Insecure Surveillance: Technical Issues with Remote Computer Searches

Steven M. Bellovin, Matt Blaze and Susan Landau

Abstract: Communications technology is changing at a breathtaking rate, and the law has been racing to keep pace. But if communications technology is complex, matching surveillance law to new communications technologies is even more so. Here we examine two recently proposed US government rules for conducting remote computer searches and illuminate the mismatch between legal proposals for handling botnet investigations and for issuing warrants in cases when anonymizing software is used to hide the location of a computer. We show that at a fundamental level, the proposals are flawed: they mistake victims for criminal actors and confuse legitimate uses of location-anonymizing software with nefarious activity. We also show that the proposals are likely to be damaging, including creating serious security problems.

1 Introduction

Law, like technology, is not static. If a legal mechanism has problems, it can be amended—patched, if you will. In the U.S., the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States can propose changes to the *Federal Rules of Criminal Procedure* (http://www.uscourts.gov/uscourts/rules/criminal-procedure.pdf); these are enacted via a long, complex approval process (see Section 4).

Rule 41 of the Federal Rules of Criminal Procedure governs the processes for authorizing searches and seizures. A proposal to amend these rules is currently moving forward through the judicial rulemaking process. The proposal is quite comprehensive, and some of the changes attempt to bring the rules in line with modern technology. We examined, from a technical perspective those proposed changes that relate to remote computer searches under two conditions: when "anonymizing software" that hides the location of a computer has been used and when the investigation involves botnets.

Under current rules, a magistrate judge can issue a warrant to search only computers located within his or her district. The proposed changes would grant judges the authority to issue a single warrant to cover remote searches of computers in other districts if the location of the computer has been concealed or if

This is an unedited version of the paper. The final version appeared in *IEEE Computer* 49.3 (March 2016): 14-24, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7433349

the computers to be searched are located in five or more jurisdictions [5, pp. 326-327].

Specifically, the proposal states:

> [A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means; or of (B) in an investigation of a violation of 18 U.S.C. §1030(a)(5) [the notation means "Section 1030(a)(5) of Title 18 of the U.S. Code;" 18 U.S.C. §1030 is more commonly known as *the Computer Fraud and Abuse Act*, the Federal anti-hacking statute; the original version was passed in 1984], the media are protected computers that have been damaged without authorization and are located in five or more districts. [5, pp. 338-339]

"Protected computer" is a legal term of art, defined in 18 U.S.C. §1030(e)(2). Without going into details, effectively any machine connected to the Internet is "protected".

Part (A) is intended to apply to situations where a criminal or spy seeks to hide their activities through disguising the location of their device. Part (B) says when protected computers in at least five districts have been damaged, a magistrate judge can authorize remote searches via a single warrant. According to the committee, this aspect of the proposed changes, which is intended to apply to botnet investigations, is meant to be used in a "limited class of investigations" [5, p. 338]. There is no explicit limitation in the proposal that would make it so. Because the rule permits law enforcement to search individual bots, the search extends to innocent victims; and it could be broad indeed. This means that the proposed changes to Rule 41 would have very wide implications, applying to a large number of cases in which computer evidence is at play.

It is worth stepping back briefly to put the discussion of search in context. In the US, this begins with the Fourth Amendment to the Constitution:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Applying the Fourth Amendment in specific situations can be complex, and there is a large body of often counterintuitive and even occasionally contradictory law here.

Our concern is the interactions of the proposed changes regarding remote computer search with the realities of the technology itself. We are specifically concerned about issues of jurisdiction, chain of custody and authenticity of evidence, specificity of search, and notice. We aim not to break new technical ground here, but instead show how technical issues, *many of which are well known to the security community,* play out and cause serious difficulties in a legal framework.

Although this paper concerns a specific detail of U.S. law, the underlying issues are important worldwide. All countries must deal with questions of jurisdiction, if only because of national boundaries. The problem of investigating botnets is global. Democracies, with their limits on police powers, have to cope with identifying the true perpetrators without doing massive dragnet searches.

2 How Electronic Searches are Conducted

Although the FBI has been conducting surreptitious remote computer searches for over a decade, the bureau has said very little about how remote searches are performed today. The first public mention of such tools goes back to 2001 [17]. No one seemed to pay much attention until 2007, when there was a court filing on the FBI's use of the "Computer IP Address Verifier" (CIPAV) package, software that collects IP and MAC addresses, open ports, running programs, default browser and version, default OS and version, current logged-in user name [14]. (Also see https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government and http://politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf.) In that case, CIPAV was used to track down a student threatening to bomb a high school in Lacey, Washington.

