Comments on Proposed Remote Search Rules

Steven M. Bellovin
Columbia University*

Matt Blaze
University of Pennsylvania*

Susan Landau
Worcester Polytechnic Institute*

Thank you for the opportunity to submit comments on the proposed amendments to the Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure[1] rules for remote search. We are focusing our comments on the suggested changes to Rule 41, and in particular to the discussion of remote search. While we do not oppose the concept in principle, it poses a number of very serious concerns that must be resolved first. Above all, it should be the subject of sustained public discussion, and should most likely be authorized by specific legislation.

The three of us are technologists, and we address the topic initially from a technological perspective. We note, however, that our research has long focused on the intersection between technology and public policy. We have previously published law review articles, including one paper relevant to this discussion.[2] The issues we discuss include jurisdiction, chain of custody and authenticity of evidence, specificity of search, and notice.

Searches of Victim Computers

Botnets, a collection of compromised computers that are controlled by a "command-and-control" system, pose a complex challenge to law enforcement. First, they are large; they can range in size from several thousand to well over a million "bots," the name for victims' machines that have been taken over to perform tasks determined by the "botmaster," or command-and-control system. The challenge is two-fold: a botnet can be very large, and the machines taken over are *victims'* devices.

It is precisely the multiplicity of the victims that encourages law enforcement to seek a single warrant approach, but this approach must be avoided. It is legally and technically dangerous to use a "common scheme to infect the victim computers with malware."[3]

From a technical standpoint, the danger is that such a common scheme may easily go out of control. Current botnet technology is simple: the malware is virtually the same on all victims' machines, and thus it is easy to know where to find out and how to disable it. *There is no technical reason why, in future, botnet malware may not be far more sophisticated.* In particular, botnet malware could be configured in a multiple of different ways that would not necessarily be easily predictable. What this means is that the "common scheme to infect the victim computers with malware" may fail, and not simply fail by not working. Such a scheme could easily fail by damaging the victims computers in unpredictable and unexpected ways. As we know from such examples as Stuxnet, malware downloaded on victims' machines must be carefully tailored

*Affiliation listed for identification purposes only.

[1] Committee on Rules of Practice and Procedure of the Judicial Conference of the United States. *Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure*. Aug. 2014. URL: `http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf` (henceforth cited as Preliminary Draft).

[2] *See* Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet". In: *Northwestern Journal of Technology & Intellectual Property* 12.1 (2014). URL: `http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1/`.

[3] *See Preliminary Draft* at 325.

to the device.[4] This is both to prevent the malware from damaging other parts of the victims computer (important for the uses being prescribed in the change to Rule 41) and also to prevent the malware from causing damage should it escape the victim's computer.

From a legal standpoint, the lack of specificity is highly problematic. As noted in the paragraph above, currently botnet command-and-control malware is typically found in only a few places on a victim's machine. *There is no theoretical reason why this should be so.* What that means is that a technically sophisticated criminal could hide data in victims' machines in different places on their machines. If furthermore, the botnet information were to be encrypted—*and thus not visible in plain sight*—the resulting search would be essentially indistinguishable from a general warrant.

For these two sets of reasons, we strongly urge you to reject the multiple-victims-one-search-warrant approach, which we find exceedingly dangerous.

Location and Jurisdiction

One very crucial issue is the location of the target computer and hence jurisdiction. Apart from the legal issue of determining from which judicial district a valid warrant may be issued,finding the location of an arbitrary computer is not an easy task, even if its IP address is known.[5]

This is a serious concern. This must be addressed because of the uncertainty caused by *In re Warrant*.[6]

There are certainly times when ascertaining location is extremely difficult or impossible. Tor ("The Onion Router") is designed to provide strong guarantees of anonymity; finding Tor nodes without remote search is difficult at best.[7] Open standards and procedures for making location determination are essential. The proposed rule is problematic, though. (b)(6)(A) provides that any magistrate in a district affected may issue a warrant if "the district where the media or information is located has been concealed through technological means." This does not deal well with situations where location is not readily nor not correctly ascertainable even though the subject has not taken any steps to "conceal" location. For example, some of us regularly use Virtual Private Networks (VPNs) to our campuses, not to conceal our location or identity but because public and hotel networks are notoriously insecure;[8] indeed, even some cellular network providers are known to tamper with web traffic.[9] What should happen to the fruits of a search in event of erroneous location determination is a purely legal issue that we are not qualified to opine on; we nevertheless note that such outcomes are not at all improbable, even when no concealment has been attempted. We also note the 'forum-shopping' issues raised by Professor Orin Kerr regarding the transformation of physical searches into remote ones.[10].

