Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | December 2016

Introduction

This month we focus on cybersecurity and law enforcement powers to investigate computer crimes. Megan Brown looks at two recent cybersecurity reports, from the Commission on Enhancing National Cybersecurity and the U.S. Department of Homeland Security's report, *Strategic Principles for Securing the Internet of Things (IoT)*. Both focus on IoT, among other topics. We expect both to be a focus of at least some meaningful attention in a new Administration that has expressed material concerns about the country's overall cybersecurity posture. Matt Gardner examines the recent changes to the Federal Rules of Criminal Procedure that grant law enforcement enhanced powers to investigate computer crimes.

We'll be following the full range of developments in the areas of privacy and cybersecurity in the new Administration and in general in the year ahead. As always, please let me know if you have questions or comments on any of these topics, or if we can be of assistance in connection with any of these developments. Please let me know if you have thoughts on topics you would like us to address in future issues of *Privacy in Focus*. I can be reached at 202.719.7335 or knahra@wileyrein.com. Thank you for reading. ■

— Kirk Nahra, Privacy and Cybersecurity Practice Chair

The Federal Government's Power to Use Computer Hacking to Investigate Criminal Activity

On December 1, 2016, amendments to Federal Rule of Criminal Procedure 41 (Rule 41) went into effect, granting law enforcement enhanced powers to investigate computer crimes. The scope and wisdom of these amendments have been hotly debated. Privacy advocates have claimed that the Federal Bureau of Investigation (FBI) can now engage in mass hacking of targets. The U.S. Department of Justice (DOJ) responded that the change is limited to mere considerations of venue. This article seeks to separate fact from rhetoric and describe the actual scope of the amendments.

Background on Rule 41 and the Fourth Amendment

The Fourth Amendment to the United States Constitution provides limits on the federal government's power to search property as part of a criminal investigation. In general, the Fourth Amendment provides two important limitations. First, searches must be done pursuant to warrants that are supported by probable cause. *See, e.g.*, *Illinois v. Gates*, 462 U.S. 213 231 (1983); *United States v. McLamb*, 2016 WL 6963046 (E.D.Va. 2016). Second, search warrants must describe with particularity the place to be searched, i.e., a specific address of a house that is believed to contain evidence of a crime. *See, e.g.*, *United States v. Henderson*, 2016 WL 4549108 (N.D.Ca. 2016) ("Particularity means the warrant must make clear exactly what it is that he or she is authorized to search for and seize.").

Rule 41 sets out the procedures for how law enforcement can obtain a warrant, including authorizing federal magistrate judges to issue warrants. Under the previous version of Rule 41, magistrate judges, with exceptions, could only issue warrants for property that was located within their district. So, as a general matter, a magistrate judge in one state could not sign a search warrant allowing agents to search a house in another state.

Background on the Dark Web

These basic Fourth Amendment safeguards for obtaining search warrants are

continued on page 2

ALSO IN THIS ISSUE

continued from page 1

routinely applied in investigations of computer crimes. However, the decentralized and anonymous nature of the dark web presents more difficult questions. To understand why, some background on the dark web is necessary.

The dark web can only be accessed by special software, most notably The Onion Router, which is commonly referred to as Tor. All Internet traffic on Tor is anonymous. Tor sends each communication through numerous "nodes" or routers, thereby stripping the original or true IP address of the person connecting to the dark web. Similarly, web servers on Tor send all of their traffic through numerous routers, allowing for the location and true IP address of the server to be masked.

While the social utility of Tor is constantly debated, there is no question that criminals love it. The benefit of anonymous activity facilitates myriad criminal activities, such as drug trafficking, terrorism, murder-for-hire, and child exploitation.

The Playpen Investigation

A recent FBI investigation into a child exploitation website known as Playpen illustrates how Tor pushed the limits of the previous incarnation of Rule 41. Playpen was devoted to child pornography, and it was hosted on Tor, meaning savvy pedophiles could access it anonymously. In 2015, the FBI had a break: They were able to seize the servers that hosted Playpen. But, even with the servers, they could not tell who was accessing the site—Tor prevented them from seeing the true IP address of the targets.

The FBI developed a work-around: a small bit of code that was downloaded to the home computer of anyone who accessed the Playpen website and entered a username and password. Once downloaded to the target's computer, the code secretly sent the target's true IP address to servers that were maintained by the FBI. The FBI referred to the code as a Network Investigative Technique (NIT). Privacy advocates are more blunt. They call it malware and computer hacking.