CIPAV has been used in multiple cases across the country. The tool's use is complicated. First it must be downloaded onto a target machine by law enforcement, perhaps by an email targeted to the user, perhaps by other means. Then it must search the machine for information such as that described above, report it, and then download spyware onto the machine to capture particular data. An FBI memo notes "a good deal of uncertainty under what authority is required to deploy an IPAV [*sic*]." (See the EFF web page mentioned above.) After consulting with their Office of General Counsel and the National Security Law Branch, the FBI opted for a two-step legal process: a search warrant for the computer intrusion, and a so-called "Pen Register/Trap-and-Trace" order for the subsequent monitoring.

There are other techniques in use as well. In one well-publicized case, the FBI apparently hacked into an Irish child pornography server in Ireland and patched it to serve malware to visitors running a particular version of Firefox over Tor [8]. The malware did nothing except to send an alert with the real IP address of the machine to a server located in Virginia; this, of course, is an important step in finding the users of this site.

A search warrant is almost certainly legally sufficient for the penetration, and is quite likely necessary. The second order, the pen register/trap-and-trace order, authorizes the FBI to collect ongoing information on the endpoints of new communications during this period. Of course, if private information or communication content is to be obtained during a remote search, these orders must be a warrant or the "super warrant" needed for wiretaps.

The protections of the Fourth Amendment stop at the border. If the FBI wishes to plant a CIPAV on a foreign computer, there is no obstacle in U.S. law to them simply doing so, as long as no "U.S. persons" are involved. In a 2013 District Court case in the Southern District, Texas (*In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.~Supp.~2d 753 (S.D. Tex. 2013), available at https://s3.amazonaws.com/s3.documentcloud.org/documents/692822/in-re-warrant-to-search-a-target-computer-at.pdf), Judge Stephen Smith ruled that because "the current location of the Target Computer is unknown, it necessarily follows that the current location of the information on the Target Computer is also unknown," and that because of Rule 41 he therefore didn't have the authority to issue the warrant. Indeed, these changes to the rule were proposed partially in response to his opinion. Of course, hacking into a foreign computer may violate the law of that country.

3 Specifics of the Proposed Rule 41 Changes

In this section we examine the various technical problems posed by the proposed Rule 41 changes. Some are particularly problematic for the investigation of botnets, while others are problems with remote search generally.

3.1 Searches of Victim Computers

Botnets pose complex challenges to law enforcement. Botnet size is one problem; the fact that the machines that have been taken over are *victims'* devices is another. Because of the multiplicity of victims, law enforcement sought to simplify % the situation investigations by using a single warrant approach to search multiple machines participating in a botnet.

The proposal suggests using a "common scheme to infect the victim computers with [law enforcement] malware" [5, p. 325]. This is a dangerous approach.

From a technical standpoint, the danger is that such a "common scheme" may easily go out of control. Current malicious botnet technology is generally relatively simple: the malware is typically essentially the same on all victims' machines, and thus it is relatively easy to know where to find it and how to disable it. *There is no technical reason why, some time in future, botnet malware could not be far more sophisticated,* *but the proposed rule is heavily focused on the current state of criminal practice, and not on how technology is likely to change*. 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. Such a scheme could easily fail by damaging the victims’ computers in unpredictable and unexpected ways. As we know from such examples as Stuxnet, any law enforcement malware downloaded on victims’ machines must be carefully tailored to the device [20]. 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 law enforcement malware from causing more widespread damage should it escape the victim’s computer.

From a legal standpoint, the lack of specificity is also highly problematic. A technically sophisticated criminal could hide data in victims’ machines in different places on different 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, since it would require searching the entire computer for a very few files.

In combination, these two sets of reasons make the multiple-victims-one-search-warrant approach exceptionally dangerous.

3.2 Location and Jurisdiction

Remote search creates new complexities, with potentially serious problems, for legal jurisdiction. The Fourth Amendment requires that warrants “particularly describ[e] the place to be searched.” 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. This is true even if its IP address is known.

“IP geolocation” techniques attempt to map IP addresses to locations. This can be done using the *whois* database and DNS records (limited in value since many sites use a third party as host), using Internet topology, or even by human inference, such as by examining the language used in a webpage [7]. But while such techniques are often “good enough” for some purposes, IP geolocation can be incorrect relatively frequently, sometimes undetectably so. For example, because many cellular carriers use carrier-grade NAT, IP geolocation information is often inaccurate with smartphones, and IP location (which is not associated with a cell base station) can be picked up only coarsely.