In a minor vein, we note that the current text of Rule 41 requires that warrants generally be executed during "daytime" in the subject's local timezone.[11] Obviously, if a location is incorrect, the timezone may

[4] *See* Nicolas Falliere, Liam O Murchu, and Eric Chien. *W32.Stuxnet Dossier*. Symantec Security Response. Version 1.4. Feb. 2011. URL: `http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf`.

[5] There is a technology known as "IP geolocation" which maps an IP address to a location. Accuracy of geolocation mechanisms vary; they are at their least accurate when dealing will smartphones. One of us has seen a situation where a phone located in Singapore was identified as being in Kuwait. Apparently, the geolocation mechanism being used relied on the registration address of the cellular company.

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

[7] *See* `https://www.torproject.org/`.

[8] *See* e.g., Maurits Martijn. "Maybe Better If You Don't Read This Story on Public WiFi". In: *Medium* (Oct. 15, 2014). URL: `https://medium.com/matter/heres-why-public-wifi-is-a-public-health-hazard-dd5b8dcb55e6`.

[9] *See* e.g., David Kravets. "Comcast Wi-Fi Serving Self-Promotional Ads via JavaScript Injection". In: *Ars Technica* (Sept. 8, 2014). URL: `http://arstechnica.com/tech-policy/2014/09/why-comcasts-javascript-ad-injections-threaten-security-net-neutrality/` and Robert Lemos. "Verizon Wireless injects identifiers that link its users to Web requests". In: *Ars Technica* (Oct. 24, 2014). URL: `http://arstechnica.com/security/2014/10/verizon-wireless-injects-identifiers-link-its-users-to-web-requests/`.

[10] Orin Kerr, Memo to Members of the Rule 41 Committee, February 8, 2014, as cited in *Advisory Committee on Criminal Rules*, New Orleans, LA, April 7–8, 2014, at 251–252, Advisory Committee on Criminal Rules

[11] *Federal Rules of Criminal Procedure* Rule 41(e)(2)(A)(ii).

be incorrect as well. Presumably, this would be dealt with by an explicit exemption in the warrant itself, as is permitted by the current rules.

The fact that a target machine may be abroad makes this even more critical. While US law may permit such searches, the law of the host country almost certainly does not. Coordination with other signatories to a mutual legal assistance treaty (MLAT) is essential;[12] in particular, law enforcement must be sure that American criteria for remote access are valid abroad. Some countries, in fact, prohibit such activity. Russia has charged an FBI agent with hacking for a remote search; the German courts have held that their constitution prohibits remote search entirely.[13] It is not clear that these issues have been properly considered in promlugating the proposed rule.

Danger and Intrusiveness

One fact that every working computer programmer or system administrator learns early on is that software often fails. This is especially true of patches or modifications to existing code. To give just one example, a recent release of iOS broke the ability of some iPhones to make calls.[14] The key word is "some": Apple presumably tested the iOS 8.0.1 update before shipping it, but on *some* machines it had serious side-effects.

There are many reasons for this difficulty, but one is that every computer is different. They all have different software or different usage patterns or a different network environment. This means that testing *cannot* be comprehensive; there will *always* be some situation that will occur on deployed code that was never tried in the test lab. Therein lies danger: all too often, an unsuspected failure can occur.

Remote search software is not immune. In fact, given some of its characteristics—it must run as a privileged ("root" or "administrator") program, in order to hide and to override file protections and examine hidden parts of the machine—it is more likely to cause unanticipated problems. Furthermore, errors in privileged programs can cause more damage; the same privileges that let them read protected files will also let them overwrite or delete files.

