MEMORANDUM

To: Members of the Advisory Committee on Criminal Rules
From: American Civil Liberties Union
Date: October 31, 2014
Re: Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media

Dear Members of the Committee,

The American Civil Liberties Union submits these comments to aid the Committee's consideration of the proposed amendment to Rule 41 concerning "remote access" searches of computers and other electronic devices. The amendment was proposed by the Department of Justice last year, and modified by the Committee at its April 2014 meeting.[1]

We appreciate the careful scrutiny that the Committee has given to the proposed amendment so far and, in particular, the changes made during the Committee's April 2014 meeting. By narrowing the proposed circumstances in which warrants for remote access searches may be sought, the Committee addressed many of the problems identified by the ACLU in the original proposal.

Nonetheless, we continue to have serious concerns about the breadth of the proposed amendment, and we urge the Committee to reject the proposal in full.

This comment raises questions about the first prong of the proposal, which would permit law enforcement agencies to remotely install surveillance software on a target's computer if "the district where the media or information is located has been concealed through technological means."[2] Although the second prong of the proposal, which the government has argued is necessary for botnet investigations,[3] also raises serious questions, the ACLU leaves it to others to flesh out those questions.[4]

[1] *See generally* Advisory Comm. on Criminal Rules, Materials for April 7–8, 2014 Meeting 155–266 ("Advisory Committee Materials"), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2014-04.pdf
[2] Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure: Request for Comment 338 (Aug. 2014) ("Proposed Amendments Materials"), *available at* http://www.regulations.gov/#!documentDetail;D=USC-RULES-CR-2014-0004-0001.
[3] *See* Advisory Committee Materials at 172.
[4] Given the technical complexity associated with the botnets, we recommend that the committee solicit input from botnet experts from both academia and industry.

This comment begins by describing the technological means by which law enforcement agencies will likely carry out the "remote access searches" that would be authorized by the proposed amendment, and the computer security and policy concerns raised by such operations. It then explains that the proposal does not merely regulate procedure, but in fact affects substantive rights and substantively expands the government's investigative power. Finally, it argues that the substantive authority sought by the government through its proposal raises serious constitutional questions. On the basis of these serious policy and constitutional questions, the ACLU recommends that the Committee reject the proposal as going beyond the scope of the Rules' limited purpose and defer to Congress to address this issue in the first instance.

We very much appreciate the Committee's consideration of this comment and look forward to discussing our concerns with the Committee during the upcoming public meeting.

I. The Means Available to the Government to Conduct "Remote Access" Searches

The proposed amendment to Rule 41 would allow a magistrate judge to issue a warrant authorizing law enforcement "to use remote access to search electronic storage media and to seize or copy electronically stored information."[5] Neither the proposed amendment nor the proposed committee note define "remote access." Submissions from the Department of Justice to the Subcommittee on Rule 41 provide some description of what is meant by "remote access" and how such searches might be carried out, but crucial details remain missing.[6] In order for the Committee to make an informed assessment of the implications of the proposed amendment, we begin this comment with a detailed explanation of what the government means by "remote access" search, how such surveillance is carried out, and why authorizing use of these techniques raises serious technological and policy concerns.

A. Federal law enforcement agencies have used malware for nearly fifteen years.

Since at least 2001, federal law enforcement agencies have used sophisticated surveillance software as part of criminal and national security investigations.[7] This software, whether delivered through trickery, by hacking into the computers of targets,[8] or through other covert techniques, permits agents to track and locate the computers and mobile devices of targets, as well as access private information stored on them.

---

[5] Proposed Amendments Materials at 338.

[6] *See generally* Advisory Committee Materials at 179–235.

[7] *See FBI Sheds Light on 'Magic Lantern' PC Virus*, Reuters, Dec. 13, 2001, http://usatoday30.usatoday.com/life/cyber/tech/2001/12/13/magic-lantern.htm.

[8] The Department of Justice has stressed that it is merely engaging in remote computer searches, not "hacking." *See* Advisory Committee Materials at 245. However, internal FBI emails use the terms "penetration" and "exploit" when describing the CIPAV software, which, like hacking, are both terms of art from the computer security community. *See* Email from [redacted] (OTD) (FBI) to [redacted] (OTD) (FBI) et al. (June 20, 2007), *available at* https://www.eff.org/document/fbicipav-08pdf, p. 50; Email from [redacted] (OGC) (FBI) to [redacted] (SL) (FBI) (Nov. 20, 2008), *available at* https://www.eff.org/document/fbicipav-08pdf at p. 154. Using the term "hacking" is descriptively accurate.

In 2001, journalists revealed that the FBI had developed a software suite capable of covertly accessing information stored on suspects' computers.[9] In the initial media reports revealing the existence of the FBI's *Magic Lantern* tool, a spokesperson for the FBI described it as a "a workbench project" that had not yet been deployed. One year later, in a then-classified memo, a DOJ prosecutor wrote that the tool, later renamed the Computer and Internet Protocol Address Verifier (CIPAV), had already entered regular use, and was "being used needlessly by some agencies."[10]

Although the existence of this tool was first revealed by the press in 2001, it was not until 2007 that journalists discovered a case in which it had been used.[11] Indeed, although the FBI has employed similar surveillance software for nearly fifteen years, only a handful of cases have come to the public's attention. This is, we believe, due to a concerted policy by the FBI of keeping everything about its use of this technology out of the public eye.[12] For now, the only law enforcement agency known to use malware[13] is the FBI. However, it is likely that other federal, state and local law enforcement agencies have also acquired hacking software.[14]

---

[9] *FBI Sheds Light on 'Magic Lantern' PC Virus*, Reuters, *supra*.

[10] *See* Memorandum from [redacted] to CTCs 1 (Mar. 7, 2002), *available at* https://www.eff.org/document/fbicipav-05pdf.

[11] *See* 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 ("The court filing offers the first public glimpse into the bureau's long-suspected spyware capability, in which the FBI adopts techniques more common to online criminals.").

[12] *See* Email from [redacted], Unit Chief, FBI Cryptologic and Electronic Analysis Unit to [redacted] (SE) (FBI) (July 18, 2007), *available at* https://www.eff.org/document/fbicipav-08pdf at p.10 ("[W]e try to make every effort possible to protect the FBI's sensitive tools and techniques...we want to ensure that the capabilities of the CIPAV are minimized [in future media reports], if discussed at all. This and many tools deployed by the FBI are law enforcement sensitive and, as such, we request that as little information as possible be provided to as few individuals as possible."); *see also* Email from [redacted] (OTD) to [redacted] (OTD) (CON) et al. (Aug. 15, 2004), *available at* https://www.eff.org/files/filenode/cipav/fbi_cipav-07.pdf at p.11 ("We never discuss how we collect the [information about a target computer obtained by the CIPAV software] in the warrants/affidavits or with case agents, AUSAs, squad supervisors, outside agencies, etc.").

[13] "Malware" and "spyware" are terms of art in the computer security community that describe software used to covertly gain access to and extract information from the computers of targets. *See Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F. 3d 1169, 1171 (9th Cir. 2009) (describing "malicious software, known as 'malware,' that can compromise the security and functionality of a computer"); *see also* Morgan Marquis-Boire et al., Police Story: Hacking Team's Government Surveillance Malware, Citizen Lab (July 24, 2014), https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant/ (describing the capabilities of a malware tool sold by a commercial surveillance company to law enforcement and intelligence agency customers around the world); *Worldwide Threat Assessment of the US Intelligence Community: Hearing on Global Security Threats and Intelligence Operations Before the S. Select Comm. on Intelligence*, 113th Cong. 3 (2013) (statement of James Clapper, Director of National Intelligence), *available at* http://intelligence.senate.gov/130312/clapper.pdf ("[A] handful of commercial companies sell computer intrusion kits on the open market. These hardware and software packages can give governments and cybercriminals the capability to steal, manipulate, or delete information on targeted systems. Even more companies develop and sell professional-quality technologies to support cyber operations—often branding these tools as lawful-intercept or defensive security research products.").

[14] *See* Cora Currier & Morgan Marquis-Boire, *Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide*, Intercept (Oct. 30, 2014), https://firstlook.org/theintercept/2014/10/30/hacking-team/ ("Hacking Team's efforts include a visible push into the U.S. . . . The company has made at least some sales to American entities . . . ."); Kade Crockford, *Spy Tech Secretly Embeds Itself in Phones, Monitors and Operates Them from Afar*, PrivacySOS (Aug. 18, 2012), https://www.privacysos.org/node/789 (describing the capabilities of mobile malware sold by a Virginia-based company, Oceans' Edge, which has apparently sold its software to both the FBI and DEA).

B. Capabilities of the FBI's surveillance software

Like much of the commercially available 'lawful interception' malware sold by surveillance companies to governments around the world, it appears that the FBI's malware tools have a number of capabilities that can be customized for the particular operation, depending on what features are needed, and what the magistrate judge has approved.

In one of the more basic modes of operation, for example, the software can collect the IP address of the targeted computer. This is particularly useful when the target is using an anonymizing proxy, which hides his or her IP address.[15] With an IP address, agents can subpoena subscriber information from the Internet Service Provider responsible for that IP address, and then search the home or business where the targeted computer is believed to be located.

In another mode of operation, the software can collect a long list of information about a target computer, including, but not limited to: IP address; MAC address (identifying the WiFi or Ethernet card); a list of running programs; the operating system type, version and serial number; the default internet browser and version; the registered user of the operating system, and registered company name, if any; the current logged-in user name; and the address of the last website visited in the user's web browser.[16]

If a more thorough search of the computer is required, the FBI has software capable of searching a target's computer to obtain "records of Internet activity, including firewall logs, caches, browser history and cookies, 'bookmarked' or 'favorite' Web pages, search terms that the user entered into any Internet search engine, and records of user-typed Web addresses," as well as "saved user names and passwords, documents, browsing history, user profiles, e-mail contents, e-mail contacts, chat messaging logs, photographs, and correspondence."[17]

In addition to the ability to access essentially any data already stored on the target's computer, the FBI also has the ability to remotely access and enable the GPS chip, microphone, or webcam in a target's computer or mobile device.[18] As such, the FBI has the capability to

---

[15] *See* Application for a Search Warrant at 40, *In re Search of Computers that Access the Website "Bulletin Board A"*, No. 8:12-MJ-356 (D. Neb. Nov. 16, 2012), *available at* http://www.documentcloud.org/documents/1261620-torpedo-affidavit.html (listing the types of information to be obtained by the Network Investigative Technique, including the "activating" computer's IP address and information about the operating system software running on the computer).