Virtual Private Networks (VPNs) create one type of problem, while Tor (“The Onion Router”), which is specifically *designed* to obscure location, creates another. Needless to say, geolocating Tor endpoints is at best extremely difficult [6,18].

Thus open standards and procedures for making location determination are essential. The proposed rule is problematic, though. Section (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." As written this clause would apply to any VPN user, which is surely not the intent. Hiding a computer's location can occur for many legitimate reasons, and is not, in itself, a criminal activity. Thus the rule as written captures the wrong issue; the rule regarding location hiding should apply only when the machine is under suspicion of conducting nefarious activities.

We do not address the (mostly) legal question of how to deal with the "fruits" of a remote search conducted in what turns out to be the location other than where authorized, except to note that this likely will be a relatively common occurrence under current technology.

The fact that a target machine may be abroad makes this even more critical. Thus what is needed is coordination with other signatories to a "mutual legal assistance treaty" (MLAT). In the current post-Snowden international environment, it is unlikely that the searches being proposed under the changes in Rule 41 would be universally accepted by other countries. Before such rules are enacted, law enforcement must be sure that American criteria for remote access are valid abroad. Some countries, in fact, actively prohibit and prosecute foreign searches. Russia has charged an FBI agent with hacking for a remote search; the German courts have held that their constitution prohibits remote search entirely [3].

3.3 Danger and Intrusiveness

A remote search carries many risks, including those stemming from software errors. To give just one example, a recent release of iOS broke the ability of some iPhones to make calls (http://arstechnica.com/apple/2014/09/apple-releases-ios-8-0-1-with-healthkit-keyboard-iphone-6-fixes/). 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.

Remote search malware is essentially a surreptitious "patch" made to a target system. Testing *cannot* be completely comprehensive; there will almost *always* be some situation that can occur in a deployed instance that was never tested in the lab. Therein lies danger: all too often, an unsuspected failure can occur, and remote search software is not immune from such errors. 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 Vodafone Greece [15]. About a hundred phones were tapped, including the Prime Minister's, over a period of ten months. A programming error by the intruder caused a switch malfunction—text messages weren't being delivered properly—and the penetration was detected. 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 [20]. The direct impact on the centrifuges was not noticed; however, some of the PCs behaved so suspiciously that one was sent to a security firm in Belarus for examination. This company found the attack software.

We are certainly not suggesting that remote search software will *always* fail, nor 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. This creates two serious problems. The first is the issue of the government causing further damage to victims' computers, a situation that is all too likely to occur on occasion (recall that the searches will be of machines whose owners are *not* suspected of wrongdoing). The second is that too much interference with their targeted computers' operation might render the search invalid. The rules for executing search warrants are also intended to minimize excess interference with the subject's normal life. Searches that have a significant chance of causing damage to victims' computers are an even larger problem.

3.4 Discussion of Techniques

With the exception of national-security investigations that do not result in evidence used in court, under U.S. law wiretap investigations must be disclosed to the target. For example, if a wiretap is conducted under federal law, the target must be informed of the search within thirty days after the conclusion of the wiretap. Yet the surreptitious searches being proposed create certain serious conflicts with the openness lying at the heart of U.S. jurisprudence.

Surreptitious collection of evidence by compromising computers (and computerized devices such as mobile telephones) is an inherently technical endeavor, involving methods that 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 had improperly exceeded its legal authorization. Forensic examination of a possibly hostile computer is difficult [11], 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" (§705 in https://www.law.cornell.edu/rules/fre). Similarly, expert testimony must be "the product of reliable principles and methods" (§702(c)). It is simply impossible to verify that these conditions were met 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 on the technical details, 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 [9, 13]; the best assurance of quality in the U.S. court system is the adversarial process.

The courts have not always agreed on the importance of the defendants' being able to view source code (*Swendra v. Commissioner of Public Safety of Minnesota*, A07-2434; *Minnesota v. Underdahl*, A07-2293, A07-2428).
We believe 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. Declaring someone guilty "beyond a reasonable doubt", without examining the software that provided crucial evidence, is just wrong.

3.5 Chain of Custody and Authenticity of Evidence

Just as U.S. jurisprudence requires open processes, it requires that evidence be uncorrupted. 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. As described by Kerr, normal forensic procedures require that all analysis be done on a copy of a seized disk [10]. This protects the original disk from accidental corruption (opening a file can change the "last accessed" date) and makes it easier to examine blocks on the free list. The original disk and the image file are cryptographically hashed to show authenticity, but that won't help for disk images taken in a remote search.