Two incidents widely attributed to intelligence agencies illustrate this point. In the "Athens Affair", someone subverted the lawful intercept mechanism on a mobile phone switch operated by Vodaphone Greece.[15] Over a period of ten months, about a hundred phones were tapped, including the Prime Minister's. The penetration was detected because a programming error by the intruder caused a switch malfunction: text messages weren't being delivered properly. It is quite striking (and not at all surprising to the technical community) that the flaw affected a part of the switch not directly involved in the tap.

A second case is the Stuxnet attack on the Iranian nuclear centrifuge plant in Natanz.[16] The direct impact on the centrifuges was not noticed; however, some of the PCs were behaving so suspiciously that one was sent to a security firm in Belarus for examination. This company found the attack software.

We are certainly not asserting that remote search software will always fail, or even that it will do so most of the time. However, if it is used on enough machines, e.g., when doing a large-scale search of bots, there almost certainly will be problems on some of them. Apart from the ethical issue of causing further damage to victims' computers, too much interference with their operation might render the search invalid. In one case,[17] the 9th Circuit held that turning a car's telecommunications system into a remote bug violated the requirement in 18 U.S.C. §2518(4) for a "minimum of interference with the services." While this holding, pertaining to wiretap law, was based on statutory language, and was highly fact-specific, it does suggest

[12] Microsoft has stressed the need for proceeding according to an MLAT with Ireland; *See* Document 15, Case 1:13-mj-02814-UA, filed June 6, 2014, U.S. District Court for the Southern District of New York. `https://www.documentcloud.org/documents/1184809-brief-in-microsoft-case-to-search-email-outside.html`

[13] *See* Susan W. Brenner. "Law, Dissonance, and Remote Computer Searches". In: *North Carolina Journal of Law and Technology* 14 (Fall 2012–2013), pp. 43–92.

[14] *See* Andrew Cunningham. "iOS 8.0.1 disabling cellular and TouchID on some phones". In: *Ars Technica* (Sept. 24, 2014). URL: `http://arstechnica.com/apple/2014/09/apple-releases-ios-8-0-1-with-healthkit-keyboard-iphone-6-fixes/`.

[15] *See* Vassilis Prevelakis and Diomidis Spinellis. "The Athens Affair". In: *IEEE Spectrum* 44.7 (July 2007), pp. 26–33. URL: `http://spectrum.ieee.org/telecom/security/the-athens-affair/0`.

[16] *See W32.Stuxnet Dossier*, footnote 4, *supra*.

[17] *See* Company v. United States, 349 F.3d 1132 (9th Cir. 2002)

that there is a threshold of interference beyond which law enforcement should not normally go. The rules for executing search warrants are also intended to minimize excess interference with the subject's normal life; consider the the normal restriction to daytime execution.[18] Searches that have a significant chance of causing damage to victims' computers is an even larger problem.

Discussion of Techniques

Surreptitious collection of evidence by compromising computers (and computerized devices such as mobile telephones) is an inherently technical endeavor, involving the use of methods that will vary widely depending on the particular hardware and software used by the target. Over time, these techniques will change to adapt to new target devices and to circumvent new countermeasures. In practice, we would expect these tools to be constantly evolving, often quite rapidly.

It is natural to expect law enforcement and prosecutors to resist disclosing the specific tools and techniques they use to obtain access to their targets, citing the desirability of preserving sensitive "sources and methods" that might be used against other targets in the future. However, this goal must be balanced against a number of other risks, whose significance may not be immediately apparent to a non-technically trained judge.

First, it is imperative that any judge or magistrate authorizing a technical computer intrusion understand certain aspects of the specific technology that will be used to conduct the intrusion. This is necessary in order to meaningfully analyze the scope of the intrusion (what other information besides the evidence being sought will be exposed) and the risks that the technique to be employed might exceed the scope of the authorization. This is particularly important when, as is often the case, the target's device is used for real-time communication (with content covered by the wiretap statutes) as well as for processing and storing information.

A defendant, similarly, will often require detailed technical information about how an intrusion was conducted in order to raise challenges as to whether a search improperly exceeded its authorization. Forensic examination of a possibly-hostile computer is difficult,[19] and software bugs in the examination process can affect the results. We note that the Federal Rules of Evidence state that "But the expert may be required to disclose those facts or data on cross-examination."[20] Similarly, expert testimony must be "the product of reliable principles and methods".[21] It is impossible to meet these conditions without disclosing the tools that extracted that data and making them available to the defense for examination.