[16] Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, *supra*.

[17] *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 755-56 (S.D. Tex. 2013).

[18] *See id.* at 3; *see also* Jennifer Valentino-DeVries & Danny Yadron, *FBI Taps Hacker Tactics to Spy on Suspects*, Wall St. J., Aug. 3, 2013, http://online.wsj.com/articles/SB10001424127887323997004578641993388259674 ("[T]he bureau can remotely activate the microphones in phones running Google Inc.'s Android software to record conversations, one former U.S. official said. It can do the same to microphones in laptops without the user knowing, the person said."); *see also* Craig Timberg & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, Wash. Post, Dec. 6, 2013, http://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html ("The FBI has been able to covertly activate a computer's camera — without triggering

generate location information, to capture audio through the microphone, and to capture photographs or videos using the target's webcam. According to an ex-senior FBI official, the FBI even has the capability to disable a webcam's indicator light, so that there will be no way of knowing that the camera is recording.[19]

C. Methods for infecting the computers of targets with malware

There are several ways in which agents can deliver malicious software to the computer or mobile device of a target. We introduce several of the most popular methods here. This is by no means an exhaustive list, as law enforcement and intelligence agencies can be extremely creative in their efforts to surveil targets and covertly bug computers and mobile devices.

i. Social engineering

In a social engineering operation, agents will send an email or other communication to a target, with the goal of convincing the target to take a particular action, such as clicking on a link in the message, or opening an attachment.[20] Such operations almost always involve some degree of deception, as targets are unlikely to perform the desired action if it is clear from the sender information (i.e., the "From" line of an email) that it is from a law enforcement agency. As a result, agents engaging in such operations are likely to impersonate third parties, such as the target's associates,[21] or organizations known to the target. For example, in 2007, FBI agents successfully delivered CIPAV surveillance software by sending a link to a fake Associated Press article, created by agents for that investigation, to the target of the operation.[22] Presumably, as soon as the target clicked on the link to the article, the CIPAV was delivered to his computer. The FBI likely exploited a security vulnerability in his web browser to deliver the CIPAV software.

The success of this operation depends on being able to trick the target into taking the desired action. For sophisticated targets, particularly those with expertise in computer security, this may be difficult.

---

the light that lets users know it is recording — for several years, and has used that technique mainly in terrorism cases or the most serious criminal investigations, said Marcus Thomas, former assistant director of the FBI's Operational Technology Division in Quantico.").

[19] *See* Timberg & Nakashima, *FBI's Search for 'Mo,' Suspect*, *supra*.

[20] *See* Jennifer Valentino-DeVries & Danny Yadron, *supra* ("Officers often install surveillance tools on computers remotely, using a document or link that loads software when the person clicks or views it.").

[21] *See* T. N. Jagatic et al., *Social Phishing*, Comm. of the ACM, Oct. 2007, at 94, *available at* http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf (demonstrating that phishing attacks which impersonate a friend of the target are more successful than those in which the sender is not known to the target).

[22] *See* Ellen Nakashima & Paul Farhi, *FBI Lured Suspect with Fake Web Page, but May Have Leveraged Media Credibility*, Wash. Post, Oct. 28, 2014, http://www.washingtonpost.com/world/national-security/fbi-lured-suspect-with-fake-web-page-but-may-have-leveraged-media-credibility/2014/10/28/e6a9ac94-5ed0-11e4-91f7-5d89b5e8c251_story.html.

ii. Surreptitious entry

The FBI has a long, controversial history of secretly breaking into the homes or offices of targets and installing covert recording devices.[23] Surreptitious entry operations, commonly known as *black bag jobs*, are also used to install surveillance software and hardware on the computers of targets.[24] The earliest publicly known example of a black bag job was in 1999.[25] These operations of course require that agents know the physical location of the target.

iii. Watering hole attacks

Agents wishing to install surveillance software onto the computers of many individuals who all share a common interest or association may decide to perform a so called *watering hole attack*. In such operations, agents will install custom code on a website popular with the target group, which will infect the computers of everyone who visits the site. This technique has been repeatedly used by the FBI,[26] as well as by foreign state actors.[27] When this technique is used, agents may not know the identity of a particular target or targets, and may in fact not know ahead of time the identities of *any* of the targets whose computers will be eventually be compromised.

iv. Third-party service provider-aided delivery of surveillance software

By enlisting the assistance of third-party service providers, such as telecommunications and internet service providers, agents can leverage the trusted access that such providers have to a target's communications and, in some cases, their computers or mobile devices.

In a *man in the middle* attack, surveillance software can be delivered, typically with special-purpose surveillance hardware installed in an internet provider's data center (and thus, with the assistance of that company), by intercepting requests from a target's computer to access internet content, impersonating the server the target is attempting to connect to, and then sending

---

[23] *See, e.g.*, FBI Records: The Vault, Surreptitious Entries (Black Bag Jobs), http://vault.fbi.gov/Surreptitious%20Entries%20(Black%20Bag%20Jobs)%20; Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Final Report: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans 355 (1976), *available at* https://web.archive.org/web/20070414214706/http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIIf.htm.

[24] *See* Valentino-DeVries & Yadron, *supra* ("In some cases, the government has secretly gained physical access to suspects' machines and installed malicious software using a thumb drive, a former U.S. official said.").

[25] *See United States v. Scarfo*, 180 F. Supp. 2d 572, 577 (D.N.J. 2001) ("Because the encrypted file could not be accessed via traditional investigative means, [the judge's] Order permitted law enforcement officers to 'install and leave behind software, firmware, and/or hardware equipment which will monitor the inputted data entered on [defendant's] computer in the TARGET LOCATION so that the F.B.I. can capture the password necessary to decrypt computer files by recording the key related information as they are entered.'").

[26] *See* Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, Wired (Aug. 5, 2014), http://www.wired.com/2014/08/operation_torpedo/; *see also* Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired (Sept. 13, 2013), http://www.wired.com/2013/09/freedom-hosting-fbi/.

[27] *See* Michael Mimoso, *Council on Foreign Relations Website Hit by Watering Hole Attack, IE Zero-Day Exploit*, Threatpost (Dec. 29, 2012), http://threatpost.com/council-foreign-relations-website-hit-watering-hole-attack-ie-zero-day-exploit-122912/77352.

malicious software back to the target instead.[28] This technique exploits the fact that much of the content accessed on the web is unencrypted, and thus vulnerable to tampering by third parties. There are several companies that sell products designed to deliver surveillance software in this manner,[29] at least one of which has sold its products to the FBI.[30]

Another example of third-party-company–aided delivery involves forcing a service provider to push surveillance software disguised as a security update to customers. This technique has been used by at least one foreign government, using software made by a California-based surveillance company.[31]

D. The surveillance software infection process

The process of delivering surveillance software to a target's computer or mobile device generally consists of a number of different steps. In order to understand the important public policy and legal issues associated with the use of this surveillance technique, it is necessary to first understand the way in which this software is delivered to targets.

Step 1: Reconnaissance

In this step, agents determine a *selector* that can identify each target. For individual targets, this might be an email address, username, telephone number or IP address. For watering hole attacks, the agents will identify the website or server that will be used. If agents plan to infect the target device in-person, through a black bag job, then they must locate the home, office or hotel room where the target's computer or mobile device will be.

Step 2: Attack setup

In this step, agents create the phishing email, prepare the code that will be added to the webpage that the user will visit, or customize the surveillance software that will subsequently be delivered and run on the target's device.

Step 3: Delivery / Acquisition

---

[28] *See* Barton Gellman, *U.S. Firm Helped the Spyware Industry Build a Potent Digital Weapon for Sale Overseas*, Wash. Post, Aug. 15, 2014, http://www.washingtonpost.com/world/national-security/spyware-tools-allow-buyers-to-slip-malicious-code-into-youtube-videos-microsoft-pages/2014/08/15/31c5696c-249c-11e4-8593-da634b334390_story.html ("Merely by playing a YouTube video or visiting a Microsoft Live service page, for instance, an unknown number of computers around the world have been implanted with Trojan horses by government security services that siphon their communications and files. . . . Network injection allows products built by Gamma and Hacking Team to insert themselves into an Internet data flow and change it undetectably in transit.").

[29] *See* Ryan Singel, *Law Enforcement Appliance Subverts SSL*, Wired (Mar. 24, 2010), http://www.wired.com/2010/03/packet-forensics/.

[30] *See* Fed. Bus. Opportunities, Request for Quotations: Network Equipment (FBI Sept. 24, 2014), https://www.fbo.gov/index?s=opportunity&mode=form&id=bbec3296f333fa5c8f23973be4882ec7&tab=core&_cview=0.

[31] *See* John Timmer, *UAE Cellular Carrier Rolls Out Spyware as a 3G "Update"*, Ars Technica (July 23, 2009), http://arstechnica.com/business/2009/07/mobile-carrier-rolls-out-spyware-as-a-3g-update/.

In this step, agents deliver the government's surveillance software to the target's computer. If agents use social engineering, agents will send the previously prepared phishing message to an address known to be used by the target. In a watering hole attack, agents will insert the previously prepared code into the webpage on the site that targets will visit. If agents are engaged in a black bag job, in this step, agents will gain covert access to the house, office or hotel of the target, and locate the computer or mobile device.

Step 4: Exploitation

In this step, the exploit shellcode, a special piece of malicious software, is executed on the target's computer, bypassing or circumventing any security software or other built-in protections present in the targeted software application.[32] If agents use a social engineering attack, the shellcode might be executed because the target clicks on a link in the phishing email. If a watering hole attack is used, the exploitation will take place merely when the target visits the web page that has been modified by the agents. If the agents have conducted a black bag job, the agents will install the software themselves, likely using removable media such as a USB thumb drive.

In many cases, particularly in so-called *drive by download attacks*,[33] where the target's computer is infected merely by clicking on a link or visiting a particular website, the exploitation step will typically involve the exploitation of one or more security vulnerabilities in the web browser, word processor or operating system of the target's device, *infra* Part I.C. The use of exploits enables the surveillance software to be covertly installed on the target's computer.

Step 4a: Validation (optional)

In some operations, particularly when agents may not be confident that the device they have exploited is the correct target, an optional validation step may take place, in which specific information is extracted from the infected computer in order to identify the device and its owner. Examples of such information might include, for example, the computer's IP address, the MAC address identifying the WiFi interface, and other permanent device identification numbers.

