MEMORANDUM

To: Members of the Advisory Committee on Criminal Rules
From: American Civil Liberties Union
Date: April 4, 2014
Re: ACLU Comment on the Proposed Amendment to Rule 41 Concerning Remote Searches of Electronic Storage Media

---

The American Civil Liberties Union writes to offer its perspective on the proposed amendment to Rule 41 concerning remote searches of electronic storage media. The Rule 41 Subcommittee approved the proposal (over a dissenting vote) on March 12, 2014, and forwarded it to the Advisory Committee on Criminal Rules ("Advisory Committee") in a March 17, 2014, memorandum. The proposal is on the agenda for consideration at the Advisory Committee's April 7–8, 2014, public meeting.

The proposed amendment would significantly expand the government's authority to conduct remote searches of electronic storage media. Those searches raise serious Fourth Amendment questions. It would also expand the government's power to engage in computer hacking in the course of criminal investigations, including through the use of malware and other techniques that pose a risk to internet security and that raise Fourth Amendment and policy concerns. In light of these concerns, the ACLU recommends that the Advisory Committee exercise extreme caution before granting the government new authority to remotely search individuals' electronic data.

Because of the importance of these issues, the ACLU submits these initial comments in advance of the April meeting. Should the proposal be approved by the Advisory Committee and published for public comment, the ACLU expects to submit more detailed comments at that time.

I. Summary of Proposed Amendment to Rule 41

The proposed amendment, approved by the Rule 41 Subcommittee upon the recommendation of the Department of Justice ("DOJ"), would create a new exception to the territoriality requirement of Rule 41. Rule 41 currently provides that "a magistrate judge with authority in the district— or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property **located within the district**." Fed. R. Crim. P. 41(b)(1) (emphasis added). This territoriality limitation is subject to several narrow exceptions. *See id.* 41(b)(2)–(5).

The proposed amendment would add a new exception to the general rule that magistrate judges may grant warrants for searches only within their district: "(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize electronically stored information located within or outside that district." Advisory Comm. on Criminal Rules, Materials for April 7–8, 2014 Meeting 165 ("Advisory Committee Materials").[1] The proposal would also add language to Rule 41's notice requirement, providing that for remote access searches, law enforcement "must make reasonable efforts to serve a copy [of the warrant] on the person whose property was searched or whose information was seized. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person." *Id.* at 166.

The Department of Justice asserts that it needs this expanded authority for three primary reasons:

1) to enable investigators to obtain warrants where the location of the computer to be searched is unknown, including where a suspect is using anonymization tools like Tor or other proxy services to mask his or her internet protocol ("IP") address and other identifying information;

2) to enable investigators to obtain warrants to search Internet-connected computers in many districts simultaneously when those computers are being used as part of "complex criminal schemes." As an example, DOJ describes crimes involving "the surreptitious infection of multiple computers with malicious software that makes them part of a 'botnet,'" where investigating and addressing the threat posed by the botnet may involve law enforcement action in many judicial districts simultaneously; and

3) to enable investigators who obtain a warrant to search a physical computer in a particular location to also use that same warrant to search information that is accessible from that computer but stored remotely in another district, such as information stored on cloud-based services (e.g., Dropbox or Amazon Cloud Drive) or web-based email (e.g., Gmail or Yahoo! Mail).

Advisory Committee Materials 172–73, 261.

In response to DOJ's proposal, one member of the Subcommittee, Professor Orin Kerr, offered a more limited amendment, intended to provide authority to search where the location of the target computer is unknown, but not to conduct remote searches of computers or servers whose location is known or can reasonably be ascertained. Professor Kerr's proposal reads:

> (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant authorizing remote access of electronic storage media to obtain electronically stored information **if**

[1] *Available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2014-04.pdf.

the district (if any) in which the electronic storage media is located cannot reasonably be ascertained.

Advisory Committee Materials 241. The Subcommittee did not adopt this language.

II. Remote Searches of Cloud Data Pose Fourth Amendment, Statutory, and Policy Problems

Gone are the days when all or most of a person's electronic files were stored on her own computer. Increasingly, people and businesses store large amounts of data on servers owned by third-party companies that are remotely accessible via the internet.[2] This is known as "cloud" storage. Under current law, if law enforcement wishes to search data stored on the cloud it must obtain an order or warrant pursuant to the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2703.[3] A warrant issued under ECPA and Fed. R. Crim. P. 41 must demonstrate probable cause justifying search of the data held by the third-party company, and must be served on the company so that its employees may produce the requested data to the government. *See Warshak*, 631 F.3d at 288.

The government's proposed amendment would create a new mechanism for accessing cloud-based data, whereby police could obtain a warrant to search a suspect's physical computer, and then use that computer to directly access, search, and copy files stored remotely on cloud-based services. This raises significant and troubling Fourth Amendment and policy concerns, some of which were highlighted by Professor Kerr in his memoranda, and some of which have not yet been presented to the Advisory Committee:

Forum Shopping and Jurisdictional Overreach: Except in limited circumstances, magistrate judges are empowered to issue search warrants for "property located within the district" in which they serve. The proposed amendment would expand the power of magistrate judges to grant search warrants in two ways: it would permit a magistrate judge "in any district where activities related to a crime may have occurred" to issue a remote access search warrant; and it would allow such warrants to authorize searches for data or files stored "within or outside that district." These changes, taken together, create opportunities for forum shopping and raise federal jurisdictional concerns.