The techniques used to obtain access to a computer can also have bearing on the authenticity, provenance, and context of the evidence collected. For example, it is possible that, depending the technical details, that a law enforcement intrusion could expose the target's computer (and any evidence collected from it) to tampering by others. Such claims can only be raised by the defense (or refuted) through analysis, possibly involving expert testimony, of the specific tools and techniques used. Other fields of forensic examination have been plagued by bad science;[22] the best assurance of quality is the adversarial process.

For these reasons, it is imperative that as much information as possible about the technology used to conduct a remote search be disclosed to the judge authorizing the search as well as to the defense in any case in which such evidence is used.

Chain of Custody and Authenticity of Evidence

It is much harder to maintain the integrity of evidence during a remote search than in a normal search done on a physically seized computer. Normal forensic procedures require that all analysis be done on a copy of

[18] *Federal Rules of Criminal Procedure* Rule 41(e)(2)(A)(ii). 41(a)(2)(B) defines "daytime".

[19] *See* Gary C. Kessler. "Anti-Forensics and the Digital Investigator". In: *Australian Digital Forensics Conference*. 2007. URL: `http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1000&context=adf`.

[20] *Federal Rules of Evidence* §705.

[21] *Id.*, §702(c).

[22] *See* e.g., Jane Campbell Moriarty and Michael J. Saks. "Forensic Science: Grand Goals, Tragic Flaws, and Judicial Gatekeeping". In: *Judges Journal* 44 (2005), pp. 16–33.

a seized disk. Kerr describes the process well.[23]

> To ensure the evidentiary integrity of the original evidence, the computer forensics process always begins with the creation of a perfect "bitstream" copy or "image" of the original storage device saved as a "read only" file. All analysis is performed on the bitstream copy instead of the original. The actual search occurs on the government's computer, not the defendant's.
>
> A bitstream copy is different from the kind of copy users normally make when copying individual files from one computer to another. A normal copy duplicates only the identified file, but the bitstream copy duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original. Whereas casual users make copies of files when their machines are running, analysts generally create bitstream copies using special software after the computer has been powered down. The bitstream copy can then be saved as a "read only" file so that analysis of the copy will not alter it.
>
> The accuracy of the bitstream copy often is confirmed using something called a "one way hash function," or, more simply, a "hash." A hash is a complicated mathematical operation, performed by a computer on a string of data, that can be used to determine whether two files are identical. If two nonidentical files are inputted into the hash program, the computer will output different results. If the two identical files are inputted, however, the hash function will generate identical output. Forensic analysts can use these principles to confirm that the original hard drive and the bitstream copies are identical.

There are a number of very important points in this excerpt. First, proper handling procedure for evidence requires that an "image copy" be made of the target disk. One reason for doing an analysis on a read-only image copy is that normal mechanisms for examining files change some of the metadata. Figure 1 is an example taken from one author's Mac computer while composing this submission: note the column labeled "Date Last Opened". Simply displaying a file will change that value.

Kerr notes that image copies also include the "slack space"—the free space—on the disk. This is very important for forensic analysis: when a file is deleted, its data is generally *not* overwritten; rather, the disk blocks are simply returned to the list of free storage. Indeed, information can be concealed there deliberately: "Even if the agents know specific information about the files they seek, the data may be mislabeled, encrypted, stored in hidden directories, or embedded in 'slack space' that a simple file listing will ignore."[24]

Finally, Kerr notes that the image file and the original device should be "hashed" to ensure that the two are identical. Even a difference of a single bit will change the hash output. It is not possible to calculate a useful hash of a disk drive that is booted, even if the computer is idle; there are too many hard-to-notice changes occurring because of normal operating system activities.

All of this is important for evidentiary reasons. If a defendant challenges the authenticity of prosecution evidence, the case is much stronger if these procedures are followed. In a recent hearing in the "Silk Road" case, precisely such challenges have been made.[25]

Yet technology does not match needs. Simply making an image copy from a machine right next to the user can take hours. Creating such an image copy is infeasible for remote search; disks are too big and communications lines are too slow. Consider a two terabyte disk (normal on new desktop computers) and a 25M bps Internet link. Running the link flat-out, the minimum time to copy the entire drive is 640,000 seconds, more than one week. Real throughput rarely exceeds half the link speed; furthermore, latency—the

[23] *See* Orin S. Kerr. "Searches and Seizures in a Digital World". In: *Harvard Law Review* 119.2 (Dec. 2005), pp. 531–585. URL: `http://www.jstor.org/stable/4093493` at 540–541. Internal citations omitted.