Step 5: Installation

In this step, the full surveillance software suite, or *payload*, will be downloaded and installed on the computer of the target.

Step 6: Exfiltration

---

[32] Amit Klein, *Multi-Stage Exploit Attacks for More Effective Malware Delivery*, Trusteer Blog (May 2, 2013), http://www.trusteer.com/blog/multi-stage-exploit-attacks-for-more-effective-malware-delivery ("Most drive-by exploit kits use a minimal exploit shellcode that downloads and runs the final payload. This is akin to a two-stage ICBM (InterContinental Ballistic Missile) where the first stage, the exploit, puts the rocket in its trajectory and the second stage, the payload, inflicts the damage. In the cybercrime world, the de-coupling of the first stage from the payload is designed to make sure that an exploit kit is as generic as possible and can deliver all possible payloads.").

[33] Marco Cova et al., Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code, Proceedings of the 19th International Conference on World Wide Web (2010), *available at* http://www.site.uottawa.ca/~nelkadri/CSI5389/Papers/40-Cova_et_al_WWW2010.pdf.

In this step, the surveillance software collects the desired information on the target and then transmits that information back to a server controlled by the government. This may involve searching documents or other files on the computer, as well as activating the webcam or microphone in the device. In some operations, the surveillance software may collect the information sought, transmit it back to the government, and then erase itself from the target's computer. In other cases, where long-term surveillance is desired, the software may remain on the target's computer, collecting data, and regularly transmitting that data back to the government.

II. Technological and Policy Concerns

There are a number of serious technical and policy concerns related to the covert installation and use of surveillance software by law enforcement agencies.

A. Security flaws in surveillance software can weaken the security of the target's device and expose it to compromise by other unauthorized parties

In 2011, security researchers in Germany obtained a copy of surveillance software that the German authorities had, for two years, used to remotely monitor targets in criminal investigations. The researchers analyzed the software, and discovered that the developers of the software had made elementary programming mistakes,[34] the most serious of which exposed devices running the surveillance software to remote control by other, unauthorized parties.[35] This is not the only example of security vulnerabilities being discovered in surveillance software. Indeed, significant security flaws have repeatedly been discovered in several widely used interception and surveillance software products.[36]

That security vulnerabilities exist in surveillance software is not surprising. All software programs have bugs, some of which may eventually be exploited by hackers. But as one leading scholar has noted, security flaws in surveillance systems can be particularly problematic, as their exploitation can lead to a catastrophic loss of communications confidentiality.[37] The risk of these

[34] See Admin, *Chaos Computer Club Analyzes Government Malware*, Chaos Computer Club (Oct. 8, 2011), http://ccc.de/en/updates/2011/staatstrojaner ("The analysis also revealed serious security holes that the trojan is tearing into infected systems. The screenshots and audio files it sends out are encrypted in an incompetent way, the commands from the control software to the trojan are even completely unencrypted. Neither the commands to the trojan nor its replies are authenticated or have their integrity protected. Not only can unauthorized third parties assume control of the infected system, but even attackers of mediocre skill level can connect to the authorities, claim to be a specific instance of the trojan, and upload fake data. It is even conceivable that the law enforcement agencies' IT infrastructure could be attacked through this channel. The CCC has not yet performed a penetration test on the server side of the trojan infrastructure.").

[35] *Id.*

[36] *See* Dan Goodin, *Root Backdoor Found in Surveillance Gear Used by Law Enforcement*, Ars Technica (May 28, 2014), http://arstechnica.com/security/2014/05/root-backdoor-found-in-surveillance-gear-used-by-law-enforcement/; Micah Sherr et al., *Can They Hear Me Now?: A Security Analysis of Law Enforcement Wiretaps*, CCS '09: Proceedings of the 16th ACM Conf. on Computer & Comms. Security (2009), at 512-523, *available at* http://www.crypto.com/papers/calea-ccs2009.pdf.

[37] Stephanie K. Pell, *Jonesing for a Privacy Mandate, Getting a Technology Fix -- Doctrine to Follow*, 14 N.C. J. L. & Tech. 489 (2013).

flaws being exploited is not theoretical. Sophisticated state actors have hacked into communications surveillance systems and databases on multiple known occasions,[38] in some cases using security flaws in the surveillance software itself.[39]

B. The US government, and the FBI in particular, do not have a strong track record of technical excellence.

If the US government had a strong track record of creating and deploying secure software, perhaps the risks associated with security flaws in government surveillance software could be ignored. Unfortunately, the government's track record is less than solid. The government's information technology (IT) procurement process is widely acknowledged to be broken, leading to the government paying far too much money for poorly written, often flawed software.[40] Examples of botched IT procurement can be found in practically every agency. High-profile instances include Healthcare.gov[41] and the FBI's Sentinel case management system.[42]

Federal government agencies have a particularly poor track record when it comes to data security. Agencies struggle with the most basic security practices, such as using good passwords, updating anti-virus software, and encrypting internet traffic on their websites.[43] The results are predictable: data breaches by federal agencies are now routine—there were a staggering 25,000

---

[38] *See, e.g.*, Vassilis Prevelakis & Diomidis Spinellis, *The Athens Affair*, IEEE Spectrum (June 29, 2007), http://spectrum.ieee.org/telecom/security/the-athens-affair (describing how "hackers broke into a [Greek] telephone network and subverted its built-in wiretapping features for their own purposes . . . . While the hack was complex, the taps themselves were straightforward. When the [Greek] prime minister, for example, initiated or received a call on his cellphone, the exchange would establish the same kind of connection used in a lawful wiretap—a connection to a shadow number allowing it to listen in on the conversation."); *see also* Ellen Nakashima, *Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say*, Wash. Post, May 20, 2013, http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html.

[39] *See* Nat'l Sec. Agency, DOCID No. 352694, Phone Freaks Can Invade Your Privacy (1976), *available at* http://explodingthephone.com/docs/db904 (declassified NSA memo describing how interfaces used by phone company employees to determine if a line was busy were subverted by outsiders to listen to phone conversations).

[40] *See, e.g.*, Craig Timberg & Lena H. Sun, *Some Say Health-Care Site's Problems Highlight Flawed Federal IT Policies*, Wash. Post, Oct. 9, 2013, http://www.washingtonpost.com/business/technology/some-say-health-care-sites-problems-highlight-flawed-federal-it-policies/2013/10/09/d558da42-30fe-11e3-8627-c5d7de0a046b_story.html ("[T]he root cause is not simply a matter of flawed computer code but rather the government's habit of buying outdated, costly and buggy technology. The U.S. government spends more than $80 billion a year for information-technology services, yet the resulting systems typically take years to build and often are cumbersome when they launch.").

[41] *See* Amy Goldstein, *Poor Planning and Oversight Led to HealthCare.gov Flaws, GAO Finds*, Wash. Post, July 30, 2014, http://www.washingtonpost.com/national/health-science/poor-planning-and-oversight-led-to-healthcaregov-flaws/2014/07/30/2f1a04aa-1814-11e4-9e3b-7f2f110c6265_story.html.

[42] *See* Evan Perez, *FBI Files Go Digital, After Years of Delays*, Wall St. J., Aug. 1, 2012, http://online.wsj.com/articles/SB10000872396390444130304577561361556532528.

[43] *See* Minority Staff of the Homeland Sec. & Governmental Affairs Comm., 113th Cong., The Federal Government's Track Record on Cybersecurity and Critical Infrastructure 7 (2014), *available at* http://www.hsgac.senate.gov/download/?id=8BC15BCD-4B90-4691-BDBA-C1F0584CA66A.

data breaches reported by federal agencies in 2013.[44] Foreign governments have repeatedly penetrated federal systems,[45] with the White House's network being the latest to be breached by foreign hackers.[46]

Given the extreme difficulty of writing secure software and the federal government's poor track record in securing its own systems, it is extremely likely that the surveillance software that federal law enforcement agencies deploy will not be secure and will leave the computers of targets vulnerable to compromise by other parties.

C. Law enforcement agencies will increasingly need zero-day exploits

In order to exploit a security vulnerability in the software on a target's computer, the target's computer must either be running out-of-date software with a known software vulnerability, or agents must know of a vulnerability for which no update exists. As such, targets that regularly patch their software (or use software that automatically updates) may be much harder to infect with malware.

In order to be able to successfully compromise the computers of targets with up-to-date software, law enforcement and intelligence agencies are increasingly seeking to purchase or discover so called "zero-day" (or "0-day") software exploits. Zero-day exploits are special computer code that exploits vulnerabilities in software that are not known to the manufacturer of the software program, and thus, for which no software update exists.[47] Zero day exploits are extremely valuable, because there is no defense against them.[48]

U.S. law enforcement and intelligence agencies have, in recent years, increasingly turned to zero-day exploits in order to gain access to the computers of high value targets. [49] This has in

---

[44] Jeryl Bier, *Security Breaches of Personal Information at Federal Agencies More than Doubles Since 2009*, Wkly. Standard (Apr. 3, 2014), http://www.weeklystandard.com/blogs/security-breaches-personal-information-federal-agencies-more-doubles-2009_786450.html.

[45] *See* Fred Barbash, *Chinese Hackers May Have Breached the Federal Government's Personnel Office, U.S. Officials Say*, Wash. Post, July 10, 2014, http://www.washingtonpost.com/news/morning-mix/wp/2014/07/09/report-chinese-hacked-into-the-federal-governments-personnel-office/.

[46] *See* Ellen Nakashima, *Hackers Breach Some White House Computers*, Wash. Post, Oct. 28, 2014, http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html.

[47] *See* Leyla Bilge & Tudor Dumitras, Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World, Proceedings of the 2012 ACM Conference on Computer and Communications Security (2012), available at http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf ("A zero-day attack is a cyber attack exploiting a vulnerability that has not been disclosed publicly. There is almost no defense against a zero-day attack: while the vulnerability remains unknown, the software affected cannot be patched and anti-virus products cannot detect the attack through signature-based scanning.").

[48] *The Digital Arms Trade*, Economist, Mar. 30, 2013, http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade ("It is a type of software sometimes described as 'absolute power' or 'God'. Small wonder its sales are growing.").