Terminology aside, the code was a search. It went onto an individual's computer and searched that computer for its true IP address. As such, the FBI obtained a warrant to conduct the search. The Playpen servers were located in the Eastern District of Virginia, and the FBI obtained a warrant from a magistrate judge there to deploy the NIT and search for the true IP addresses of the users of the Playpen website.

The concern, however, is that the users of Playpen could have been anywhere in the world. Their IP addresses, and therefore physical location, were unknown. Under Rule 41, what was the authority of the magistrate judge in Virginia to issue a warrant to allow for a NIT to search computers that would almost certainly be located outside of Virginia? Moreover, if the magistrate judge in Virginia could not properly issue the warrant, who could? Because Tor is anonymous, law enforcement could not at the outset identify the location of any individual target and, therefore, could not determine in which district to seek a warrant.

Playpen Decisions

Using the NIT, the FBI collected the true IP addresses of over a hundred users of the Playpen website. Using those IP addresses, law enforcement across the country obtained a second set of warrants. Now able to identify the location of the computers using Playpen to view child pornography, the FBI obtained warrants for those individuals' houses. In the subsequent criminal cases, several defendants have challenged the original warrant authorizing the NIT as a violation of Rule 41. The courts' decisions have predominately—but not uniformly—upheld the validity of the search under Rule 41. *See, e.g.*, *United States v. Henderson,* 2016 WL 4549108 (N.D.Ca. 2016), (warrant was valid under Rule 41); *United States v. Allain*, 2016 WL 5660452, (D. Mass. 2016), (same); *but see United States v. Levin*, 2016 WL 2596010 (D.Mass. 2016) (warrant violated Rule 41's jurisdictional requirement and was void *ab initio*). The split among the reviewing courts shows that this type of investigative technique is a close call under the previous version of Rule 41.

Amendments to Rule 41

The DOJ, most notably in a series of blog posts by Assistant Attorney General Leslie R. Caldwell, advocated for amending Rule 41 to make it clear that a magistrate judge can issue a warrant under these circumstances. *See* November 21, 2016 Blog Post by AAG Caldwell, *Ensuring Tech-Savvy Criminals Do Not Have Immunity From Investigation*. On December 1, those amendments went into effect. Specifically, Rule 41(b)(6) now states, "a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or

continued on page 5

President's Cyber Commission Calls for Fast IoT Action, Consumer Focus

Reports to outgoing Presidents rarely have long-term policy impact. But as the new President's cyber priorities take shape, the December 2 Report of the Commission on Enhancing National Cybersecurity (Commission) may set expectations. The Internet of Things (IoT) features prominently in the 100-page Report, and this discussion highlights the Commission's perspective on IoT.

The Commission observes that "IoT devices can be significant weak links in our global networks, easily weaponized to deliver destructive and destabilizing attacks." It states that "[t]he United States must lead a global push to drive security and secure development concepts into IoT design and development. The hour for doing so is already late." What would that look like?

Standards, Studies, and Incentives

The Commission suggests agencies and others create "a set of general security principles … and IoT recommendations tailored to specific sectors, applications, and risks." It calls for an army of federal regulators to launch IoT efforts. Agencies that "currently regulate IoT devices" should model "the National Highway Traffic Safety Administration" and work "immediately with industry to develop voluntary and collaborative guidelines to secure IoT devices."

The Report calls for numerous guidelines, roadmaps, standards, assessments, and studies, ranging from "a comprehensive set of risk-based security standards," to a study on "how best to improve network security through incentives," roadmaps for action, and a "standard template" for consumer information.

IoT liability concerns are addressed. Helpfully, the Commission heard concerns and suggests that "[t] he Department of Justice should lead an interagency study with the Departments of Commerce and Homeland Security and work with the Federal Trade Commission, the Consumer Product Safety Commission, and interested private sector parties to assess the current state of the law with regard to liability for harm caused by faulty IoT devices and provide recommendations within 180 days."

Consumers Focus

Consumers are a big focus, with calls for labels and more than one "Bill of Rights." The Commission recognizes that consumers and end users are key, and makes several recommendations designed to promote user awareness and cyber hygiene for IoT.