[24] *See* Office of Legal Education. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. 2009. URL: `http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf` at 76.

[25] The case is 1:14-cr-00068-KBF, U.S. District Court for the Southern District of New York. The judge did not rule on the merits of the argument. *See* Brian Krebs. "Silk Road Lawyers Poke Holes in FBI's Story". In: *Krebs on Security* (Oct. 14, 2014). URL: `http://krebsonsecurity.com/2014/10/silk-road-lawyers-poke-holes-in-fbis-story/` for a description of the technical dispute.

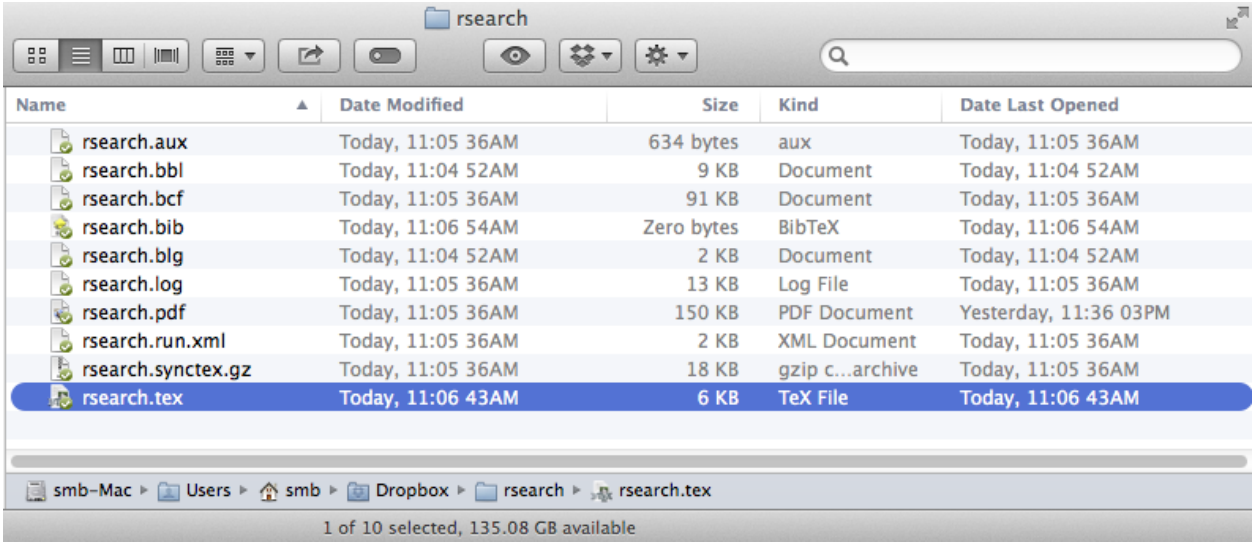

Figure 1: A screen shot noting that the last time a file is used is recorded by some operating systems.

round trip time between the source and the destination, which is limited by the speed of light—is inversely proportional to the effective bandwidth.[26] Copying a disk from San Francisco to Washington is inherently much slower than a similar copy from New York, simply because of the distance. The issue of the difficulty of creating an image copy has been ignored in the discussion of the proposed amendment, yet it is extremely important.

Specificity

As noted, the meaning of "specificity" for electronic searches remains the subject of continuing constitutional debate.[27] While we are not opining on the general question, we note that this issue becomes particularly serious when victim computers are the targets of remote search warrants. As the Preliminary Draft observed, botnets "may range in size from hundreds to millions of compromised computers".[28] While no one seriously calls into question whether a police officer, taking a crime report from a victim, should act if contraband is in plain view, scale makes a difference. The situation is not a single victim, or even a pair of victims, but potentially millions of such targets. Allowing broader seizures of information from millions of machines simply because they were the victims of computer crime seems wrong. Per our comments on page 1, we suggest an explicit requirement that all remote search software be configured extremely narrowly when used on victim computers.