[49] *See* Craig Timber & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, Wash. Post, Dec. 6, 2013, http://www.washingtonpost.com/business/technology/fbis-search-for-mo-suspect-in-bomb-threats-highlights-use-of-malware-for-surveillance/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html (describing the use of a zero-day exploit by the FBI to take over webcams without the indicator light turning on)*; see also* Liam Murchu, *Stuxnet Using Three Additional Zero-Day*

turn fueled a largely unregulated market for zero-day exploits, in which government agencies are active and are often the highest bidder.[50]

Governments spend a lot of money to acquire zero-day exploits. Although there is little verifiable data about the market for such exploits, anecdotal reports suggest that the cost of commercial exploits can be in the hundreds of thousands of dollars.[51] These vulnerabilities are their most effective when no one else knows about them, so rather than alerting the companies whose software can be exploited, governments, including the United States, quietly exploit them.[52] Quite simply, governments that rely on zero-day exploits have prioritized offense over defense.

Although zero-days undoubtedly make it easier to deliver malware to targets and to gain access to difficult-to-penetrate systems, there are significant collateral costs associated with the purchase and use of zero-days by governments. That is, by exploiting these vulnerabilities rather than notifying the companies responsible for the software, governments are putting their own citizens at risk.[53] Several senior ex-U.S. government officials have acknowledged these risks, including ex-NSA/CIA director Michael Hayden,[54] and ex-'cyber czars' Howard Schmidt[55] and Richard Clarke.[56]

Vulnerabilities, Symantec Official Blog (Jan. 23, 2014), http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities (describing the use of zero days in Stuxnet, a piece of malware attributed to the US and Israeli governments); David Sanger, *Obama Orders Sped Up Wave of Cyberattacks Against Iran*, N.Y. Times, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all.

[50] *See, e.g.*, *The Digital Arms Trade*, *supra* ("Other reputable customers, such as Western intelligence agencies, often pay higher prices. Mr Lindelauf reckons that America's spies spend the most on exploits. . . . [B]risk sales are partly driven by demand from defence contractors that see cyberspace as a "new battle domain", says Matt Georgy, head of technology at Endgame, a Maryland firm that sells most of its best exploits for between $100,000 and $200,000."); Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. Times, July 13, 2013, http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?pagewanted=1&_r=1 ("But increasingly the businesses are being outbid by countries with the goal of exploiting the flaws in pursuit of the kind of success. . . that the United States and Israel achieved. . ."); Joseph Menn, *Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback*, Reuters, May 10, 2013, http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510 ("Even as the U.S. government confronts rival powers over widespread Internet espionage, it has become the biggest buyer in a burgeoning gray market where hackers and security firms sell tools for breaking into computers.").

[51] *See* Perlroth & Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, *supra* (describing hackers searching for "secret flaws in computer code that governments pay hundreds of thousands of dollars to learn about and exploit").

[52] Joseph Menn, *U.S. Cyberwar Strategy Stokes Fear of Blowback*, Reuters, May 10, 2013, http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510 ("The core problem: Spy tools and cyber-weapons rely on vulnerabilities in existing software programs, and these hacks would be much less useful to the government if the flaws were exposed through public warnings. So the more the government spends on offensive techniques, the greater its interest in making sure that security holes in widely used software remain unrepaired.").

[53] *Id.* ("The strategy is spurring concern in the technology industry and intelligence community that Washington is in effect encouraging hacking and failing to disclose to software companies and customers the vulnerabilities exploited by the purchased hacks.").

[54] *Id.* ("Acknowledging the strategic trade-offs, former NSA director Michael Hayden said: 'There has been a traditional calculus between protecting your offensive capability and strengthening your defense. It might be time now to readdress that at an important policy level, given how much we are suffering.'").

Indeed, at a time when cyber-attacks are, according to government officials, one of the biggest threats faced by this country,[57] the collateral damage associated with exploiting, rather than fixing, security vulnerabilities is a topic of considerable debate. For example, the President's NSA Review Group observed last year that "[a] vulnerability that can be exploited on the battlefield can also be exploited elsewhere"[58] and recommended that "US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks."[59] Moreover, "in almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection. Eliminating the vulnerabilities—'patching' them—strengthens the security of US Government, critical infrastructure, and other computer systems."[60]

Because so little is known about how the FBI currently delivers malware to surveillance targets, we have no way of knowing how frequently it uses zero-days, or how many it has purchased or otherwise acquired. Even so, as the technology industry moves steadily towards automatic security updates,[61] a practice largely motivated by cybersecurity concerns, the FBI

---

[55] *Id.* ("'It's pretty naïve to believe that with a newly discovered zero-day, you are the only one in the world that's discovered it," said Schmidt, who retired last year as the White House cybersecurity coordinator. 'Whether it's another government, a researcher or someone else who sells exploits, you may have it by yourself for a few hours or for a few days, but you sure are not going to have it alone for long.'"); *see also* Perloth & Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, *supra* ("Governments are starting to say, 'In order to best protect my country, I need to find vulnerabilities in other countries,'" said Howard Schmidt, a former White House cybersecurity coordinator. 'The problem is that we all fundamentally become less secure.'").

[56] Menn, *U.S. Cyberwar Strategy Stokes Fear of Blowback*, *supra* ("Former White House cybersecurity advisors Howard Schmidt and Richard Clarke said in interviews that the government in this way has been putting too much emphasis on offensive capabilities that by their very nature depend on leaving U.S. business and consumers at risk. 'If the U.S. government knows of a vulnerability that can be exploited, under normal circumstances, its first obligation is to tell U.S. users,' Clarke said. 'There is supposed to be some mechanism for deciding how they use the information, for offense or defense. But there isn't.'").

[57] James Clapper, the Director of National Intelligence, and James Comey, the Director of the FBI, have both told Congress that cyber-attacks are the most serious national security threat faced by the United States. *See* Jim Garamone, *Clapper Places Cyber at Top of Transnational Threat List*, Armed Forces Press Service, Mar. 12, 2013, http://www.defense.gov/news/newsarticle.aspx?id=119500; Greg Miller, *FBI Director Warns of Cyberattacks; Other Security Chiefs Say Terrorism Threat Has Altered*, Wash. Post, Nov. 14, 2013, http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0_story.html ("FBI Director James B. Comey testified Thursday that the risk of cyberattacks is likely to exceed the danger posed by al-Qaeda and other terrorist networks as the top national security threat to the United States and will become the dominant focus of law enforcement and intelligence services.").

[58] Review Grp. on Intelligence and Commc'n Techs., Liberty and Security in a Changing World 187 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[59] *Id.* at 37, 219.

[60] *Id.* at 220.

[61] *See* Ellen Messmer, *Microsoft to Start Automatic Updates of IE Without Asking the User*, Network World (Dec. 15, 2011), http://www.networkworld.com/article/2184071/windows/microsoft-to-start-automatic-updates-of-ie-without-asking-the-user.html; *see also* Gregg Keizer, *Google's Chrome Now Silently Auto-Updates Flash Player*, Computer World (Apr. 1, 2010), http://www.computerworld.com/article/2516595/networking/google-s-chrome-now-silently-auto-updates-flash-player.html; Thomas Duebendorfer & Stefan Frei, Why Silent Updates Boost Security (2009), *available at* http://www.tik.ee.ethz.ch/file/ef72343372ca8659a9ae8a98873167c0/TIK-Report-302.pdf.

may increasingly need zero-days in the future, as it will no longer be able to rely on targets running out of date, insecure software.

For example, the FBI has performed several successful watering hole attacks targeting visitors to websites that could only be accessed using Tor.[62] In at least one of these operations, the FBI's malware was delivered with code that exploited a security vulnerability for which a fix existed, and had been included in an update to the Tor Browser Bundle software that was made available a month before the FBI's operation.[63] Until September of 2014, the Tor Browser Bundle did not include a built-in security update mechanism.[64] When updates were available, users had to go to the Tor Project website and download the updates for themselves. Many users did not do this, and so it is not surprising that FBI was able to successfully deliver malware to a number of Tor users without needing to exploit a zero-day vulnerability. Earlier this year, The Tor Project introduced a mechanism to more easily update the Tor browser software, and the organization has long been working on making security updates automatic.[65]

The Department of Justice has told this Committee that one of the primary motivations for its proposal is the problem posed by anonymizing technologies like Tor.[66] However, once the Tor Project completes the planned automatic security update feature, the successful compromise of Tor users will require zero day security vulnerabilities. This committee should therefore understand that if it wishes to provide law enforcement agencies the ability to identify and locate Tor users, then that ability will necessarily require blessing the exploitation of zero day vulnerabilities as a law enforcement technique. The raises significant public policy concerns.

D. The tech industry's embrace of cloud computing significantly complicates watering hole attacks.

In August 2013, all of the websites hosted by Freedom Hosting—a service that hosted websites through the Tor network— began serving an error message with hidden code embedded

---

[62] *See* Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, *supra*; Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, *supra*. "Tor 'is a network of virtual tunnels that allows people to improve their privacy and security.' Originally developed by the Naval Research Lab and subsequently funded by the Defense Advanced Research Projects Agency ('DARPA') to facilitate anonymous online activities by government personnel. Tor is an 'onion routing' technology which hides a user's IP address, making it appear to originate from a Tor server rather than the actual address from which the user is connecting to the Internet." Pell, *supra*, at 38 (citations omitted).

[63] *See* Posting of Andy Isaacson, adi@hexapodia.org, to liberationtech@ lists.stanford.edu (Aug. 5, 2013) (*available at* https://mailman.stanford.edu/pipermail/liberationtech/2013-August/010498.html) (stating that the fix to the exploit had been included in an update to the Tor Browser Bundle released on June 26, 2013).

[64] *See* mikeperry, *Tor Browser 3.6.5 and 4.0-alpha-2 Are Released*, Tor Blog (Oct. 30, 2014), https://blog.torproject.org/blog/tor-browser-365-and-40-alpha-2-are-released (describing the new update mechanism included in the 4.0 alpha-2 release of the Tor Browser bundle).