The Commission promotes consumer labeling, writing that "an independent organization should develop the equivalent of a cybersecurity 'nutritional label' for technology products and services—ideally linked to a rating system of understandable, impartial, third-party assessment that consumers will intuitively trust and understand." The Commission acknowledges the complexity of this, and avoids whether such a standard label or rating should be mandatory.

The Federal Trade Commission (FTC) features prominently, with several expected actions, like developing "a standard template for documents that inform consumers of their cybersecurity roles and responsibilities as citizens in the digital economy—along with a 'Consumer's Bill of Rights and Responsibilities for the Digital Age.'" In another action item, the Commission calls for "consumer organizations [to] work with industry and the FTC to develop a consumer 'cybersecurity bill of rights and responsibilities.'"

Future Implications

While the new Administration and Congress can ignore this Report, some of its many observations are likely to appear in agency inquiries, state efforts, and legal papers. It may inspire IoT efforts at agencies, or in the States, and it may be used by consumer groups to advocate for more regulation or promote disclosures. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

IoT Security: "I'm From the Government and I'm Here to Help"?

Ronald Reagan joked that the most terrifying words in the English language are: "**I'm From the Government and I'm Here to Help**." When it comes to security and the Internet of Things (IoT), government wants to be helpful, for better or for worse. The National Institute of Standards and Technology (NIST), the National Telecommunications and Information Administration (NTIA), the U.S. Department of Homeland Security (DHS), the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), the National Highway Traffic Safety Administration (NHTSA), and the U.S. Food and Drug Administration (FDA) are all looking at IoT. Congressional IoT interest abounds. As President-elect Trump and a new Congress take over, the fate of ongoing activities is unclear, but widespread interest and divergent approaches at DHS (and other agencies) and on the Hill promise future scrutiny.

On one hand, DHS released a report, *Strategic Principles for Securing the Internet of Things (IoT)*, finding it "imperative that government and industry work together, quickly, to ensure the IoT ecosystem is built on a foundation that is trustworthy and secure." DHS states that the "role of government" is to "provide tools and resources so companies, consumers, and other stakeholders can make informed decisions about IoT security." DHS offers principles to "motivate and frame conversations about positive measures for IoT security among developers, manufacturers, service providers," and consumers. These (unsurprising) principles are:

- Incorporate Security at the Design Phase
- Promote Security Updates and Vulnerability Management (citing NTIA's Multistakeholder Process on Patching and Updating for IoT)
- Build on Recognized Security Practices (citing the NIST Cybersecurity Framework)
- Prioritize Security Measures According to Potential Impact
- Promote Transparency across IoT (including, among other things, vendor risk assessments and a publicly disclosed way to use vulnerability reports)
- Connect Carefully and Deliberately (targeted at consumers)

DHS offers next steps, including coordination of activities, building awareness of risks, evaluating incentives, and international standards activity. A notable contribution is DHS interest in how "tort liability, cyber insurance, legislation, regulation," voluntary initiatives, and other efforts can improve security. Given recent litigation over aspects of IoT security, the government might help by protecting innovators and companies from class action lawsuits.

On the other hand, some want regulation. Some Democratic Hill staff lament that there are no federal requirements for security in IoT devices. Some commentators think regulation should force manufacturers to meet minimum security standards: Bruce Schneier from Harvard's Berkman Center recently told a House Subcommittee hearing that "the only solution is to regulate. The government could impose minimum security standards on IoT manufacturers, forcing them to make their devices secure even though their customers don't care. They could impose liabilities on manufacturers." Regulation is premature and even agency "guidance" can prejudge technology and stymie innovation.

At bottom, while regulation is exceedingly unlikely in a new Congress and Administration, these sorts of reports provide fodder for agencies struggling with what, if anything, to do about IoT security. More troubling, States may get in on the action, and class action plaintiffs are looking for the next ubiquitous technology that can provide a basis for litigation. Innovators must watch these efforts and look for ways the government can help, not hurt. ■

For more information on this or other IoT issues, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

continued from page 2

copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means." This provision allows for precisely the type of NITs that were used in the Playpen investigation.

Concerns About Law Enforcement Engaging in Computer Hacking

Privacy advocates, including the American Civil Liberties Union (ACLU) and the Electronic Freedom Foundation (EFF), joined by numerous companies including Google and PayPal, opposed the amendments. The main concern voiced by the opponents is that "Congress and the public need adequate time to have an informed debate about government hacking—and an opportunity to consider what safeguards must be instituted—before the usage of these dangerous investigative tools becomes widespread." *See* June 21, 2016 Letter to Congress signed by dozens of organizations, including ACLU, EFF, Google, and PayPal.

