Insecure Surveillance: Technical Issues with Remote Computer Searches

Steven M. Bellovin, Columbia University
Matt Blaze, University of Pennsylvania
Susan Landau, Worcester Polytechnic Institute

Proposed changes to federal rules authorizing warrants for remote computer searches mistake victims for criminals, confuse legitimate uses of location-anonymizing software with nefarious activity, and are likely to be both intrusive and damaging, creating serious security problems and potentially compromising criminal investigations.

Law, like technology, is not static. If a legal mechanism has problems, it can be amended—patched, if you will. In the US, the Judicial Conference—an administrative body of senior federal judges headed by the chief justice of the Supreme Court—frames policy guidelines for all federal courts. Proposed changes to federal rules are submitted, after public comment, by five advisory committees to the Judicial Conference’s Standing Committee on Rules of Practice and Procedure, which upon its approval forwards them to the Supreme Court and Congress for final approval.

Rule 41 of the Federal Rules of Criminal Procedure governs the authorization of searches and seizures. A proposal to amend this rule is currently moving forward through the judicial rulemaking process. The proposal is quite comprehensive, and some of the proposed changes attempt to bring the rule in line with modern technology. We examined, from a technical perspective, those changes that relate to remote computer searches under two conditions: when anonymizing software that hides a computer’s location has been used, and when the investigation involves botnets—robot networks of Internet-connected computers hijacked and used to carry out malicious activities including spam propagation and distributed denial-of-service attacks.

This article concerns a specific detail of US law, but 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. Identifying the true perpetrators without doing massive dragnet searches is a problem for all democracies.
A NOT-SO-MODEST PROPOSAL

Currently, magistrate judges—who are appointed by district court judges to assist them in performance of their duties—can issue a warrant to law enforcement to search computers, but only ones located within their district. The proposed changes would grant judges the authority to issue a single warrant to cover remote searches of a computer in other districts if its location has been hidden or if it is located in five or more jurisdictions. 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 (B) in an investigation of a violation of 18 U.S.C. §1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.2

The legal section referred to is Section 1030(a)(5) of Title 18 of the US Code, more commonly known as the Computer Fraud and Abuse Act, which was enacted by Congress in 1986. “Protected computer” is a legal term of art defined in 18 U.S.C. §1030(e)(2); without going into detail, effectively any machine connected to the Internet is “protected.”

Part A of the proposed rule applies to investigations of criminals or spies who attempt to hide their online activities by disguising their device’s location. According to the drafters, part B is intended to apply to a “limited class” of botnet investigations.2 However, there is no explicit limitation in the new language: Rule 41 permits law enforcement to search individual bots, and such searches could extend to devices owned by many innocent victims.

In the US, all law pertaining to searches is rooted in the Fourth Amendment to the Constitution, which guarantees “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—especially when the criminal activity involves computers—and has produced counterintuitive and potentially contradictory law.

Our concern here is the interaction of the proposed changes regarding remote computer search with the realities of the technology itself. We focus on the technical aspects of the proposed Rule 41 changes, which, though well known to the security community, seem to be either underappreciated by or unknown to judicial rule makers.

REMOTE SEARCHES AND THE LAW

Although the Federal Bureau of Investigation (FBI), the nation’s primary federal domestic law enforcement agency, has been conducting surreptitious remote computer searches for over a decade, little is known about the methods or tools it uses to perform such searches. In 2001, the first public mention of such a tool was made in connection with software dubbed “Magic Lantern” that injected a virus onto a suspect’s machine to obtain its encryption keys.3 The media paid little attention to the issue until 2007, when a Freedom of Information Act (FOIA) request by the Electronic Frontier Foundation (EFF) revealed the FBI’s use of the Computer IP Address Verifier (CIPAV) package, software that collects a system’s IP and MAC addresses, open ports, running programs, default browser and version, default OS and version, and current logged-in user name.4,5 In that case, CIPAV was used to track down a student threatening to bomb a high school in Lacey, Washington.

The FBI has employed CIPAV in multiple criminal investigations across the country. The tool’s use is complicated: after being downloaded onto a target machine through an email to the user or some other means, CIPAV searches the machine for information, reports it, and downloads spyware to capture particular data. According to an FBI memo released in response to the EFF’s FOIA request, years after first deploying the tool there was “still admittedly a good deal of uncertainty under what authority” the bureau used it.5 After consulting with its Office of General Counsel and National Security Law Branch, the FBI opted for a two-step legal process: a search warrant for the computer intrusion, and a pen register/trap-and-trace (PR/TT) order for subsequent monitoring.

The FBI employs other remote search techniques as well. In a recent well-publicized case, it apparently hacked into an Irish server hosting a child pornography website and
patched it to serve malware to visitors running a particular version of Firefox over the Tor network. The malware sent an alert with the user’s real IP address to a server in the US, obviously an important step in unclinking the site’s users.