[65] *See* phobos, *Google Funds an Auto-Update for Vidalia*, Tor Blog (June 6, 2008), https://blog.torproject.org/blog/google-funds-auto-update-vidalia; *see also* Tor Browser Launcher, Micah Lee's Blog, https://micahflee.com/torbrowser-launcher/ (describing an independent effort to create an automatic Tor security update delivery mechanism)

[66] *See* Advisory Committee Materials at 171 ("The proposed amendment would better enable law enforcement to investigate and prosecute botnets and crimes involving Internet anonymizing technologies, both which pose substantial threats to members of the public."); *id.* at 160 ("Currently, the Department obtains remote access warrants primarily to combat Internet anonymizing techniques.").

in the page.[67] That code was specifically designed to exploit a security flaw in a version of the Firefox web browser used to access Tor hidden servers.[68] According to an FBI agent who later testified in an Irish court, the Freedom Hosting service hosted at least 100 child pornography websites.[69] But the service also hosted a number of legitimate sites, including TorMail, a web-based email service that could only be accessed over the Tor network, and the Hidden Wiki, which one news site described as the "de facto encyclopedia of the Dark Net."[70] Even though these sites were serving lawful content, the FBI's watering hole attack was performed in an overbroad manner, forcing all of the Freedom Hosting sites to deliver malware to visitors, not just those sites that were engaged in the distribution of illegal content.

We are now firmly in the age of cloud computing, in which hundreds of websites may share resources provided by the same powerful servers. Law-abiding Internet users have no way of knowing if the sites that they are visiting are hosted on the same physical server as a site that facilitates illegal conduct. That websites with a potential connection to illegal conduct are hosted on the same server as legitimate websites is not sufficient reason to permit law enforcement agencies to hack into the computers of every person who interacts with a particular server.

The court order that the FBI presumably obtained before launching watering hole attacks from the many Freedom Hosting websites is not public. As such, it is impossible to know what the FBI agents told the court, or what the court authorized. We do not know if the judge authorized watering hole attacks against all visitors to all sites running on the server owned by Freedom Hosting, or if the FBI agents exceeded the scope of the warrant. In any event, this episode demonstrates the importance of strict limits on bulk delivery of remote access malware, including through watering hole attacks.

III. The Proposed Amendment Substantively Expands the Government's Powers and Should Be Addressed by Congress in the First Instance

The Federal Rules of Procedure are limited to "regulating procedure." *Sibbach v. Wilson & Co.*, 312 U.S. 1, 10 (1941). They may not "abridge, enlarge or modify any substantive right." 28 U.S.C. § 2072(b). Although the proposed Committee Note purports to leave "constitutional questions" to be addressed in future case law,[71] in practice the amendment will enlarge the government's substantive power to conduct searches and will decide contested questions of law *sub silentio.*

By amending Rule 41, the government seeks to obtain the power to conduct a category of searches that it is currently barred from conducting. Where the government seeks to remotely search a computer the location of which is unknown, it does not now have a venue in which to

---

[67] *See* Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired (Sept. 13, 2013), http://www.wired.com/2013/09/freedom-hosting-fbi/.
[68] *See* Goodin, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, supra*.
Attackers Wield Firefox Exploit to Uncloak Anonymous Tor Users, Ars Technica (Aug. 5, 2013), http://arstechnica.com/security/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users/.
[69] Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, supra*.
[70] Patrick Howell O'Neill, *An In-Depth Guide to Freedom Hosting, the Engine of the Dark Net*, The Daily Dot (Aug. 4, 2013), http://www.dailydot.com/news/eric-marques-tor-freedom-hosting-child-porn-arrest/.
[71] Proposed Amendments Materials at 341.

apply for a warrant. *In re Warrant to Search a Target Computer at Premises Unknown* ["*In re Warrant*"], 958 F. Supp. 2d 753, 756–58 (S.D. Tex. 2013). In effect, the government lacks the substantive authority to conduct remote access searches in such circumstances. For that reason, the proposed amendment will almost certainly result in a marked increase in government use of remote hacking techniques and zero-day exploits. What looks like a procedural change actually creates a new substantive power: to use zero-day exploits, malware, spyware, and other software packages to circumvent privacy-protective proxy services, including at least one, Tor, which was created by the US government, and continues to receive US government funding.

The government's desire to augment the investigative tools available to it is understandable, but the best, and indeed the proper way to address the government's asserted needs is for it to present its demand to Congress. Lawmakers can then craft a legislative solution to any gap in the government's search powers. As the Supreme Court has remarked, "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." *United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment) (citing Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 805–806 (2004)); *see also City of Ontario, Cal. v. Quon*, 560 U.S. 746, 759 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

When presented with similar questions of invasive technological searches and surveillance, Congress has opted to step in and set detailed legislative rules. This was true of the wiretapping and bugging of wire, oral, and electronic communications through Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III" or the "Wiretap Act"), 18 U.S.C. § 2518, and the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1804. It was likewise true of searches of the contents of stored electronic communications and other digital data in the Stored Communications Act, 18 U.S.C. § 2703, and of real-time individualized telephony metadata collection in criminal and national security investigations in the two acts addressing pen registers, 18 U.S.C. § 3123 and 50 U.S.C. § 1842. Congress clearly has the capacity and the will to legislate in this area, and legislative action is preferable because it lends itself to setting substantive limits on questionable search practices in a way that procedural rulemaking does not. Indeed, members of Congress have begun to take note of this proposed amendment,[72] and would likely welcome the chance to hold hearings and contemplate legislative reform. The Federal Rules should not be amended to give the government new power to conduct remote access searches using zero-day exploits and spyware to defeat privacy-protective tools like Tor. Congress should be given the opportunity to weigh the competing constitutional and policy concerns that the government's proposal raises, and to craft detailed statutory language regulating how, when, and where the government may conduct "remote access" searches.

Instead of using the procedural rulemaking process to suddenly and substantially increase the government's use of remote hacking techniques in criminal investigations, the Committee should reject the proposed amendment and leave the government to present its case to Congress and the American people.

[72] *See* Letter from Sen. Patrick Leahy to Attorney General Eric Holder (Oct. 30, 2014), *available at* https://www.documentcloud.org/documents/1349789-leahy-to-holder-re-fbi-fake-ap-article.html.

IV. The Proposed Amendment Raises Significant Constitutional and Statutory Concerns.

A. Use of Zero-Day Exploits and Malware May Constitute an Unreasonable Search.

Under the Fourth Amendment, use of zero-day exploits or malware may constitute an unreasonable search. It is well established that some searches in the physical world are too intrusive, destructive, or dangerous to be reasonable:

> The general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant. Excessive or unnecessary destruction of property in the course of a search may violate the Fourth Amendment, even though the entry itself is lawful and the fruits of the search are not subject to suppression.

United States v. Ramirez, 523 U.S. 65, 71 (1998) (citation omitted).

Surgically removing evidence from a suspect's body,[73] using a powerful motorized battering ram to break into a residence,[74] and "employ[ing] a flashbang device [to enter a house] with full knowledge that it will 'likely' ignite accelerants and cause a fire"[75] have all been ruled unreasonable under the Fourth Amendment. Zero-day exploits may well pose analogous concerns. When the government unleashes zero-day exploits and malware, it will rarely be able to control who can intercept the code in transmission, whether it will reach its intended target, whether it will be copied and reused by others, and whether it will spread virally across the internet and cause damage to innocent persons and businesses.[76] *See* Part II, *supra*. These factors are relevant to individual warrant applications, but also to the Advisory Committee's consideration of the proposed Rule amendment, because these outcomes are entirely predictable as a natural result of the kinds of searches the government wants the authority to conduct.

For example, when the United States and Israel launched the Stuxnet cyber-attack against Iranian nuclear enrichment facilities several years ago, it quickly spread beyond the targeted

---

[73] *Winston v. Lee*, 470 U.S. 753, 759, 766–67 (1985) (holding that the health risks posed by the "compelled surgical intrusion into an individual's body for evidence" make that search unreasonable under the Fourth Amendment); *see also Schmerber v. California*, 384 U.S. 757, 771–72 (1966) (requiring that a search involving drawing a suspect's blood be "performed in a reasonable manner," including that it be carried out by medical personnel in a medical environment); *Rochin v. California*, 342 U.S. 165, 172 (1952) (conduct by agents trying to obtain swallowed evidence, including "the forcible extraction of [the defendant's] stomach's contents," violates due process).

[74] *Langford v. Superior Ct. of L.A. Cnty.*, 729 P.2d 822, 827 (Cal. 1987) (holding that, because a motorized battering ram can cause "potential danger from collapse of building walls and ceilings or through rupture of utility lines," which could cause fires that "could threaten the safety not only of occupants, but of entire neighborhoods," "routine deployment of the ram to enter dwellings must be considered presumptively unreasonable unless authorized in advance by a neutral magistrate, and unless exigent circumstances develop at the time of entry").

[75] *Bing ex rel. Bing v. City of Whitehall, Ohio*, 456 F.3d 555, 570 (6th Cir. 2006).

[76] *E.g.*, Rachel King, *Stuxnet Infected Chevron's IT Network*, Wall St. J., Nov. 8, 2012, http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/.

computer systems.[77] Major U.S. companies, including Chevron, discovered that the Stuxnet software had infected their networks as well.[78] If a piece of targeted malware developed with the vast resources of defense and national security agencies can go astray in this way, there is no reason to think law enforcement surveillance malware won't do so too.

Although it took several years before Stuxnet was discovered by security researchers,[79] the Stuxnet code and the zero-days it leveraged were extensively analyzed by a world-wide network of security experts. Although Microsoft rushed to develop and distribute patches for these vulnerabilities, criminals also took note, and exploited the same vulnerabilities for their own nefarious purposes.[80]

More broadly, the use of malware and zero-day exploits is more invasive than other forms of permissible searches because the consequences and collateral damage associated with their use are inherently unpredictable and often irreversible. Because computers and the software they run are incredibly complicated systems, the consequences of their surreptitious penetration and exploitation by the government are inherently unpredictable. Malware can cause computer systems to fail in many unintended ways, causing the loss of property entirely unrelated to the government's searches. For example, a piece of malware could—whether through poor design or unpredictable interaction with other software on the target's computer—cause the destruction of data (such as family photos or document drafts) or the corruption of the operating system. The resulting data loss might or might not be reversible, depending on the circumstances.

The technological and internet-security implications of remote access searches are unavoidably complex. Before courts wade into the constitutional questions that the use of malware and zero-day exploits raise, it would be best for Congress to affirmatively address the wisdom and parameters of their use after informed public discussion. The policy and constitutional concerns that remote access searches raise are better suited to comprehensive legislative regulation than to authorization through procedural changes to the Federal Rules.

B. The Proposed Amendment Authorizes Searches That Can Only Be Carried Out Pursuant to a Title III Wiretap Order, and Would Be Illegal if Authorized by a Simple Rule 41 Warrant

Depending on the means used to conduct remote access searches and the information gathered, such searches may only be permissible pursuant to an order issued under the Wiretap Act, 18 U.S.C. § 2518, or a surveillance warrant containing equivalent protections. A normal warrant application submitted under Rule 41 may be constitutionally insufficient and infirm.