Because searching a victim's computer for botnet malware exposes a non-suspect, the victim, to an unwitting search, it is particularly crucial to limit the reasons that such a search might be conducted. There would seem to be only three legitimate objectives for doing so: to demonstrate that a crime has indeed taken place (and even that is debatable, since arguably probable cause would be sufficient), to find pointers to the indivdidual responsible for the botnet, and to ascertain the extent of the damage We can separate this into two cases: when the behavior of the botnet is understood, and when it is not.

When dealing with known botnets, law enforcement should be able to develop a clear understanding of exactly how the malware in question works. In particular, the computer security community has had great

[26] See the TCP bandwidth equation, given in Matthew Mathis, Jeffrey Semke, Jamshid Mahdavi, and Teunis Ott. "The Macroscopic Behavior of the TCP Congestion Avoidance Algorithm". In: *ACM SIGCOMM Computer Communication Review* 27.3 (1997), pp. 67–82. URL: `http://dl.acm.org/citation.cfm?id=264023` at 68. "RTT' is the round trip time.

[27] *Preliminary Draft* at 341.

[28] *Preliminary Draft* at 325.

success studying botnets and locating their "command and control" nodes without hacking into other victim computers. The computer security community uses so-called "honeypot" systems—machines intended to be infected, and that engage in the same sort of risky behavior as unwitting machines do—that can be instrumented and monitored.[29] While law enforcement needs evidence to prove guilt beyond a reasonable doubt, the use of honeypots provides a less intrusive method of investigation, and law enforcement should use this type of approach first. Even if this does not suffice, the evidence will be in a very few, easy-to-locate places. It is thus feasible to construct search software that looks precisely and solely for the necessary indicia, rather than rummaging more broadly through the computer.

The alternative situation involves a more sophisticated sort of attack, where the necessary evidence may not be in a single, easy-to-examine place. A sophisticated attacker may, for example, split a contraband file into several pieces and stash them in different places. There are techniques known that allow a file to be split in such a way that some subset of the total number of shares will suffice to reconstruct it, but no information is gained by fewer shares.[30] While we haven't heard of criminals actually using such sophisticated techniques (so-called m out of n secret-sharing), it is certainly possible. That sort of scenario will likely require an examination that is less easily automated. But the complexity of the search *involving many locations on a victim's machine* would indicate that the victim should be necessarily be informed prior to downloading malware to track the attack. Given the sophistication of the attack, and the problems that could conceivably ensue on the victim's machine, we suspect that most victims would be happy to cooperate at ridding their own systems of the infection.

There is an alternative to searching the victims' machines for evidence; one could instead find such evidence at the ISP used by the victims. ISPs have been experimenting with sending notices to owners whose machines appear to be infected by a botnet; the ISP uses their knowledge of the machine's IP address to associate this with a billing address and thus an out-of-band mailing. An approach using Internet Service Providers (ISPs), discussed briefly in a paper by one of us,[31] has the advantage that it also provides law enforcement with a better way to inform the victim of the problem. ISPs might also be used to detect infection, though this also raises privacy issues that deserve a thorough policy vetting.

We thus suggest that language mandating narrow searches, especially of victim machines, be added to the rule:

> An application for a warrant issued pursuant to (b)(6)(B) must include a statement specifying precisely which data is to be be seized. The warrant itself must limit the investigation to those specific facts.

To do otherwise would be to turn a phishing attack into a fishing expedition.

Notice

Search warrants generally require notice to the target, including a receipt for items seized.[32] As noted in the proposal, this is problematic for remote search.[33] We feel that the problem is even more difficult than indicated.

We can think of only four feasible mechanisms for notifying the target of a search: a file left on the computer; a pop-up window; an email message; or a physical letter. All are problematic, especially for mass searches.

[29] *See* Kirill Levchenko et al. "Click trajectories: End-to-end analysis of the spam value chain". In: *IEEE Symposium on Security and Privacy*. IEEE. 2011, pp. 431–446. URL: `http://www.icir.org/christian/publications/2011-oakland-trajectory.pdf` for a description of a non-intrusive analysis of a bonnet.

