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*

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

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),

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, u(f)-5.50 Td [(f)9.7(o4(s)5.dD.8(l)-17.2(y ( )Tbt157Tw (Sw.1(,)-9(mg717.2(3a)-4.1(t)Sw.(na)-7.8(l)-5.1(Tw 11(r)-Q9-5.1

malicious software back to the target instead.

In this step, agents deliver the government’s surveill

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). S

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 g8n ( )T..bnn me ta 410(s)9(-2.b)2(2(o)10(t)-1(g)1 9(-2.b)2(a(c)-6(c)-(k)1 b)2((he)6(c)-2(o)
ns(Fc)a.9(3.w(an.12((ct)3)t,5)6(ed16 4e)6(k)i)a9(b b)912(i) Tc 0.01 Tw [(ot)3-28.24 Td 4(r)(o)b10(t)k.

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.

.34DC 6775 0.62(to)14(-)24(0d(4DC 48 T2971 15 Td451 Tc 0.204 Tw 0.25 04 15 293)Ti -06.)l)5(e)646(e)flTJ 0)12(i-)10oeS(to

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

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

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 mechanism3(')-7(s)9(o)10(pe)-6(t)-24S1(o)8s o FB

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

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 exploitsyy8(e)4(Fw [(zw [(r)3 Tc 0 Tw 12 1)5e(e)10Ti Tw

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.w0.2 0 T0.2 576Td [Tm10 Tw D.o

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

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 reas06 Tw [(G)2(r)-1(oh T2g.(t)3(at)(or)cTw 22.]540)10(

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. T

are likely to be ill-equipped to provide robust review of applications for remote access warrants without adversarial briefing

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 investigatgnv Ac h1B

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.

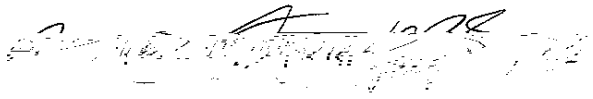
been consulted prior to submission of the application, and the basis for the determinations made with regards to the issues above;
Prohibit the impersonation of third parties by law enforcement agencies in their efforts to deliver malware to targets, unless those third parties provide informed consent 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