---

[77] Sanger, *supra* ("An error in the code, they said, had led it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world.").

[78] King, *Stuxnet Infected Chevron's IT Network*, *supra*.

[79] David Kushner, *The Real Story of Stuxnet*, IEEE Spectrum (Feb. 26, 2013), http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[80] Pierluigi Paganini, *Kaspersky Revealed that Stuxnet Exploits Is Still Used Worldwide*, Security Aff. (Aug. 19, 2014), http://securityaffairs.co/wordpress/27633/cyber-crime/stuxnet-flaw-still-targeted.html.

The Wiretap Act, also known as Title III, applies when the government seeks to intercept wire, oral, or electronic communications in real time. Because this sort of electronic surveillance raises, "understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens," special protections are required. *United States v. U.S. District Ct.*, 407 U.S. 297, 312 (1972). Under Title III, these protections include requirements that the government particularly describe the place and person to be surveiled, that the government show it has exhausted other investigative procedures prior to seeking a Title III order, and that the court limit the duration of the surveillance and require minimization of interception of non-pertinent communications. 18 U.S.C. § 2518(1)–(5). Moreover, unlike with search warrant applications, attorneys at DOJ's Office of Enforcement Operations review each wiretap application before it is submitted to a court.[81] Courts have also imposed Title III's requirements on applications for warrants to authorize surreptitious video surveillance, even though such surveillance is not technically covered by the statute. *See, e.g.*, *United States v. Cuevas–Sanchez*, 821 F.2d 248, 250 (5th Cir. 1987); *United States v. Biasucci*, 786 F.2d 504, 510–11 (2d Cir. 1986); *United States v. Torres*, 751 F.2d 875, 884 (7th Cir. 1984). These requirements, for both wiretapping and video surveillance, derive from and are required by the Fourth Amendment. *See Berger v. New York*, 388 U.S. 41, 58–59 (1967) (wiretapping); *Torres*, 751 F.2d at 884 (video surveillance).

Remote access searches can raise identical or analogous concerns. Certainly, if the government seeks to activate the built-in camera on a target computer, it must meet the heightened requirements for video surveillance. *In re Warrant*, 958 F. Supp. 2d at 759–61. If the government's remote access surveillance software is configured to turn on the target computer's microphone or to collect the contents of incoming or outgoing electronic or wire communications (such as emails, instant messages, or internet-based phone calls), Title III procedures would be required. *See* 18 U.S.C. § 2518. Further, "[s]oftware that can retrieve [other stored] information—Internet browser history, search terms, e-mail contents and contacts, 'chat', instant messaging logs, photographs, correspondence, and records of applications run, among other things"—also calls for heightened Fourth Amendment protections, because surreptitious and remote retrieval of such a "volume of information" raises constitutional concerns. *In re Warrant*, 958 F. Supp. 2d at 760. Electronic surveillance that "is identical in its indiscriminate character to wiretapping and bugging" cannot be authorized by a normal Rule 41 warrant. *Torres*, 751 F.2d at 885 (emphasis omitted).

Indeed, as explained above, remote access searches raise even more significant concerns in that malware and the exploitation of zero-day flaws can cause entirely unpredictable and irreversible damage to a target's computer or data. Reducing the likelihood of, or mitigating the harms of, such unintended consequences would require significant technical expertise and

[81] H.R. Rep. No. 112-546, at 10 (2012), *available at* http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt546/pdf/CRPT-112hrpt546.pdf ("In a letter to Chairman Issa, the Deputy Attorney General acknowledged that the Office of Enforcement Operations (OEO), part of the Justice Department's Criminal Division, is 'primarily responsible for the Department's statutory wiretap authorizations.' According to the letter, lawyers in OEO review these wiretap packages to ensure that they 'meet statutory requirements and DOJ policies.' When OEO completes its review of a wiretap package, federal law provides that the Attorney General or his designee—in practice, a Deputy Assistant Attorney General in the Criminal Division—reviews and authorizes it. Each wiretap package includes an affidavit which details the factual basis upon which the authorization is sought.").

regulation of the manner in which the government develops and deploys its remote access software. Courts are ill-suited to oversee such mitigation efforts in the first instance.

Any malware, spyware, or other government software that remains on a target computer and collects information on an ongoing basis also implicates these concerns. Clandestine entry into a person's computer, installation of software there, and use of that software to conduct real-time surveillance should require the heightened showing of a Title III order. A warrant issued under normal Rule 41 procedures that authorizes an ongoing search will necessarily violate the Fourth Amendment; restrictions are needed "to guarantee that . . . [these searches] occur[] only when there is a genuine need for [them] and only to the extent that [they are] needed." *Dalia v. United States*, 441 U.S. 238, 250 (1979). Yet, it is clear that the government is *already* collecting information about computer users on an ongoing basis using remote access malware without obtaining a Title III order or equivalent judicial process. Approving the proposed amendment would give sanction to this highly problematic practice.

In an investigation in Washington State in 2007, the FBI applied for a hybrid order to justify its installation and monitoring of the CIPAV surveillance software: a Rule 41 warrant to authorize transmission and installation of the software and its one-time use to collect location, identification, and other data from the target computer, combined with a pen register order to authorize ongoing collection of "routing and destination addressing information for electronic communications originating from the activating computer."[82] A hybrid order of this type cannot substitute for the strictures of Title III.

A pen register order is intended to be served on a "person or entity providing wire or electronic communication service," 18 U.S.C. § 3123(a)(1), to compel their assistance in turning over "dialing, routing, addressing, or signaling information," *id.* § 3127(3). Installation of spyware on a person's computer and contemporaneous monitoring of information about all types of electronic communications originating from that computer is a good deal more invasive, because it relies on entry into a person's private space and maintenance of a presence there to collect information. This is, in effect, a trespassory search. *Cf. United States v. Jones*, 132 S. Ct. 945, 949 (2012) (holding that a Fourth Amendment search occurred when "[t]he Government physically occupied private property for the purpose of obtaining information"). It is also the kind of unusually intrusive surveillance to which the heightened standard of Title III applies. The government appears to want to use the pen register statute to authorize what a Rule 41 warrant cannot standing alone, but that defies common sense. As Judge Stephen Smith explained while rejecting a variant of the government's hybrid order theory in another context, "[s]urely if these various statutory provisions were intended to give birth to a new breed of electronic surveillance, one would expect Congress to have openly acknowledged paternity somewhere along the way. This is especially so given that no other form of electronic surveillance has th[is] mixed statutory parentage." *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 764–65 (S.D. Tex. 2005). Invasive monitoring carried out by

[82] Affidavit of Norman B. Sanders Jr. at 4, 13, *In re Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Message(s) Delivered to that Account by the Government*, MJ-07-88 (W.D. Wash. June 12, 2007), *available at* https://www.eff.org/document/fbicipav-08pdf.

installing malware on a target's computer should require a Title III order—or new congressional legislation—not a cobbled-together patchwork of lesser permissions.

Adopting the proposed amendment to Rule 41 risks facilitating violations of Title III and deciding by administrative rulemaking a question better left to Congressional regulation—how to regulate and circumscribe the controversial and invasive search techniques at issue here.

C. The Proposed Amendment Will Facilitate Violations of the Fourth Amendment's Particularity Requirement and Will Result in Searches of Non-Suspects as to Whom There is No Probable Cause.

The proposed amendment would allow police to remotely search many people's computers using a single warrant, often without particularly describing those computers or demonstrating probable cause as to their owners or users. A warrant that does not particularly describe the place to be searched and things to be seized is invalid. *Groh v. Ramirez*, 540 U.S. 551, 557 (2004) (citing U.S. Const. amend IV). For this reason, courts have been skeptical of warrants authorizing searches of multiple locations not owned by the same person.[83] In the context of physical searches, "[t]he general rule is that a warrant for a building that has multiple units must specify the individual unit that is the subject of the search to satisfy the particularity requirement."[84] The same concerns and rules should apply when police search digital "occupancies." Indeed, "[t]he need for particularity . . . is especially great in the case of eavesdropping." *Berger*, 388 U.S. at 56. So, too, for remote access hacking.

Further, a search warrant that demonstrates probable cause as to one suspect or location does not thereby justify any search anywhere. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 554 (1978) (second emphasis added) ("[V]alid warrants may be issued to search *any* property, whether or not occupied by a third party, *at which there is probable cause* to believe that fruits, instrumentalities, or evidence of a crime will be found.").[85] The Wiretap Act illustrates application of this principle to warrants authorizing invasive electronic surveillance: the government must demonstrate not only that there is probable cause of commission of a qualifying criminal offense, but also that there is probable cause for belief "that particular communications concerning that offense will be obtained through such interception" and that the facilities or places to be wiretapped or bugged are being used in connection with the offense or

[83] "[I]n the case of multi-location search warrants, the magistrate must be careful to evaluate each location separately. 'A search warrant designating more than one person or place to be searched must contain sufficient probable cause to justify its issuance as to each person or place named therein.'" *Greenstreet v. Cnty. of San Bernardino*, 41 F.3d 1306, 1309 (9th Cir. 1994) (quoting *People v. Easely*, 671 P.2d 813, 820 (Cal. 1983)).

[84] Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1045 n.173 (2010) (citing *Jacobs v. City of Chicago*, 215 F.3d 758, 767 (7th Cir. 2000)). *See also United States v. Hinton*, 219 F.2d 324, 325–26 (7th Cir. 1955) ("For purposes of satisfying the Fourth Amendment, searching two or more apartments in the same building is no different than searching two or more completely separate houses."); *United States v. Clark*, 638 F.3d 89, 98 (2d Cir. 2011) (warrant defective where issuing judge was not informed of building's size or number of residential units and was incapable of making probable cause determination of defendant's control of entire multi-family building).

[85] *See also, e.g.*, *Commonwealth v. Cefalo*, 409 N.E.2d 719, 726 (Mass. 1980) ("In the case of a search warrant, . . . the affidavit must, in order to establish probable cause, contain enough information for the issuing magistrate to determine that the items sought are related to the criminal activity under investigation, *and that they may reasonably be expected to be located in the place to be searched*." (emphasis added)).

used by the targeted person. 18 U.S.C. § 2518(3)(a)–(d). Remote, surreptitious computer searches should be held to the same standard.