A difference of a single bit anywhere in the input, of course, will change hash output (that is, indeed, part of the usefulness of hashing). But it is not generally possible to calculate a useful hash of a disk drive running in a live system, even when the computer is idle; in most file systems, there are continual changes made to the file system image through normal operating system activities. A file system is effectively a moving target.

All of this is important for evidentiary reasons. A defendant can challenge the authenticity of prosecution evidence if procedures are not followed or discrepancies are found

Current technology simply does not match our needs here, and this is not likely to change in the foreseeable future. Simply making an image copy from a machine can take hours under ideal conditions and with the cooperation of the machine's owner. Creating such an image copy of a non-trivial size disk is generally infeasible for surreptitious remote search; disks are too big and communications lines are too slow. (Copying a two terabyte disk that is behind a 25 Mbps link would take more than a week even without considering network latency, contention for the disk or link, etc.) The issue of the difficulty of creating an image copy has been ignored in the discussion of the proposed rule changes, yet it is extremely important.

3.6 Specificity

Sometimes a difference in scale can be a difference in kind, and we believe it is in the case of searches of the victims of botnets. The proposed rule change is not about a single victim, or even a handful 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 in Section 3.1, we suggest an explicit requirement that all remote search software be configured extremely narrowly when used on victim computers.

As noted, the meaning of "specificity" for electronic searches remains the subject of continuing constitutional debate [5, p. 341]. 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" [5, p. 325]. While no one seriously calls into question whether or not a police officer, taking a crime report from a victim, should act if contraband is in plain sight, the meaning of "plain sight" in a computer search is by no means clear.

Because searching a victim's computer for botnet malware exposes the victim, a non-suspect, to an unwitting search, it is particularly crucial to limit the reasons under which 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 individual 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 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 [12]. 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, using, for example, Shamir secret-sharing [16]. Such sophisticated techniques are 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 quite willing to cooperate at ridding their own systems of the infection—once law enforcement properly authenticated itself of course.

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 can send an out-of-band mailing. An approach using Internet Service Providers (ISPs) [4] 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. To do otherwise would be to turn a phishing attack into a fishing expedition.

3.7 Notice

Search warrants generally require notice to the target, including a receipt for items seized (Rule 41(f)(1)(C)). As noted in the proposal, this is problematic for remote search [5, p. 327]. 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.

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 depositing 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. (See http://www.fbi.gov/scams-safety/e-scams.)

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 without highly trained users.

Hackers can be expected to abuse law enforcement-generated pop-up messages in similar ways. Indeed, they already have abused similar mechanisms, to serve ads (http://www.atg.wa.gov/InternetSafety/PopUpAds.aspx). Furthermore, there is little evidence that people would pay attention to such boxes. (http://www.w3.org/2006/WSC/wiki/Glossary).

Physical mail might suffice, but that 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. Physical mail 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.

That all possible forms of notice are problematic is exactly our point. The standard in the proposed rule—”reasonable efforts”—is probably the best that can be achieved here; we do not know how to do better. We thus suggest that the Department of Justice develop and (after suitable public comment) enact regulations for how this will work in practice.

3.8 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 have previously raised some of these in our recent papers on the subject [1,2].

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. Whether due to a software flaw or an explicit “backdoor,” virtually any vulnerability 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) 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. The use of vulnerabilities for law enforcement must be balanced against the need to protect citizens from criminals who might exploit them themselves [2].

4 What Has Transpired

In early November 2014, the Judicial Conference’s Advisory Committee on the Federal Rules of Criminal Procedure held hearings on the proposed changes. A number of organizations, including the Electronic Frontier Foundation, the American Civil Liberties Union, the Center for Democracy and Technology, and Google submitted comments. Many were critical, and raised some of the same points we have raised here. The Justice Department even replied specifically to Google’s objections (http://www.regulations.gov/#!documentDetail;D=USC-RULES-CR-2014-0004-0055). The objections notwithstanding, on March 16, 2015, the Advisory Committee approved the changes by an 11-1 vote.

The process of amending the rules is complex. (For details, see http://www.uscourts.gov/rules-policies/about-rulemaking-process/how-rulemaking-process-works/overview-bench-bar-and-public.) The full Judicial Conference has since approved the changes and sent them on to the Supreme Court (www.uscourts.gov/file/18641/download); if it approves them, Congress has the right to block the changes. If there are no hold-ups—and opposition continues—the rule change will go into effect on December 1, 2016.

5 Securely Conducting Lawful Surveillance

Law enforcement's role is traditionally the *solution* of crimes, with *prevention* usually only a secondary goal. The practice of computer security, on the other hand, generally focuses chiefly on prevention.