These concerns, however, ignore the fact that the amendments to Rule 41 do not authorize the government to engage in hacking—the government already had that power, so long as the hacking is a search that is deemed reasonable under the Fourth Amendment and is pursuant to a warrant supported by probable cause. To put the powers of law enforcement in some perspective, consider the second set of warrants in the Playpen investigation. Far more intrusive than hacking, those warrants allowed armed federal agents to enter peoples' homes without consent, seize every item of computer media in house, and conduct a detailed forensic analysis of that media.

Further, the amendments to Rule 41 do not in any way abrogate the traditional safeguards for all law enforcement searches: the Fourth Amendment's protections of a warrant supported by probable cause and a particular description of the place to be searched. Again, the Playpen investigation shows how those protections have real meaning even in the context of investigations into computer crimes.

First, the warrant authorizing the NITs was supported by probable cause. *See, e.g.*, *Allain*, 2016 WL 5660452 (Probable cause supported by "the appearance and content of Playpen, the fact that it was a hidden service on the Tor network, and its registration terms."). The only computers that were searched were those of people who voluntarily visited a secret website devoted to child pornography and logged into that website with a username and password. That is certainly a sufficient connection to criminal activity to justify a warrant. Second, the property to be searched was described with particularity. *See Henderson*, 2016 WL 4549108 (The description of Attachment A of the warrant met the particularity requirement because it was "limited only to individuals that log onto the Playpen website using a username and password."); *United States v. Anzalone*, 2016 WL 5339723 (D.Mass. 2016).

Privacy advocates have raised other concerns as well, including the potential that law enforcement may inadvertently cause damage when engaging in hacking pursuant to a warrant. That is certainly a valid consideration. But, again, the risk of collateral damage is inherent in any non-consensual search by law enforcement. Certainly the risk of collateral damage by a NIT is less than that of armed agents entering a person's house without warning.

Further, as with any new Rule, courts will have to determine the scope of Rule 41(b)'s limitation that NITs can only be used outside of a magistrate judge's district if the target's location "has been concealed through technological means." The change will also put additional pressure on magistrate judges to understand the technical searches that they are being asked to evaluate. While these issues will certainly require attention, they are not as grave as the specter of rogue computer hacking by the FBI.

The last several years have seen an emerging tension between industry and law enforcement, epitomized by conflicts like that between Apple and the FBI about encryption and the search of the iPhone of the San Bernardino shooters. Every indication is that this tension will only increase as private industry grapples with wanting to protect itself and its customers' data from governmental intervention. The debate over the amendments to Rule 41 has become a flash point in that debate. But, a closer examination of how the powers of law enforcement were—and were not—expanded by the amendments shows that the rhetoric of this debate may have outpaced the actual increase in governmental power. ■

For more information about this debate, please contact:

Matthew J. Gardner
202.719.4108
mgardner@wileyrein.com

SPEECHES & EVENTS

Acclimating to Changing Regulatory, Legislative & Enforcement Activities and Breach Notification Requirements

ACI's 21st National Advanced Global Legal and Compliance Forum on Cyber Security and Data Privacy & Protection

Kirk J. Nahra, Moderator

JANUARY 30, 2017 | WASHINGTON, DC

What Companies Need to Know About Data Transfers Under the New EU Privacy Regime

Bloomberg Law Privacy Outlook 2017

Kirk J. Nahra, Panelist

FEBRUARY 28, 2017 | WASHINGTON, DC

Hot Topics in Privacy and Security

NAID 2017 Annual Conference

Kirk J. Nahra, Speaker

MARCH 23, 2017 | LAS VEGAS, NV

Navigating the HIPAA Enforcement Landscape

The 26th National HIPAA Summit: The Leading Forum on Healthcare EDI, Privacy, Confidentiality, Data Security, and HIPAA Compliance

Kirk J. Nahra, Speaker

MARCH 29-31, 2017 | WASHINGTON, DC

Privacy Boot Camp

IAPP Global Privacy Summit 2017

Kirk J. Nahra, Speaker

APRIL 18, 2017 | WASHINGTON, DC

Contributing Authors

Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Matthew J. Gardner	202.719.4108	mgardner@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com