Authorizing the kinds of remote access searches that the government seeks to conduct threatens to violate the Fourth Amendment's particularity and probable cause requirements in several ways. First, if the government configures a website or server to deliver malware to the computer of every person who visits it (a watering hole attack), it will likely end up searching the computers of people who it cannot particularly identify or describe and as to whom it lacks probable cause. There do exist a small subset of websites or servers where all access may violate the law (websites that do nothing more than distribute child pornography might qualify). However, issuing a search warrant authorizing the surreptitious delivery of malware onto the computers of an unknown number of targets raises serious legal and policy questions. Moreover, even if orders for bulk installation of malware are deemed to be proper, the vast majority of websites or servers that the government might commandeer to deliver malware to visitors' computers will be visited by both legitimate targets and non-targets alike. For example, members of the press, researchers, policymakers, and attorneys regularly visit websites associated with terrorist groups, cyber-criminals, and drug dealers.[86] Were courts to authorize the installation of malware to all visitors to these and other types of websites, the government would undoubtedly end up searching the computers of innocent people who are not engaged in any crime, who have a perfectly valid reason to have visited the site, and as to whom there is no probable cause.

The same may be true of more targeted delivery of remote access hacking software. For example, when the government delivered spyware to a suspect in a 2007 investigation in Washington, it did so by creating a fake Associated Press story and then sending a link to one of the suspect's social media accounts.[87] "When the suspect clicked on the link, the hidden FBI software [installed itself on his computer and] sent his location and Internet Protocol information to agents."[88] Had the suspect forwarded the link to acquaintances, posted it on social media, or otherwise distributed it, people as to whom the government lacked probable cause would likely have clicked on the link and triggered a search of their computers. The same would have happened if the government had posted the link to a public portion of the suspect's social media account (it is not known whether the government did so because public information about the search is limited). Likewise, if an internet search engine had indexed the fake page,[89] any internet user could have happened upon the link during a search, clicked on it, and triggered a search of their computer. Once released into the world, government malware is difficult to contain.[90] A warrant could not have authorized these collateral, but foreseeable searches because

[86] Indeed, the reason the American public learned about the Target data breach (and many others) is because a journalist regularly reads invitation-only cyber-crime forums. *See* Brian Krebs, *Cards Stolen in Target Breach Flood Underground Markets*, Krebs on Security (Dec. 20, 2013), http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/#more-24093.

[87] Gene Johnson, *FBI Says It Faked AP Story to Catch Bomb Suspect*, Associated Press, Oct 28, 2014, http://bigstory.ap.org/article/29ae75189b254e47bfb79c3a0de256ec/ap-seattle-times-upset-about-fbi-impersonation; *see also* Mike Carter, *FBI Created Fake Seattle Times Web Page to Nab Bomb-Threat Suspect*, Seattle Times, Oct. 27, 2014, http://seattletimes.com/html/localnews/2024888170_fbinewspaper1xml.html.

[88] Carter, *supra*; *see also* Johnson, *supra*.

[89] *See* Google, Crawling & Indexing, http://www.google.com/insidesearch/howsearchworks/crawling-indexing.html ("We use software known as 'web crawlers' to discover publicly available webpages.").

[90] *See, e.g.*, Rachel King, *Stuxnet Infected Chevron's IT Network*, Wall St. J., Nov. 8, 2012, http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/.

the government would have lacked probable cause as to the people searched, and could not have particularly described the places to be searched or digital files to be seized.

Individual magistrate judges reviewing warrant applications may be able to address some of these concerns in some cases. But because these defects will pervade remote access warrant applications and are entirely predictable, the best course is to reject the proposed amendment and allow Congress the opportunity to set detailed rules concerning particularity and probable cause.

D. The Proposed Amendment Weakens Rule 41's Notice Requirement

The proposed amendment modifies Rule 41's notice requirement so that for remote access searches the government "must *make reasonable efforts* to serve a copy of the warrant on the person whose property was searched or whose information was seized or copied."[91] The means of service must be "*reasonably calculated* to reach that person."[92] This departs from the normal requirement that "[t]he officer executing the warrant *must* give a copy of the warrant and a receipt for the property taken to the person" subject to the search. Fed. R. Crim. P. 41(f)(1)(C) (emphasis added).

The proposed language clearly contemplates searches for which no notice can be provided. Indeed, the circumstances in which the government will likely seek authority to conduct remote access searches all but guarantee that notice will be difficult if not impossible to provide in many or most cases. If, for example, the government seeks to learn the identity and location of a particular internet user, it might often be the case that all it learns is that the user is connected to the internet from an IP address associated with a coffee shop in a large urban area. It is not at all clear that any means would be available to the government to reliably provide notice in that likely typical scenario.

But failure to provide notice "casts strong doubt on [a warrant's] constitutional adequacy." *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (citing *Berger*, 388 U.S. at 60). As the Ninth Circuit has explained,

> [a] warrant [i]s constitutionally defective [if it] fail[s] to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry. . . . We take this position because surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment. The mere thought of strangers walking through and visually examining the center of our privacy interest, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth Amendment, demands that surreptitious entries be closely circumscribed.

Id.; see also United States v. Villegas, 899 F.2d 1324, 1337 (2d Cir. 1990) ("[I]f a delay in notice is to be allowed, the court should nonetheless require the officers to give the appropriate person notice of the search within a reasonable time after the covert entry.").

[91] Proposed Amendments Materials at 340 (emphasis added).
[92] *Id.* (emphasis added).

Surreptitious entry into a repository of a person's electronic files, containing digital analogues of her diaries, address books, letters, and photo albums, raises no less important concerns. *See United States v. Payton*, 573 F.3d 859, 861–62 (9th Cir. 2009) ("There is no question that computers are capable of storing immense amounts of information and often contain a great deal of private information. Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers."). Even when police seek to search only a limited set of data on a computer, the importance of notice is paramount. Computers "store and intermingle a huge array of one's personal papers in a single place[, which] increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs." *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009). And even if no data is copied during the search, the surreptitious entry itself raises concerns, particularly when it is achieved using means that may expose the computer user to malicious incursions by other actors taking advantage of the government's means and method of entry.[93]

Another problem with the proposed amendment is that it will allow the government to provide notice to either "the person whose property was searched *or* whose information was seized or copied."[94] When those are different people, notice should be given to both. If, for example, the government were to conduct a remote access search of a computer owned by one person but used by others, it could interpret the rule to allow it to provide notice to only the owner, but not to the person whose files ("information") were actually seized or copied. This would be so even if the seized files were located in a password-protected folder and were clearly identifiable as being the property of someone other than the computer's owner. The computer's owner may fail to, or be ordered not to, inform the target of the search upon receiving notice from the government. Thus, the target might never learn of the search, and therefore never be able to challenge its constitutionality. To avoid this problem, "or" should be replaced with "and."

Finally, even in situations where the government's efforts to provide notice to the proper person eventually succeed, notice will often be delayed. An increase in delayed-notice searches occasioned by the proposed amendment raises concerns. In the context of Title III, Congress has implicitly authorized covert entry and delayed notice when installing and operating surveillance equipment, but only when the government complies with "detailed restrictions" that "guarantee that wiretapping or bugging occurs only when there is a genuine need for it and only to the extent that it is needed." *Dalia*, 441 U.S. at 250; *see* 18 U.S.C. § 2518 (imposing duration and minimization requirements on wiretap orders). Similar safeguards have been imposed by courts to regulate video surveillance. *See, e.g.*, *Biasucci*, 786 F.2d at 510–11. Delayed notice may be permissible if it is of short duration and reviewed by a judge, but it has the potential to interfere with substantive Fourth Amendment rights if too heavily, widely, or extensively used. To the extent "remote access" searches are permissible at all, any delay of notice must be specifically

[93] The proposed amendment may also violate the knock-and-announce rule. As the Supreme Court has explained, the Fourth Amendment does not "permit[] a blanket exception to the knock-and-announce requirement for [an] entire category of criminal activity." *Richards v. Wisconsin*, 520 U.S. 385, 388 (1997). Neither the government nor courts may "dispens[e] with case-by-case evaluation of the manner in which a search [is] executed," including when it comes to knock-and-announce. *Id.* at 392. To the extent that remote access search warrants are permissible at all, unannounced searches may sometimes be justified by a specific factual showing under the circumstances of a particular case. But a categorical rule permitting unannounced searches may violate the Fourth Amendment.

[94] Proposed Amendments Materials at 340 (emphasis added).

justified in the individual case, notice must be given "within a reasonable time after the covert entry," and the restrictions currently imposed on wiretap and video surveillance warrants must be observed. *Villegas*, 899 F.2d at 1336–37.

It is perhaps for the very reason that remote access searches raise intractable notice problems that neither Congress nor the courts have yet seen fit to permit the government the general authority to search individuals whose locations are entirely unknown. It may be that the inability to guarantee notice in the mine-run of remote access searches could be overcome in some technological or legislative manner. But that possibility is best left to congressional inquiry in the first instance.

V. The Proposed Amendment Raises Wide-Ranging Questions That the Committee Should Consider Now, Because Those Questions are Unlikely to Be Addressed in Individual Cases for Years to Come

The Advisory Committee should proceed with extreme caution before expanding the government's authority to conduct remote electronic searches. As explained above, the proposed amendment would significantly expand the government's authority to conduct searches that raise troubling and wide-ranging constitutional, statutory, and policy questions. If the Committee approves the proposed amendment, courts are unlikely to address these questions in individual cases, at least not in the foreseeable future. Therefore, it is vital that the Committee carefully consider all of the implications of the proposed amendment now. If those implications cannot be adequately addressed through a change to the Federal Rules—which they cannot—the Committee's best course would be to reject the proposal and leave it to Congress to take up the question.

Even if the Advisory Committee determines that the proposed amendment will "govern[] only 'the manner and the means' by which the litigants' rights are 'enforced,'" and will not "alter[] 'the rules of decision by which [the] court will adjudicate [those] rights,'" *Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 407 (2010) (second and third alterations in original), it should still be reticent to approve the amendment. The constitutional questions raised by the amendment include what limitations the particularity, probable cause, and reasonableness requirements of the Fourth Amendment impose on remote access searches. These will likely not be addressed by courts for years, if ever. Moreover, important policy questions involving cybersecurity and government exploitation of internet and software vulnerabilities are implicated, as are conflicts with the text and intent of the Wiretap Act. In order to prevent violations of the Fourth Amendment and an unchecked expansion of government power, this Committee should grapple with these issues now. The Department of Justice should request the authority it seeks from Congress, so as to permit a public debate about the propriety of the intrusive techniques it proposes to use and about possible alternatives that Congress would be in a unique position to craft.