The phrase "in any district where activities related to a crime may have occurred" radically expands the fora in which the government can apply for a warrant. Most federal criminal investigations and prosecutions rely for their federal jurisdiction on the crime's effect

[2] *See, e.g.*, Quentin Hardy, *IBM Plans Big Spending for the Cloud*, N.Y. Times, Jan. 16, 2014, http://bits.blogs.nytimes.com/2014/01/16/ibm-plans-big-spending-for-the-cloud/; Tim Bradshaw, *Dropbox Faces Growing Competition in Cloud Storage Wars*, Fin. Times, Aug. 18, 2013, http://www.ft.com/cms/s/2/88be965e-edd8-11e2-816e-00144feabdc0.html.

[3] Under ECPA, access to certain stored content information requires a warrant. 18 U.S.C. § 2703(a); *see also United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (requiring warrant for all remotely stored email content). Other information about stored electronic communications and records, not including their content, may be obtained with a court order issued on a relevance and materiality standard. 18 U.S.C. § 2703(c)–(d).

on, relation to, or involvement in interstate commerce.[4] This means that in most federal criminal investigations law enforcement agencies will be able to identify multiple districts where "activities related to the crime may have occurred." Further, internet-enabled or -connected crimes will frequently involve conduct in multiple districts; in many cases, the government will be able to choose among dozens of districts in which to seek a warrant.

Suppose an internet fraudster sends unsolicited email to people in two dozen districts. Perhaps those emails travel through servers in another dozen districts on their way across the Internet.[5] And suppose the suspect purchased his computer from a vendor in yet another district, and uses a cloud-based email service to generate the messages, the servers of which are spread across an additional five districts. The government would apparently be able to select among any of those 42 districts in which to apply for a warrant. This raises familiar forum-shopping concerns,[6] permitting the government to choose the district in which it expects to receive the least skeptical judicial reception.

It also raises jurisdictional issues. There is at least a serious question as to whether a court in a district where a bare minimum of "activities related to a crime" occurred—or especially where activities related to a crime merely "*may* have occurred"—has authority to issue an extraterritorial warrant, especially one that authorizes searches nationwide. *See Weinberg v. United States*, 126 F.2d 1004, 1006 (2d Cir. 1942) ("[E]ven though the statute, 18 U.S.C.A. § 611, authorizing the issuance of search warrants, does not contain an express limitation of the district court's power to its own district, that seems clearly understood, in view of the constitutional provisions and the general rule of territorial limitation. We, therefore, cannot hold silence to mean that search warrants may be used anywhere in the country."). The proposed rule would be convenient to the government, but at the cost of allowing a single judge to authorize searches in multiple districts, some at great distance, likely without regard to any differences in binding circuit law at the various sites of those searches.[7] Unlike terrorism investigations (for which out-of-district search warrants are currently authorized, Fed. R. Crim. P. 41(b)(3)), remote searches of electronic storage media are likely to occur with great frequency. The proposed rule is not a minor procedural update; it is a major reorganization of judicial power.

Circumvention of ECPA: The Electronic Communications Privacy Act provides several important protections that will be evaded under the proposed amendment. First, to obtain a

---

[4] *See* 1 Wayne R. LaFave et al., Crim. Proc. § 1.2(c) (3d ed.) ("[T]he dramatic expansion of federal criminal law was based primarily on Congress' authority under the Commerce Clause . . . .").

[5] *See* World Science Festival, *There and Back Again: A Packet's Tale – How Does the Internet Work?*, YouTube (June 6, 2012), https://www.youtube.com/watch?v=WwyJGzZmBe8; Glenn Fleishman, *To Sail Data Across the Web, Computers Seek the Best Routes*, N.Y. Times, Dec. 31, 1998, http://www.nytimes.com/1998/12/31/technology/to-sail-data-across-the-web-computers-seek-the-best-routes.html.

[6] *See, e.g.*, *United States v. Bailey*, 193 F. Supp. 2d 1044, 1051 (S.D. Ohio 2002) ("Courts should uniformly discourage forum shopping or judge selection."); *see also* Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 Miss. L.J. 85, 102 (2005).

[7] For example, the Sixth Circuit is the only court of appeals to have definitively ruled that there is a reasonable expectation of privacy in the contents of email communications stored on an email provider's servers. *Warshak*, 631 F.3d at 288. The Ninth Circuit has explained the need for particularly robust procedures for regulating computer searches. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1175–77 (9th Cir. 2010). What happens when a magistrate judge in Louisiana authorizes remote searches within the Sixth, Ninth, and other circuits that violate some circuits' law but not others? When a suppression motion is brought, whose law governs?

warrant for stored content (as opposed to non-content information) under ECPA, the government must demonstrate probable cause as to evidence held by each service provider whose data it seeks to search. The proposed amendment would permit the government to make a single showing of probable cause—that evidence of the crime will be found on a physical computer and any cloud services to which it is connected—and then use that showing to search as many cloud storage accounts as can be accessed from the computer. Thus, a single warrant could result in police searching a suspect's computer hard drive, and then embarking on a fishing expedition through her work emails stored on her employer's email server, her personal emails on Gmail or Outlook, her word processing files stored on Dropbox, her vacation photos on Flickr, her private conversations with family members on Facebook, and a log of her personal budget and purchases on Mint.com. Unless police know what cloud-based services a person uses before searching her computer, they will be unlikely to demonstrate probable cause as to each one when applying for a remote access warrant. A warrant granting blanket authority to search any and all of these services—without even knowing which ones a suspect uses or which can be easily accessed from her computer—would raise particularity problems as well.

