iPhone So Far," *CBS News*, April 13, 2016, http://www.cbsnews.com/news/source-nothing-significant-found-on-san-bernardino-iphone.

57. Christina Warren, "Apple: San Bernardino County Screwed Up the iPhone the FBI Wants Us to Fix," *Mashable*, February 19, 2016, http://mashable.com/2016/02/19/apple-fbi-san-bernadino-

iphone/#YfjsaJYoKPqG.

58. Evan Perez and Tim Hume, "Apple Opposes Judge's Order to Hack San Bernardino Shooter's iPhone," *CNN*, February 18, 2016, http://www.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple.

59. Ellen Nakashima and Mark Berman, "FBI Asked San Bernardino to Reset the Password for Shooter's Phone Backup," *Washington Post*, February 20, 2016, https://www.washingtonpost.com/world/national-security/fbi-asked-san-bernardino-to-reset-the-password-for-shooters-phone-backup/2016/02/20/21fe9684-d800-11e5-be55-2cc3c1e4b76b_story.html.

60. In the Matter of the Search of an Apple iPhone Seized during the Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M (C.D. Calif. 2016), 1-3 http://www.ndaa.org/pdf/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf.
61. Tim Cook, "A Message to Our Customers," Apple, February 16, 2016, https://www.apple.com/customer-letter/.

62. Tim Cook, "A Message to Our Customers."

63. Brian Barrett, "Tech Giants Agree: The FBI's Case Against Apple Is a Joke," *Wired*, March 3, 2016, https://www.wired.com/2016/03/apple-fbi-tech-industry-support-amicus-brief/; "Amicus Briefs in Support of Apple," Apple, https://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html.

64. Amy Davidson, "The Dangerous All Writs Act Precedent in the Apple Encryption Case," *The New Yorker*, February 19, 2016, http://www.newyorker.com/news/amy-davidson/a-dangerous-all-writ-precedent-in-the-apple-case; Brian Barrett, "The Apple-FBI Fight Isn't About Privacy vs. Security. Don't Be Misled," *Wired*, February 24, 2016, https://www.wired.com/2016/02/apple-fbi-privacy-security/; Mark Berman and Ellen Nakishima, "FBI Director: Victory in the Fight with Apple Could Set a Precedent, Lead to More Requests," *Washington Post*, March 1, 2016, https://www.washingtonpost.com/news/post-nation/wp/2016/03/01/fbi-apple-bringing-fight-over-encryption-to-capitol-hill/?utm_term=.21a226f6df19.

65. Elizabeth Weise, "Apple v. FBI Timeline: 43 Days That Rocked Tech," *USA Today*, March 30, 2016, http://www.usatoday.com/story/tech/news/2016/03/15/apple-v-fbi-timeline/81827400.

66. There has been heavy speculation as to who was the party that provided the iPhone hack. The director of the FBI stated that the tool used to hack the phone only works on an iPhone 5C running iOS 9. Although rumors surfaced that a company known as Cellebrite provided the hack, unnamed FBI sources reportedly denied that the hack was done by the Israeli company. A Washington Post article cited anonymous sources saying that professional hackers were paid a one-time flat fee to discover vulnerabilities in the phone's software. Mark Hosenball, "FBI Paid under $1 Million to Unlock San Bernardino iPhone: Sources," *Reuters*, May 4, 2016, http://www.reuters.com/article/us-apple-encryption-idUSKCN0XQ032; Director Comey Remarks During May 11 'Pen and Pad' Briefing with Reporters, May 14, 2016, https://www.fbi.gov/news/pressrel/press-releases/director-comey-remarks-during-may-11-pen-and-pad-with-reporters; Weise, "Apple v FBI Timeline: 43 Days That Rocked Tech"; Ellen Nakashima, "FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone," *Washington Post*, April 12, 2016, https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html.

67. Ellen Nakishima, "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.

68. Danny Yadron, "FBI Confirms It Won't Tell Apple How It Hacked San Bernardino Shooter's iPhone," *The Guardian*, April 28, 2016, https://www.theguardian.com/technology/2016/apr/27/fbi-apple-iphone-secret-hack-san-bernardino.

69. Ellen Nakishima, "Comey defends FBI's purchase of iPhone hacking tool."

70. Ellen Nakishima and Adam Goldman, " FBI Weighs If It Can Share Hacking Tool With Local Law Enforcement," *Washington Post*, April 1, 2016, https://www.washingtonpost.com/world/national-security/fbi-weighs-if-it-can-share-hacking-tool-with-local-law-enforcement/2016/04/01/f4ff94ce-f831-11e5-a3ce-f06b5ba21f33_story.html; Salvador Hernandez, "FBI Tells Local Law Enforcement It Will Help Unlock Phones," *BuzzFeed*, April 2, 2016, https://www.buzzfeed.com/salvadorhernandez/fbi-tells-local-law-enforcement-it-will-help-unlock-phones?utm_term=.0xeB4xKKr#.snjjOWAAx.

71. Kim Zetter, "So Now the Government Wants to Hack Cybercrime Victims," *Wired*, May 4, 2016, https://www.wired.com/2016/05/now-government-wants-hack-

cybercrime-victims.

72. Proposed Amendments to the Federal Rules of Criminal Procedure, Rule 41(b)(6), April 28, 2016, https://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf.

73. Brett Soloman, "This Arcane Rule Change Would Give U.S. Law Enforcement New Power to Hack People Worldwide," *Slate*, May 11, 2016, http://www.slate.com/blogs/future_tense/2016/05/11/the_rule_41_change_would_give_u_s_law_enforcement_power_to_hack_people_worldwide.html.

74. Kim Zetter, "Everything We Know About How the FBI Hacks People."

75. Declan McCullagh, "FBI Hacks Alleged Mobster."

76. Joseph Cox, "Judge Rules FBI Must Reveal Malware It Used to Hack Over 1,000 Computers," *Motherboard*, February 18, 2016, https://motherboard.vice.com/read/judge-rules-fbi-must-reveal-malware-used-to-hack-over-1000-computers-playpen-jay-michaud.

77. Devlin Barrett, "FBI Plans to Keep Apple iPhone-Hacking Method Secret," *Wall Street Journal*, April 26, 2016, http://www.wsj.com/articles/fbi-plans-to-keep-apple-iphone-hacking-method-secret-sources-say-1461694735?mod=trending_now_3; Andy Greenberg, "Global Web Crackdown Arrests 17, Seizes Hundreds Of Dark Net Domains," *Wired*, November 7, 2014, https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/.