There are several reasons why courts are unlikely to address Fourth Amendment limits on remote access searches in the near future. For one, warrant applications are considered by judges *ex parte* and without adversarial argument. While magistrate judges are experienced in assessing general questions of particularity and probable cause in run-of-the-mill warrant applications, they

are likely to be ill-equipped to provide robust review of applications for remote access warrants without adversarial briefing, particularly when the search warrant applications do not make clear that agents are seeking permission to hack into the computers of surveillance targets. Full appraisal of these applications requires technical expertise about electronic data storage issues, internet architecture, and cybersecurity. Applications that appear reasonable on their face in light of a magistrate judge's limited technical understanding may in fact fail the particularity and reasonableness requirement upon closer study. But without detailed technical knowledge—or adversarial briefing explaining the issues—many of these concerns will go unnoticed and unaddressed.

Further, orders granting or denying warrants are rarely published and are usually sealed.[95] The likelihood of magistrate judges *sua sponte* publishing detailed opinions analyzing Fourth Amendment issues involved in electronic searches is particularly low when they are unable to independently identify the constitutional infirmities of the warrant application. Indeed, although the government has already sought warrants to authorize remote access searches,[96] there is only one published opinion of a magistrate judge grappling with the Fourth Amendment issues involved. *See In re Warrant*, 958 F. Supp. 2d 753. There is no telling how long it will be until there is another.

Additionally, notice may be delayed for significant periods of time, thus forestalling the time when the target of a remote access search could challenge its constitutionality. *See* Fed. R. Crim. P. 41(f)(3); 18 U.S.C. § 3103a(b)–(c). And even when notice is given, ex post judicial review is limited by doctrines precluding or discouraging a ruling on the constitutionality of the government's conduct. In criminal prosecutions, defendants may challenge the constitutionality of a search through motions to suppress. In response to such motions, the government is likely to argue that investigating officers were relying in good faith on a facially valid warrant when conducting the search. *See United States v. Leon*, 468 U.S. 897 (1984). Courts frequently address the good-faith exception before—and to the exclusion of—the substantive Fourth Amendment claim when denying motions to suppress.[97] Thus, even in cases where a remote access warrant fails the particularity, probable cause, or reasonableness requirements of the Fourth Amendment, courts will generally avoid ruling on the issue.

The doctrine of qualified immunity functions in much the same way to preclude substantive adjudication in suits seeking damages for violations of Fourth Amendment rights.[98]

---

[95] *See* Laura Donahue, Professor, Georgetown Univ. Law Ctr., Remarks at Panel on the Legal and Policy Implications of Hacking by Law Enforcement at Yale Law School ("Remarks by Laura Donahue"), at 18:00–21:40 (Feb. 18, 2014), http://vimeo.com/88165230 (stating knowledge of dozens of cases involving government use of hacking tools, but explaining that most of the relevant magistrate judge orders are sealed).

[96] *Id.*

[97] *See, e.g.*, *United States v. Clay*, 646 F.3d 1124, 1128 (8th Cir. 2011) ("[T]he district court properly denied [the defendant's] motion to suppress based on the *Leon* good-faith exception. In light of this conclusion, we need not reach the underlying question of probable cause."); *United States v. Woodbury*, 511 F.3d 93, 99 (1st Cir. 2007) ("We need not address [the defendant's] particularity arguments because we find that the *Leon* good faith exception applies."); *United States v. Cherna*, 184 F.3d 403, 407 (5th Cir. 1999) ("If [the *Leon* good faith exception applies], we end our analysis and affirm the district court's decision to deny the motion to suppress. . . . If the good-faith exception applies, we need not reach the question of probable cause.").

[98] *See Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388 (1971). Suits for injunctive and declaratory relief are likely to be barred by standing doctrine, on the basis that a person targeted by a remote

Qualified immunity "protects government officials from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known." *Pearson v. Callahan*, 555 U.S. 223, 231 (2009) (internal quotation marks omitted). Courts have discretion to address qualified immunity before determining whether the government has violated a plaintiff's constitutional rights, *id.* at 236, and they frequently do so. Courts often dispose of cases seeking relief for Fourth Amendment violations by concluding that there was no clearly established law at the time of the search which would have put law enforcement on notice that their conduct was unconstitutional. *See, e.g.*, *Messerschmidt v. Millender*, 132 S. Ct. 1235 (2012) (finding qualified immunity and declining to rule on whether facts stated in a warrant application established probable cause). The issues raised by warrants for remote, extra-district electronic searches are necessarily novel because the Federal Rules have not heretofore authorized them. Therefore, the government will almost certainly argue that qualified immunity applies. Perversely, the very absence of case law addressing these searches will mean there is likely to be little development of case law addressing the constitutionality of these searches in the future.

Accordingly, the time to address the constitutional concerns raised by the proposed amendment is now. Speculation that these important issues will be fully dealt with in future case law is unlikely to prove correct, at least in the near future. The significant issues involved counsel caution, and the right course is to reject the proposed amendment and let Congress act.

These problems are exacerbated by the government's lack of candor about the nature of its remote access searches. The DOJ's explanations of its remote access search capability in the sample warrant applications,[99] in warrant applications actually filed in federal court,[100] and in its recent memoranda to this Committee fail to fully describe the nature and invasiveness of its contemplated and completed remote access searches. As described above, one use of the proposed amendment will be to enable searches involving malware or spyware that take advantage of zero-day vulnerabilities and that travel over the open internet. But nothing in the government's descriptions of its "network investigative techniques"[101] or "remote network techniques"[102] would put a magistrate judge (or, for that matter, a member of this Committee) on notice that the government seeks to hack into the computers of targets, exploiting publicly unknown security flaws in the software on those devices using techniques that may create significant cybersecurity collateral damage to the target and to others, and that may fail the reasonableness and particularity requirements of the Fourth Amendment.[103]

---

access search in the past will not be able to prove a likelihood that they will be subjected to such a search again in the future. *See City of L.A. v. Lyons*, 461 U.S. 95 (1983).

[99] *See* Advisory Committee Materials at 181–235.

[100] *See, e.g.*, Affidavit of Justin E. Noble in Support of Application for Search Warrant, *In re Search of Network Investigative Technique ("NIT") for E-mail Address 512SocialMedia@gmail.com*, No. 12-mj-748-ML (W.D. Tex. Dec. 18, 2012); Third Amended Affidavit of William A. Gallegos In Support of Application for Search Warrant, *In re Search of Network Investigative Technique ("NIT") for Email Address texan.slayer@yahoo.com*, No. 12-sw-05685-KMT (D. Colo. Dec. 11, 2012).

[101] *See, e.g.*, Advisory Committee Materials 200–03.

[102] *See, e.g.*, *id.* 216.

[103] *See* Remarks by Laura Donahue, *supra*, at 21:45–22:17 ("Often [the government's] applications do not include detailed technology, or technological explanation as to how it is actually going to be executed, enter the computer, exactly what information is going to be obtained, which other devices might be infected, how many devices may be infected, and so on.").

It is crucial that the government provide full and accurate information to magistrate judges (and to this Committee) when seeking authority to conduct novel and invasive searches.[104] The Advisory Committee should not authorize new search powers without ensuring that the duty of candor has been and will be satisfied. At a minimum, the Advisory Committee Notes accompanying the proposed amendment should speak to this issue.

VI. Recommendations

The ACLU recommends that the Committee reject the proposed amendment to Rule 41. The proposed amendment raises myriad technological, policy, and constitutional concerns. Some of those might be addressed through careful regulation; others are inherent in even the most circumscribed versions of the proposal. The dramatic expansion of investigative power that the government seeks should not be authorized through a change to the Rules of Procedure. Rather, if the government wants this power, it should seek congressional action.

Should Congress decide that remote access searches in the situations covered by the proposed amendment are to be permitted, the ACLU would recommend a set of restrictions to mitigate its concerns, including:

- Require a Title III order for any remote access search that collects information on an ongoing basis or forces a target's device to generate or collect new data (such as by turning on a computer's webcam or microphone);
- Only permit use of malware against specific and particularly described persons. Watering hole attacks, particularly when performed against sites that share computing resources with other innocent websites, present significant public policy and legal issues which make such attacks problematic;
- Require that the government make explicit in warrant applications that it intends to conduct a remote access search using malware and that it will exploit security vulnerabilities in the software on the target's device to do so, and require the government to describe in detail how the malware will work, how many computers it will affect, how long it will remain installed on those computers, what code will remain on those computers indefinitely, the extent to which there may be irreversible changes or damage to devices, the extent to which insertion of the malware requires the assistance of a third party service provider, what impact there will be on the security of computers of targets and non-target third parties, whether it is reasonably foreseeable that government malware could malfunction, target the wrong people, or fall into the wrong hands, what technical experts have

[104] *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1178 (Kozinski, C.J., concurring) ("[O]mitting . . . highly relevant information [about a search of electronic data] is inconsistent with the government's duty of candor in presenting a warrant application. A lack of candor in this or any other aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data."); *cf.* Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 Yale J. L. & Tech. 134, 162 (2013) (discussing government's lack of candor to judges when seeking authority to use "Stingray" cell phone tracking devices).

been consulted prior to submission of the application, and the basis for the determinations made with regards to the issues above;

- Prohibit the impersonation of third parties by law enforcement agencies in their efforts to deliver malware to targets, unless those third parties provide informed consent in writing;
- Require that any assistance of a service provider in delivering the malware be consensual or explicitly required by the warrant;
- Require law enforcement malware to include identifying markings in the computer code, such that if the code is subsequently discovered by security researchers, they will know who to contact if, for example, the malware malfunctions, spreads, or ends up on the computers of non-suspects;
- Prohibit the use by law enforcement of zero-day exploits in general-use software and hardware; and
- Prohibit the approval of warrants in which there is a reasonable likelihood that execution of the warrant will result in damage to third parties who are not the intended law enforcement target.

Many of these proposed constraints are beyond this Committee's power to enact. The ACLU recommends that the Committee not adopt the proposed amendment and allow the government to seek legislation in Congress.

* * * * * * *

Thank you for your consideration of these comments.

Respectfully,

Nathan Freed Wessler
Christopher Soghoian
Alex Abdo
American Civil Liberties Union
Speech, Privacy, and Technology Project
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org