Second, under ECPA the government must serve a warrant on each service provider, thus providing them with notice that their servers will be searched. This allows the companies to protect both their own legal interests and those of their customers. Service providers are able to subject warrants to scrutiny, and to challenge the government if a warrant seeks information that appears too broad in scope, too vaguely defined, or is otherwise deficient.[8] Given the vast quantities of data stored on cloud services, much of which will be irrelevant to most investigations, these protections are an important aspect of ensuring compliance with the Fourth Amendment. Most individuals served with a search warrant lack the legal expertise or institutional clout to challenge the terms of the warrant before its execution.[9] And for delayed notice searches, no challenge is even theoretically possible.

Finally, the government asserts that the proposed amendment is needed to prevent cloud-stored documents from being deleted or encrypted after a physical computer is searched but before the government can obtain an ECPA warrant directed at the cloud storage provider.[10] This problem can be avoided with the simple expedient of a preservation request directed at the provider. 18 U.S.C. § 2703(f). Such requests can be sent immediately and unilaterally by law

---

[8] *See* Google, *Way of a Warrant* , YouTube (Mar. 17, 2014), https://www.youtube.com/watch?v=MeKKHxcJfh0 (explaining that Google employees scrutinize warrants to catch errors and identify overly vague or broad requests, and that they ask investigators to narrow the scope of warrants when appropriate); Google, Transparency Report, Requests for User Information, Legal Process, http://www.google.com/transparencyreport/userdatarequests/legalprocess/#what_types_of_legal ("If we believe a request is overly broad, we'll seek to narrow it."). *See also Permanent Provisions of the Patriot Act: Hearing Before the Subcomm. On Crime, Terrorism & Homeland Sec. of the H. Comm. on the Judiciary* 112th Cong. 69 (2011) (statement of Todd M. Hinnen, Acting Assistant Attorney Gen. for Nat'l Sec.), *available at* http://judiciary.house.gov/_files/hearings/printers/112th/112-15_65486.PDF (after congressman asks Acting Assistant AG Hinnen "why would [a service provider] . . . have an incentive to hire lawyers to protect [their subscribers' privacy] rights?," Mr. Hinnen responded that "telecommunication providers and Internet service providers take the privacy of their customers and subscribers very seriously and I think are often an effective proxy for defending those rights").

[9] This is not to say that only service providers should receive notice. Rather, notice to both service providers *and* users is crucial to protect Fourth Amendment rights.

[10] Advisory Committee Materials 261.

enforcement, without the need to seek judicial approval, and require providers to preserve relevant records and evidence pending issuance of a warrant. The government ignores this power in arguing that ECPA warrants are insufficient.

Use of a Single Warrant to Search Multiple Locations Owned or Controlled by Other Parties: The proposed amendment would allow police to remotely search multiple hard drives, servers, and web-based accounts under a single warrant, without reason to believe that all locations to be searched are under the investigative target's exclusive control. Courts are particularly skeptical of warrants authorizing searches of multiple locations not owned by the same person.[11] This skepticism is partly animated by the concern that the use of multiple-location search warrants could divest one or another occupant of individually held Fourth Amendment rights. 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."[12] The same concerns and rules should apply when police search digital "occupancies."

Remote access searches can raise concerns about joint and divided ownership in several ways. First, physical computers may be shared, but may provide access to remotely stored data that is not. For example, all members of a family might use the same desktop computer. But the cloud storage accounts directly accessible from it might belong exclusively to different people: the Dropbox account might be registered to one family member, the Facebook account to another, the Flickr photo archiving account to a third, and the Yahoo! email account to a fourth. A warrant authorizing a search for evidence of one family member's crime, but permitting access to any remote data accessible through the suspect's shared computer, would result in searches of other people's digital data without probable cause.

Second, remote storage accounts may themselves be shared. A wife and husband may share a joint cloud-based email account; artists or entrepreneurs collaborating on a project may share a cloud storage account to facilitate their joint work. Courts recognize the reasonable expectation of privacy individuals may have in shared places, and doctrines of standing and consent accommodate different interests in the use, possession, and ownership of jointly controlled property.[13]

---

[11] "[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)).

[12] 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).

[13] *See, e.g.*, *State v. Lacey*, 204 P.3d 1192, 1205–06 (Mont. 2009) (discussing scope of third-party consent to search shared computer); *United States v. Elliott*, 50 F.3d 180, 186 (2d Cir. 1995) (discussing scope of landlord consent to searches of leased and unleased units).

Third, a service provider will be the owner or lessee of the servers on which a user's data is remotely stored, and may have rights to access accounts and files for some purposes and not others. *See Warshak*, 631 F.3d at 287 (discussing email service provider's limited right to access user's email account). A remote access search not involving notice to the service provider or a specific showing of probable cause may violate the provider's rights.

In order to avoid authorizing searches that violate third parties' Fourth Amendment rights, magistrate judges must determine whether a suspect's linked Gmail, Google Docs, and Google+ accounts are under another person or entity's exclusive or shared use or control. In many circumstances, however, magistrate judges will not be capable of evaluating digital "occupancy" based on the information provided by the government, because the government will not yet have accessed the computer from which it will learn about the existence and nature of remote storage accounts. Authorizing the use of a single search warrant to gain access to multiple computers or online accounts in this circumstance could infringe on individuals' substantive Fourth Amendment rights. As the number of files and locations subject to a single search warrant increases, so too does the probability that privacy rights of people other than the target of the search will be affected.