[30] *See*, e.g., Adi Shamir. "How to Share a Secret". In: *Communications of the ACM* 22.11 (1979), pp. 612–613, for a description of how to do this with encryption keys.

[31] D.D. Clark and S. Landau. "The Problem isn't Attribution: It's Multi-Stage Attacks". In: *Third International Workshop on Re-Architecting the Internet*. 2010.

[32] *Federal Rules of Criminal Procedure* Rule 41(f)(1)(C).

[33] *Preliminary Draft* at 327.

A file left on a computer probably won't be noticed, but the most serious concern is that the user has no way to determine the authenticity or provenance of such a note. If such files were actually to become a legitimate form of communication, hackers would immediately start emailing files that looked just like the real ones, except with a URL to click on "to acknowledge the message". Naturally, these URLs would not be benign.

Email, of course, would have similar problems. The FBI itself has warned of malicious spam email purporting to be from them.[34] There are, at least in theory, technical solutions involving digitally signed messages and a Public Key Infrastructure. Experience with both Web browsers and phishing emails suggest that these do not work in the absence of careful training of users.

Hackers will abuse law enforcement-generated pop-up messages in similar ways. Indeed, they already have abused similar mechanisms, to serve ads.[35] Furthermore, there is little evidence that people would pay attention to such boxes; indeed, one online source jokingly defines a "dialog box" as "A window in which resides a button labeled 'OK' and a variety of text and other content that users ignore."[36]

Physical mail might suffice, but it will often be too time-consuming and expensive. While we do not have precise cost figures for criminal investigations, reports indicate that ISPs find such requests burdensome and charge accordingly.[37] Physical email is also very difficult when dealing with unknown search targets. While a more extensive search of the target computer might yield a physical address, per the discussion in the prior section such a search would be extremely intrusive.

The language in the proposed rule—"reasonable efforts"—is probably correct; given these difficulties, we do not know how it can be done. We thus suggest that the Department of Justice develop and (after suitable public comment) promulgate binding regulations for how this should be accomplished.

Remote Access and Security Mechanisms

While not directly addressed in the proposed rules, the proposal anticipates, at least implicitly, that surreptitious remote computer searches will become an increasingly prevalent law enforcement technique in the future. We agree that this is likely, and it is important that rules of evidence and criminal procedure address them. However, these methods also raise a number of policy issues that will need to be addressed by the courts and by lawmakers. We raised some of these in our recent papers on the subject,[38] but they bear some discussion here.

Law enforcement reliance on remote computer intrusions exposes a conflict between solving some crimes by collecting evidence and preventing other crimes by better securing computers. Virtually any vulnerability (whether due to a software flaw or an explicit "backdoor") that can be exploited by law enforcement for investigative purposes has the potential for illicit exploitation by criminals and foreign intelligence services. And the computer software, hardware, and devices used by criminals (and from which evidence is collected)

[34] *See* `http://www.fbi.gov/scams-safety/e-scams`:

> Ransomware Purporting to be from the FBI is Targeting OS X Mac Users
>
> 07/18/13—In May 2012, the Internet Crime Complaint Center posted an alert about the Citadel malware platform used to deliver ransomware known as Reveton. The ransomware directs victims to a drive-by download website, at which time it is installed on their computers. Ransomware is used to intimidate victims into paying a fine to "unlock" their computers. Paying the fine does nothing to solve the problem with the computer; do not follow the ransomware instructions. The ransomware has been called "FBI Ransomware" because it uses the FBI's name...

Several of us have received other spam messages purporting to be from the FBI.

[35] Washington State Office of the Attorney General. *Pop-Up Ads*. URL: `http://www.atg.wa.gov/InternetSafety/PopUpAds.aspx`.

[36] `http://www.w3.org/2006/WSC/wiki/Glossary`.

[37] *See* Nate Anderson. "Big Cable fed up with endless P2P porn subpoenas". In: *Ars Technica* (Feb. 4, 2011). URL: `http://arstechnica.com/tech-policy/2011/02/big-cable-getting-fed-up-with-endless-p2p-porn-subpoenas/` for a news story about a civil case, where plaintiffs were offered a limited number of subpoenas per month at the discounted price of $95 apiece. For a discussion of the technical difficulties ISPs face when fielding such requests *see* Richard Clayton. "Anonymity and Traceability in Cyberspace". Also published as technical report UCAM-CL-TR-653. PhD thesis. University of Cambridge, Darwin College, 2005. URL: `http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.html`.