When one is tracking down a particular crime or set of crimes, it is difficult to see beyond immediate short-term goals. Yet whether these goals are seeking to regulate the broad use of cryptography, or the use of zero-day vulnerabilities in criminal investigations, short-term actions have long-term implications. While we recognize that the policy questions raised by the proposed Rule 41 changes may be beyond the scope of this particular proposal, we believe that it is imperative that they be addressed comprehensively including, and especially, the impact on cybersecurity. A piecemeal solution, such as is proposed here, is likely to leave society more vulnerable rather than less so. Thus any proposal to expand the use of vulnerability exploitation by law enforcement must be accompanied by a broader policy discussion of these inexorably related questions.

5.1 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. Our recommendations are a response to the current proposal rather than a complete set of recommendations for balancing the rights of defendants against the needs of law enforcement.. That is, any changes Rule 41 should at minimum satisfy these recommendations, but there may well 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 in 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 noted elsewhere that targeted hacking, with a search warrant and under suitable conditions, is likely to become an increasingly prevalent investigative tool; see [1, 2]. However, such searches must be carefully targeted and and their implementations tested, both to comply with legal requirements and mitigate some of the inherent technical risks. For example, despite being narrowly targeted and meticulously crafted, Stuxnet still managed to spread outside its apparent target; fortunately, because it was carefully designed, it does not appear to have actually caused serious damage outside of its target in Natanz.

Depositing law enforcement malware to investigate victims' machines is a very tricky business; it should never be attempted lightly. The proposal, which does not sufficiently attend to complex technical issues, must be 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.

In this article, 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 [2]—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 better suited to address this than the rulemaking process.

We note that while this paper has focused on a specific proposal that applies only to U.S. law, the issues are international. Matters of jurisdiction, proportionality, privacy, intrusiveness, preservation of evidence, and striking the balance between effective law enforcement and risk to the innocent are concerns in all democracies that operate under the rule of law. This particular debate is local; the issues and the stakes are global.

Acknowledgment:

Matthew Green made many helpful comments on a draft of this paper.

References:

[1] Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. "Going Bright: Wiretapping with-out 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: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6357177&tag=1.

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

[4] 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.

[5] 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.

[6] Roger Dingledine, Nick Mathewson, and Paul Syverson. "Tor: The Second-Generation Onion Router". In: *Proceedings of the 13th USENIX Security Symposium*. Aug. 2004.

[7] Mark Gondree and Zachary N.J. Peterson. "Geolocation of Data in the Cloud". In: *CODASPY '13*. Feb. 2013. url: http://znjp.com/papers/gondree-codaspy13.pdf.

[8] Dan Goodin. "Attackers wield Firefox exploit to uncloak anonymous Tor users". In: *Ars Technica* (Aug. 5, 2013). url: http://arstechnica.com/security/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users/.

[9] Spencer S. Hsu. "FBI admits flaws in hair analysis over decades". In: *Washington Post* (Apr. 18, 2015). url: http://www.washingtonpost.com/local/crime/fbi-overstated-forensic-hair-

matches-in-nearly-all-criminal-trials-for-decades/2015/04/18/39c8d8c6-e515-11e4- b510-962fcfabc310_story.html.

[10] 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.

[11] 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.

[12] 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://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5958044.

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

[14] Kevin Poulsen. “FBI’s Secret Spyware Tracks Down Teen Who Made Bomb Threats”. In: *Wired* (July 18, 2007). url: http://archive.wired.com/politics/law/news/2007/07/fbi_spyware.

[15] 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] Adi Shamir. “How to Share a Secret”. In: *Communications of the ACM* 22.11 (1979), pp. 612–613.

[17] Bob Sullivan. “FBI software cracks encryption wall”. In: *MSNBC* (Nov. 20, 2001). url: http://www.nbcnews.com/id/3341694/ns/technology_and_science-security /t/fbi-software-cracks-encryption-wall/.

[18] P F Syverson, D M Goldschlag, and M G Reed. “Anonymous Connections and Onion Routing”. In: *IEEE Symposium on Security and Privacy*. Oakland, California, Apr. 1997, pp. 44–54. isbn: 0-8186-7828-3. url: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=601314.

[19] Dustin Volz. “FBI’s Plan to Expand Hacking Power Advances Despite Privacy Fears”. In: *Government Executive* (Mar. 17, 2015). url: http://www.govexec.com/management/2015/03/fbis-plan-expand-hacking-power-advances-despite-privacy-fears/107712/.

[20] Kim Zetter. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*.