Particularity Concerns: Although the proposed Committee Note seeks to avoid consideration of the amendment's interaction with the Fourth Amendment's particularity requirement, that issue should be addressed now because the particularity problems likely to be raised by remote access search warrants are entirely predictable. Law enforcement agents may not, and in many cases will not, know ahead of time which cloud services a suspect uses, so warrants will be sought for authority to search any cloud storage service to which the computer is connected. Such authority has little analogue in the context of physical searches. It would be akin to a warrant authorizing the search of a particular house, and also any other building that can be accessed using keys found in the house. Without describing with particularity the places to be searched and demonstrating probable cause as to each one, remote access warrants will violate the Fourth Amendment.

Moreover, some kinds of cloud storage services might be incapable of holding evidence of the crime under investigation. A photo account on Flickr or Picasa is unlikely to contain a spreadsheet proving tax fraud. A remote music storage service will not likely contain evidence of purse snatching. But without knowing ahead of time which cloud services a person uses and which are accessible from their computer, the government cannot describe with particularity the places to be searched, nor can it provide probable cause as to each service. A blanket authority to search "any remote storage services likely to contain evidence of the crime" cannot solve these problems because it would not meaningfully cabin an officer's discretion. A warrant application must describe, and a warrant must specify, the places to be searched. Given the tremendous storage capacity of cloud storage services—more like a warehouse than a filing cabinet or home library[14]—the failure to appropriately limit remote access warrants will result in unconstitutional searches of staggering quantities of data.

[14] One gigabyte of data is, on average, the equivalent of 64,782 pages of Microsoft Word documents. LexisNexis Discovery Services, How Many Pages in a Gigabyte? (2007), http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitepapers/adi_fs_pagesinagigabyte.pdf. Dropbox currently offers accounts with 100 gigabytes of storage space for $9.99 per month. Dropbox, Choose Your Dropbox

First Amendment: Authorizing a new, expansive power to search through an individual's private email correspondences, Facebook messages, and Flickr or Dropbox accounts also raises profound First Amendment concerns. Individuals have a right to engage in expressive and associational activities in private, and government intrusions into that privacy trigger heightened scrutiny.

Electronic diaries stored on the cloud, lists of books ordered from Amazon.com, and a multitude of other remotely stored information can reveal an individual's secret thoughts, hopes, and fears. To access these private, protected records, the government must demonstrate a compelling need to obtain the material, and a substantial relationship between the investigation and the information it seeks.[15]

Private social networking information, such as from Facebook and Google+, can also disclose an individual's most significant private relationships—political, personal, or intimate—and the nature and intensity of those relationships. The First Amendment protects these associations from compelled disclosure, both because they are necessary to other associational and expressive activities and as an end in themselves.[16]

Technological improvements will continue to expand the already vast quantities of expressive and associational information that can be stored in the cloud. The proposed amendments will increase the risk of abuses and the chilling of First Amendment-protected activities.

Remote Access Searches Can Implicate the Privacy Rights of Many Innocent Third Parties: Electronic storage media remotely accessible from a physical computer are not limited to cloud storage accounts containing just a suspect's files. In many cases, remotely accessible servers will contain sensitive data about or belonging to numerous other persons as well. For example, a doctor's home computer may be connected to her patient files stored electronically on a remote server.[17] Patients have a reasonable expectation of privacy in those files,[18] and in most

---

Plan, https://www.dropbox.com/pricing. At the equivalent of 6,478,200 printed pages, this would fill more than 430 meters of shelf space. *See* Lynn Neary, *Printing Wikipedia Would Take 1 Million Pages, But That's Sort of the Point*, Nat'l Pub. Radio, Mar. 30, 2014, http://www.npr.org/blogs/alltechconsidered/2014/03/27/295262783/printing-wikipedia-would-take-1-million-pages-but-thats-sort-of-the-point.

[15] *See, e.g.*, *In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461 et seq.*, 706 F. Supp. 2d 11, 17 (D.D.C. 2009) (quashing subpoena for company records regarding sexually expressive films because customers' "right to receive ideas" outweighed prosecutorial interests); *see also Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 546 (1963) ("[I]t is an essential prerequisite to the validity of an investigation which intrudes into the area of constitutionally protected rights of speech, press, association and petition that the State convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest.").

[16] *See NAACP v. Alabama ex. rel. Patterson*, 357 U.S. 449, 462 (1958) (observing that the "inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs"); *Griswold v. Connecticut*, 381 U.S. 479, 484, 486 (1965).

[17] *See, e.g.*, Press Release, U.S. Dep't of Health & Human Servs., Doctors and Hospitals' Use of Health IT More than Doubles Since 2012 (May 22, 2013), http://www.hhs.gov/news/press/2013pres/05/20130522a.html ("HHS has met and exceeded its goal for 50 percent of doctor offices and 80 percent of eligible hospitals to have [electronic health records] by the end of 2013.").

states they are protected by privilege.[19] Searches of computers owned by lawyers, mental health professionals, and accountants would raise similar concerns. Likewise, a system administrator for a company's cloud-based email and file storage systems may have administrator credentials and login information for the accounts of every employee, including sensitive, private, and perhaps privileged data. Prior to the advent of widespread and large-capacity remote storage, these sensitive files would have been kept at an office or other secure physical storage location, and would have required a separate showing of probable cause and separate warrant to search. The ease with which remote searches can implicate these private third-party files creates new and difficult problems.