[38] *See* "Lawful Hacking", footnote 2, *supra*.

are also used by thousands—or millions—of innocent citizens to store, process, and communicate the most important and sensitive details of their lives and businesses.

This means that that any flaw used by law enforcement for laudable evidence collection purposes also represents a risk to innocent people. As discussed above, it is natural to expect law enforcement to hold information about exploitable flaws closely, to maximize their useful lifetime for investigative use. But other public policy goals must be weighed against this. In addition to the rights of defendants to use information about these techniques to challenge evidence (discussed above), there is the broader question of reporting the vulnerabilities that law enforcement exploits to vendors so they can be fixed.[39] That is, the use of vulnerabilities for law enforcement must be balanced against the need to protect citizens from criminals who might exploit them themselves.

While we recognize that such policy questions may be beyond the scope of this particular proposal, we believe that it is imperative that they be addressed comprehensively. A piecemeal solution, such as is proposed here, is likely to leave society more vulnerable than less so. Thus any proposal to expand the use of vulnerability exploitation by law enforcement must be accompanied by a broader policy discussions of these inexorably related questions.

Recommendations

As is undoubtedly clear, we have a number of concerns with the current proposal, which does not appear to have undergone a thorough vetting from the technical side. Because we are not sure of the best way to proceed to satisfy law enforcement's needs, our recommendations are a response to the current proposal rather than a complete set of recommendations. Any proposal to change Rule 41 should satisfy the following recommendations, but there are likely to be other requirements, both technical and legal, that should be met as well.

- We recommend against the use of a single warrant to conduct multiple simultaneous searches on victims' computers. Blanket warrants cover far too many machines, without the necessary specificity; furthermore, they pose a great risk of damage to some of them.
- We recommend that when a warrant is issued for searching a victim's computer, the warrant include precise, particularized specifications of the area of the computer that is to be searched.
- Remote search carries significant risk of causing international complications. Guidance to law enforcement, and perhaps the rule itself, should stress this. Except for extremely serious cases, such searches should be done only with the cooperation of the host country.
- As noted in the proposed rules, giving notice of a search is problematic. We suggest a two-pronged approach. First, there needs to be explicit guidance to law enforcement on what mechanisms should be used and under what circumstances; the conditions when notice can be omitted should also be described. Second, the Department of Justice should engage the technical community in an effort to devise better mechanisms.

We have stated previously that we think that targeted hacking, with a search warrant and under suitable conditions, is a useful investigative tool.[40] However, such searches must be targeted, both to comply with legal requirements and to avoid some of the technical risks.

Depositing malware to investigate victims' machines is a very tricky business; it should never be attempted lightly. The current proposal, which does not pay enough attention to complex technical issues, must be

[39] We discussed this issue in detail in "Lawful Hacking", footnote 2, *supra*.

[40] *See* Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. "Going Bright: Wiretapping without Weakening Communications Infrastructure". In: *IEEE Security & Privacy* 11.1 (Jan.–Feb. 2013), pp. 62–72. ISSN: 1540-7993. DOI: 10.1109/MSP.2012.138. URL: https://www.cs.columbia.edu/~smb/papers/GoingBright.pdf and "Lawful Hacking", footnote 2, *supra*. The former discusses technical aspects; the latter concentrates on the legal and policy issues.

substantially reworked to take this concern into account. Otherwise, law enforcement could be creating more damage than that which it is seeking to prevent, an approach that can neither be constitutional nor desired.

We have made recommendations on changes that should be made to the proposal, but we believe more than simple changes are required. While in this note we have identified a number of specific technical flaws with the proposed changes to Rule 41, there may be others that we have missed. In addition, for the most part, we have not addressed the many legal complexities in this proposal. So we suggest—and we have argued this at greater length earlier[41]—that a legislative fix would be best. There is, to our knowledge, no explicit statutory authority for law enforcement to hack into computers; given the intrusiveness and danger of such activities, there is a need for balance. The legislative process is best suited to address this.

[41] *See* "Lawful Hacking", footnote 2, *supra*.