III. Zero-Day Exploits and Malware

The proposed amendment would enable the government to use sophisticated remote hacking techniques—malware and so-called "zero-day" exploits—to identify and search computers that are using anonymization tools like the Tor network. Such techniques could also be used to collect private information from computers whose location is known. These techniques are technically complex, and raise significant policy and Fourth Amendment concerns. Their expanded use should not lightly be authorized.

A. Technical Description of Malware and Zero-Day Exploits

Government agencies seeking to "remotely search" a computer or mobile phone are seeking information that is neither published online, nor otherwise available to a member of the public.[20] In order to extract such information from a computer that they neither control nor have physical access to, they must deliver specific computer code to the device and cause that code to run.

In some cases, it may be possible to use trickery (a technique that security researchers generally refer to as "social engineering") in order to get the owner or operator of the computer to take an action that will cause this code to run. For example, law enforcement agents may send an email to a target with an attachment that looks to be an image file, but is in fact a specially designed program ("malware") that will covertly install itself on the target's computer and then collect data.[21]

---

[18] *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001); *Or. Prescription Drug Monitoring Program v. U.S. Drug Enforcement Admin.* ("*Oregon PDMP*"), No. 3:12-CV-02023-HA, 2014 WL 562938, at *7 (D. Or. Feb. 11, 2014).

[19] *See, e.g.*, Cal. Evid. Code §§ 900–1007; Fla. Stat. Ann. § 456.057.

[20] If the information were available online, or could be obtained by any member of the public without exceeding authorized access to a computer, the government would not need a search warrant.

[21] "The malware appears on a victim's desktop as 'exe.Rajab1.jpg' (for example), along with the default Windows icon for a picture file without thumbnail. But, when the UTF-8 based filename is displayed in ANSI, the name is displayed as 'gpj.1bajaR.exe'. Believing that they are opening a harmless '.jpg', victims are instead tricked into running an executable '.exe' file. Upon execution these files install a multi-featured trojan on the victim's computer. This malware provides the attacker with clandestine remote access to the victim's machine as well as comprehensive data harvesting and exfiltration capabilities." Morgan Marquis-Boire, From Bahrain with Love: FinFisher's Spy Kit Exposed? 3 (2012), *available at* https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/ (describing the method of infection of surveillance software used by the Bahraini government against activists).

U.S. law enforcement agencies are not the only actors seeking to use social engineering to deliver malicious software onto people's computers. This technique is also widely used by criminals and foreign governments, who have used it to hack into the computers of U.S. government agencies, consumers, and major U.S. companies, including Microsoft,[22] RSA,[23] Apple, and Amazon.[24] It is for this very reason that cyber security education efforts stress the importance of not clicking on unknown email attachments or suspicious-looking links.[25]

Social engineering will not always work, particularly against targets that are following prudent cyber security warnings about email attachments and suspicious web links. In such cases, law enforcement agencies seeking to install or execute surveillance software on the computers of targets will need to use an alternate delivery technique that does not require the user to install or execute the code.[26]

It is possible to run code on a computer or mobile device without the knowledge or assistance of the person operating that device. However, this generally requires the exploitation of security vulnerabilities in the software running on that device. For example, by exploiting vulnerabilities in a web browser, it is possible to cause a computer to download and install software when it visits a website,[27] without requiring that the target take any additional actions.

---

[22] *See* Tom Warren, *Microsoft Confirms Syrian Electronic Army Hacked into Employee Email Accounts*, The Verge (Jan. 15, 2009), http://www.theverge.com/2014/1/15/5312798/microsoft-email-accounts-hacked-syrian-electronic-army (describing a successful social engineering attack in which the Syrian Electronic Army was able to extract sensitive law enforcement surveillance documents from Microsoft employees).

[23] Riva Richmond, *The RSA Hack: How They Did It*, N.Y. Times (Apr. 2, 2011), http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/.

[24] Mat Honan, *How Apple and Amazon Security Flaws Led to My Epic Hacking*, Wired (Aug. 6, 2012), http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/.

[25] *See* Dep't of Homeland Sec., Cyber Tips for Older Americans, http://www.dhs.gov/sites/default/files/publications/Cybersecurity%20for%20Older%20Americans_0.pdf; New York Governor's Office of Employee Relations, Personal Security Responsibilities, http://www.goer.ny.gov/training_development/resources/hipaa/helpFiles/PersonalSecurityResponsibilities.htm ("Do not open attachments from the Internet or from people you do not know. Do not open any suspicious attachments."); Univ. of Va. at Wise, Policies & Security: Secure Computing Notices, http://www.wise.virginia.edu/oit/SecureComputing/notices ("Do NOT click on web address links included in email messages unless you are sure they connect to trusted web sites. It is safer to either key a known web site address directly into the address line in your browser or to use the search feature of your browser to find the website.").

[26] *See Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. On Crime, Terrorism & Homeland Sec. of the H. Comm. on the Judiciary* 112th Cong. (2011) (statement of Valerie Caproni, General Counsel, FBI), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg64581/html/CHRG-112hhrg64581.htm ("There will always be criminals, terrorists, and spies who use very sophisticated means of communications that are going to create very specific problems for law enforcement. We understand that there are times when you need to design an individual solution for an individual target, and that is what those targets present.").

[27] This website must be under the control of the attacker, or, if the attacker is able to monitor the internet connection of the target, any website that the target visits can be used to initiate a "drive by" installation. *See* Gamma Group, Remote Monitoring & Infection Solutions: FINFLY ISP (Wikileaks.org), https://wikileaks.org/spyfiles/files/0/297_GAMMA-201110-FinFly_ISP.pdf (product brochure for a government-grade surveillance appliance which can "be integrated into an ISP's Access and/or Core Network to remotely install the Remote Monitoring Solution on selected Target Systems. . . . FinFly ISP is able to infect Files that are downloaded by the Target on-the-fly or infect the Target by sending fake Software Updates for popular Software. The new release now integrates Gamma's powerful remote infection application FinFly Web to infect Targets on-the-fly by just visiting any website.").

This technique is known generally as a "drive by download,"[28] and is a technique that is used by hackers, criminals, and governments (in the United States and elsewhere) to deliver malware.[29]

In order to exploit a security vulnerability in the software on a target's computer, that computer must either be running out-of-date software with a known software vulnerability, or the hacker must know of a vulnerability for which no update exists. As such, targets who regularly patch their software (or use software that automatically updates) may be much harder to compromise with malware. In order to hack into such targets, law enforcement and intelligence agencies are increasingly seeking to purchase or discover so called zero-day (or 0-day) software exploits,[30] that is, special software that exploits vulnerabilities in software that are not known to the manufacturer of the software program, and thus, for which no software update exists. Zero-day exploits are extremely valuable, because there is no defense against them.[31]

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.[32] This has in turn fueled a largely unregulated market for zero-day exploits, in which government agencies are active and are often the highest bidder.[33]

---

[28] *See* Long Lu et al., *BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections*, Proceedings of the 17th ACM Conference on Computer and Communications Security (Oct. 2010), *available at* http://www.blade-defender.net/BLADE-ACM-CCS-2010.pdf ("Web-based surreptitious malware infections (i.e., drive-by downloads) have become the primary method used to deliver malicious software onto computers across the Internet.").

[29] *See* Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired (Sept. 13, 2013, 4:17 PM), http://www.wired.com/2013/09/freedom-hosting-fbi/; Dan Goodin, *Attackers Wield Firefox Exploit to Uncloak Anonymous Tor Users*, ArsTechnica (Aug. 5, 2013, 1:02 PM), http://arstechnica.com/security/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users/ ("A piece of malicious JavaScript was found embedded in webpages delivered by Freedom Hosting, a provider of 'hidden services' that are available only to people surfing anonymously through Tor. The attack code exploited a memory-management vulnerability, forcing Firefox to send a unique identifier to a third-party server using a public IP address that can be linked back to the person's ISP.").

[30] *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 (Oct. 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.").

[31] *The Digital Arms Trade*, Econ., 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.").

[32] *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 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.

[33] *See, e.g.*, *The Digital Arms Trade*, The Economist, Mar. 30, 2013, http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-

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 exploits can be in the hundreds of thousands of dollars, or, in some cases, up to a million dollars.[34] 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.[35] Quite simply, governments that rely on zero-day exploits have prioritized offense over defense.

B. Concerns Raised by Use of Zero-Day Exploits and Malware

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.[36] Several senior ex-U.S. government officials have acknowledged these risks, including ex-NSA/CIA director Michael Hayden,[37] and ex-'cyber czars' Howard Schmidt[38] and Richard Clarke.[39]

---

digital-arms-trade ("Other reputable customers, such as Western intelligence agencies, often pay higher prices. Mr Lindelauf reckons that America's spies spend the most on exploits. Vupen and other exploit vendors decline to name their clients. However, brisk 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.").

[34] *See* 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 (describing hackers searching for "secret flaws in computer code that governments pay hundreds of thousands of dollars to learn about and exploit").

[35] 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.").

[36] *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.").

[37] *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.'").

[38] *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, *supra* note 1

Indeed, at a time when cyberattacks are, according to government officials, one of the biggest threats faced by this country,[40] the collateral damage associated with exploiting, rather than fixing, security vulnerabilities is the topic of considerable debate. For example, the President's NSA Review Group recently observed that "[a] vulnerability that can be exploited on the battlefield can also be exploited elsewhere"[41] 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."[42] 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."[43]

These issues are complicated and serious, and they raise both policy and constitutional concerns. Under the Fourth Amendment, use of zero-day exploits 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. Surgically removing evidence from a suspect's body,[44] using a powerful motorized battering ram to break into a residence,[45] and

---

("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.'").

[39] Menn, *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.'").

[40] 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, March 12, 2013, http://www.defense.gov/news/newsarticle.aspx?id=119500. *See also* Greg Miller, *FBI Director Warns of Cyberattacks; Other Security Chiefs Say Terrorism Threat Has Altered*, Wash. Post, November 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.").

[41] 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.

[42] *Id.* at 37, 219 ("We recommend that the National Security Council staff should manage an interagency process to review on a regular basis the activities of the US Government regarding attacks that exploit a previously unknown vulnerability in a computer application or system. These are often called "Zero Day" attacks because developers have had zero days to address and patch the vulnerability. 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. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments.").

[43] *Id.* at 220.

[44] *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

"employ[ing] a flashbang device [to enter a house] with full knowledge that it will 'likely' ignite accelerants and cause a fire"[46] 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.[47] These factors are relevant to individual warrant applications, but also to the Advisory Committee's consideration of the proposed Rule amendment.

The issues described above 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. At a minimum, however, this Committee should seek comment from technical experts and from government agencies responsible for domestic cybersecurity, including the Federal Trade Commission and the Department of Homeland Security. The power the government seeks is weighty and risky, and this Committee's consideration of the proposed amendment should proceed with due deliberation and care.

IV. Botnets

The government seeks authority to obtain warrants authorizing simultaneous remote access searches of hundreds or thousands of computers that have, unbeknownst to their owners, been enlisted into a botnet and used for allegedly criminal purposes. The ACLU is sympathetic to the goal of disabling botnets and strengthening the security of the Internet, but that goal can be accomplished with a far more modest modification of Rule 41. If the government is acting primarily in a cybersecurity capacity (analogous to the government's public health function[48]), rather than in a primarily law enforcement capacity, then Fourth Amendment concerns are less acute. *See Illinois v. Lidster*, 540 U.S. 419, 423 (2004) (discussing special needs doctrine). But if the government is engaged in searches of computers for "general 'crime control' purposes," *id.*, Fourth Amendment concerns are at their zenith.

Even to the extent the government seeks to use remote access warrants only to disable botnets by identifying the command and control structure of the network and then distributing computer code that disinfects the controlled computers, there are still concerns. The techniques the government uses to disable the botnet matter. If the government wants authority to distribute

---

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).

[45] *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").

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

[47] 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/.

[48] *See* Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity* 10–14 (2011), *available at* http://www.cs.cornell.edu/fbs/publications/publicCYbersecDaed.pdf.

computer code to infected computers via remote access, it needs to specify to the magistrate judge the capabilities of that code, how it will be delivered, the risk of interception en route, and the risks of causing new damage. Only full disclosure of this type of information will enable a judge to accurately assess the likely effect of the technique on the rights of those whose computers will be targeted and others. The government also needs to propose, and judges need to adopt, robust minimization and notice procedures to mitigate the effects on innocent parties' privacy interests.

Other concerns are common to both law enforcement and cybersecurity activities. The government wants to be able to send to many hundreds or thousands of computers "remote network techniques" that will report back those computers' IP addresses, MAC addresses, and other unique identifiers. The government must explain whether it can be sure that the techniques will not target or search computers that are not part of the botnet. It must also explain in more detail the nature of the "unique identifiers" it seeks to collect. A computer may contain numerous pieces of data that constitute "unique identifiers," and the particularity and reasonableness requirements of the Fourth Amendment require that the information collected be precisely described and limited in scope. Further, an authorization to search thousands of computers to collect information from a large number of people may verge on a general warrant. The use of extra-district remote access warrants to investigate and combat botnets raises numerous questions that the government has not yet answered.

V. 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. 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). The proposed language clearly contemplates searches for which no notice can be provided. 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 v. New York*, 388 U.S. 41, 60 (1967)). 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."). 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.

A second problem with the proposed amendment is that it will allow the government to provide notice to third-party service providers rather than to the actual target of the search in many cases, which all but defeats the purpose of the notice. Notice should be given to both.[49] The proposed language provides that "the officer must make reasonable efforts to serve a copy on the person whose property was searched **or** whose information was seized." (Emphasis added). A reasonable interpretation of this language would allow the government to choose between providing notice to the third-party cloud storage provider (whose physical server was searched) *or* to the person whose information was seized. Service providers may fail to, or be ordered not to, provide their own notice to 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, as explained by Professor Kerr, the proposed amendment will likely result in more delayed-notice searches.[50] 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.

VI. Professor Kerr's Counter-Proposal Does Not Address All of the ACLU's Concerns

Professor Kerr proposes to allow remote access warrants only when "the district (if any) in which the electronic storage media is located cannot reasonably be ascertained." Although this narrows the scope of the government's remote search authority in a way that avoids some of the above concerns, it still poses problems. For example, under Professor Kerr's language, the government would still be able to obtain warrants to use malware, zero-day exploits, and other techniques that raise serious constitutional and policy questions.

Additionally, Professor Kerr's proposal can be interpreted to allow remote access searches of data stored on the cloud, even when the identity of the cloud service containing the data is known. This is because for many cloud storage services it is impossible to know where the data is physically located (in other words, on what server it resides). Many cloud storage providers distribute their servers among multiple locations, both within the United States and around the world. A digital file might be stored on any one of those servers, split up between servers, or redundantly stored on multiple servers simultaneously. A file stored on one server in California today might be automatically transferred to another server in North Carolina tomorrow. The storage location will be dictated by features of the provider's network architecture, the usage patterns and comparative loads on its servers, and other factors that are

[49] Although providing notice to the service provider is important (and compelled by ECPA and Rule 41, *see Application for Warrant for E-mail Account [redacted]@gmail.com Maintained on Computer Servers Operated by Google, Inc., Headquartered at 1600 Amphitheatre Parkway, Mountain View, CA*, No. 10-291-M-01, slip op. (D.D.C. Sept. 20, 2010), *available at* http://www.crowell.com/files/Lamberth-Opinion.pdf), it is not sufficient. Notice must be provided to the target of the search as well.

[50] Advisory Committee Materials 252.

both out of the control of users and unknowable to them. Providers do not typically disclose the physical location of the server on which any given file resides. The location of the server housing the data is likewise unknown, and probably unknowable, to law enforcement. Therefore, the district in which the electronic storage media is located cannot be reasonably ascertained, and a remote access warrant instead of an ECPA warrant could be used to conduct the search, with all of the attendant consequences described above.

VII. The Advisory Committee Should Fully Consider All the Implications of the Proposed Amendment Now, and Should Be Skeptical of its Wide Reach

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 Fourth Amendment, statutory, and policy questions.

A. The Proposed Amendment Expands the Government's Substantive Powers, and the Advisory Committee Should Grapple With Its Fourth Amendment Implications Now

The Federal Rules are limited to "regulat[ing] procedure." *Sibbach v. Wilson & Co.*, 312 U.S. 1, 13 (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,[51] in practice the amendment will enlarge the government's substantive power to conduct searches. By radically expanding the circumstances in which a magistrate judge may approve a warrant to search and seize data on computers and servers located in distant districts, including searches using malware and other hacking techniques, the proposed amendment risks abridging Fourth Amendment rights and frustrating the purposes of ECPA.

But 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,'"[52] 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 structure of ECPA. In order to prevent violations of the Fourth Amendment and an untoward expansion of government power, this Committee should grapple with these issues now. Alternatively, 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.

[51] Advisory Committee Materials 166.

[52] *Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 407 (2010) (second and third alterations in original).

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. 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.[53] 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 likely been seeking warrants to authorize remote access searches with some frequency,[54] there is only one published opinion of a magistrate judge grappling with the Fourth Amendment issues involved. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). 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.[55] 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.

---

[53] *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).

[54] *Id.*

[55] *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.").

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.[56] 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). 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, qualified immunity will likely apply. 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.

B. The Advisory Committee Should Account for the Government's Lack of Candor About the Scope and Invasiveness of its Remote Access Searches

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,[57] in warrant applications actually filed in federal court,[58] 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"[59] or "remote network techniques"[60] would put a magistrate judge (or, for that matter, a member of this Committee) on notice that the government seeks to conduct its searches using techniques that pose a serious risk

[56] *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 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 Los Angeles v. Lyons*, 461 U.S. 95 (1983).

[57] *See* Advisory Committee Materials 181–235.

[58] *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).

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

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

to cybersecurity, and that may fail the reasonableness and particularity requirements of the Fourth Amendment.[61]

The government also does not provide detailed explanation of the remote searches of data stored on cloud-based services that it seeks to conduct using warrants authorizing physical searches of computers connected to the cloud. The government does not describe the almost incomprehensibly large storage capacity of many cloud-based services, the vast amount of personal information now stored on the cloud, or the dizzying array of cloud storage services to which a computer may be connected. This information is crucial to assessing whether a warrant is appropriately limited to permit access only to cloud services as to which there is probable cause, and whether the warrant describes the locations to be searched with particularity.

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.[62] The Advisory Committee should not authorize new search powers without ensuring that the duty of candor has been and will be satisfied.

C. Expanding the Government's Remote Access Search Powers Based on Consideration of Current Technology Will Result in Increasingly More Invasive Searches as Technology Advances

If adopted, the proposed amendment will provide authority for the government to conduct remote access electronic searches for years to come. Over the coming decades, electronic storage systems will become ever more interconnected. Interconnectivity of cloud storage will likely increase at a rapid rate, and will proceed in ways that we cannot now accurately predict. This raises the specter of the authority enacted today for one purpose inadvertently enabling future searches that are considerably more invasive than anything the Advisory Committee, or even the government, now envisions.

Ten years ago, few people could have predicted the ubiquity of cloud storage, the widespread reliance on internet-connected mobile devices, or the substantial portion of people's personal and professional lives that has migrated online. It is similarly difficult to predict technological developments five or ten years from now. We are likely to see new forms of cloud storage and new linkages between cloud storage systems, giving remote access searches increasingly invasive potential. Companies are designing and marketing new types of internet-

---

[61] *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.").

[62] *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).

connected devices, from smoke detectors,[63] to "nanny cams,"[64] to televisions and refrigerators.[65] According to one estimate, "up to 200 billion devices—from games consoles to thermostats—will be hooked up to the Internet by 2020."[66] Granting the government the power to hack remotely into these devices, thus gaining a view inside people's most private spaces, is constitutionally suspect. Any amendment adopted today must account for short- and long-term changes in the nature and magnitude of cloud storage and internet connectivity, and must adequately protect Americans' rights over the coming years.

* * * * * * *

Thank you for your consideration of these comments.

Respectfully,

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

[63] *See* Rory Carroll, *Google Buys Nest Labs for $3.2bn in Bid for Smart Home-Devices Market*, Guardian, Jan. 14, 2014, http://www.theguardian.com/technology/2014/jan/13/google-nest-labs-3bn-bid-smart-home-devices-market.
[64] *E.g.*, NetGear VueZone, Nanny Cam, http://www.vuezone.com/use-ideas/nanny-cam.
[65] Gary Davis, *Smart TVs, Refrigerators Used in Internet-of-Things Cyberattack*, McAfee Blog Central, Jan. 22, 2014, https://blogs.mcafee.com/consumer/internet-of-things-cyberattack.
[66] David Nield, *Thousands of Smart Gadgets Hacked to Send out Spam Email*, Digital Trends, Jan. 18, 2014, http://www.digitaltrends.com/computing/thousands-smart-gadgets-hacked-send-spam-email.