A search warrant is almost certainly legally sufficient for remote computer penetrations, and is quite likely necessary. A PR/TT order authorizes the FBI to collect ongoing information on the endpoints of new communications during the specified monitoring period. For legal reasons, such orders, which more or less identify who is communicating with whom, do not require “probable cause” and thus are much easier to obtain than wiretap warrants. If private information or communication content is to be obtained during a remote search, investigators need either a warrant or the “super warrant” needed for wiretaps. (Because Congress felt that wiretaps were exceptionally intrusive, the Wiretap Act makes these considerably harder to obtain than ordinary search warrants.)

Fourth Amendment protection stops at the border. If the FBI wishes to plant malware on a foreign computer, there is no legal obstacle to doing so, as long as no “US persons” are involved. In a 2013 district court case in Texas, 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 thus he did not have the authority to issue a search warrant.

In the following sections we explore various technical complications associated with the proposed changes. Some of these relate to remote search generally, whereas others are particularly problematic for botnet investigations.

SOFTWARE FAILURES AND UNINTENDED CONSEQUENCES

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. The key word is “some”: Apple presumably tested the 8.0.1 update before releasing it, but on particular devices it had serious side effects.

Remote search malware is essentially a surreptitious “patch” made to a target system. Testing can never be completely comprehensive; invariably some situation will occur in a deployed instance that was never tested in the lab. Like all software, remote search software is not immune from failures. In fact, given that it must run as a privileged (“root” or “administrator”) program to hide, 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 to tap more than 100 phones of government officials, including the prime minister, over a period of 10 months. A programming error by the intruder caused a switch malfunction that prevented text messages from being delivered properly, exposing the intrusion. Notably—and not at all surprising to security experts—the flaw affected a part of the switch not directly involved in the tap. Similarly, in the Stuxnet attack on the Iranian nuclear facility in Natanz, plant authorities did not detect its impact on the targeted centrifuges but did notice that its PCs were behaving suspiciously and had one examined by a Belarusian security firm, which found the attack software.

We do not suggest that remote search software will always fail, or even that it will do so most of the time. However, if deployed on enough machines—for example, when doing a large-scale search of bots—almost certainly it will cause problems on some of those machines. This creates several serious issues. The first is the possibility of doing further damage to victims’ computers, a situation that is likely to occur on occasion. Such damage could open law enforcement to embarrassment and costly legal action. Second, software failures could reveal the intrusion and thus compromise the investigation. Third, rules for executing search warrants are generally intended to minimize interference with the subject’s normal life, and malware that is overly intrusive—for example, by interfering with a targeted computer’s operation—might render the search invalid.

REMOTE SEARCH MALWARE: ONE SIZE DOES NOT FIT ALL

Botnets pose particular challenges to law enforcement. Botnet size is one problem; the fact that the machines
that have been taken over are victims’ devices is another. Law enforcement thus has sought to simplify criminal investigations through a single warrant that authorizes the search of multiple machines participating in a botnet.

To meet this objective, the proposed Rule 41 changes suggest employing “a common scheme” by law enforcement to infect victim computers with malware. From a technical standpoint, this is dangerous because such a scheme could easily go out of control in mass searches. Current botnet technology is generally simple: the malware used to control a given botnet is essentially identical on all victims’ machines, and it is relatively easy to know where to find it and how to disable it. However, botnet malware could become far more sophisticated in the future—in particular, it could be configured in multiple and unpredictable ways. The proposed rule changes focus on current criminal practice, not on how technology is likely to evolve. As such, “a common scheme” to infect victim computers with malware is probably doomed to fail. Examples such as Stuxnet show that malware must be carefully tailored to target devices to prevent collateral damage to other parts of the machine—or to other systems should the malware escape the target computer.

LOCATION AND JURISDICTION COMPLEXITIES

The Fourth Amendment requires that warrants “particularly describe[ ] the place to be searched,” but that can be difficult with remote computer searches. In addition to the legal complexity of determining from which judicial district a valid warrant may be issued, identifying a computer’s location often is not easy, even if its IP address is known.

IP geolocation techniques attempt to map IP addresses to locations. This can be done using the WHOIS protocol to query domain name and IP registration databases (limited in value since many sites use a third party as host), Internet topology, or even human inference—for example, by examining a webpage’s language. Such techniques are suitable for some purposes but can be frustrating for law enforcement because IP geolocation information is frequently, and sometimes undetectably, incorrect. For example, because many cellular service providers use carrier-grade network address location (NAT) technology to conserve address space, IP geolocation information for smartphones might be incorrect. Virtual private networks (VPNs), which use tunneling protocols and encryption to protect user security and privacy, create another type of problem, and Tor uses onion routing expressly to obscure users’ IP address—and thus their geolocation.

We do not address the mostly legal question of the “fruits” of a remote search conducted in what turns out to be the location other than where authorized, except to note that this probably occurs fairly frequently. The fact that a target machine might be in another country compounds the problem, necessitating greater coordination of US law enforcement with their foreign counterparts on the legal issues surrounding remote search—perhaps formalized in something akin to a mutual legal assistance treaty. In the wake of Edward Snowden’s revelations about the National Security Agency spying on foreign governments and citizens, it is unlikely that the proposed changes to Rule 41 would be universally accepted by other nations. Law enforcement must be sure that American criteria for remote search are valid abroad. Some
countries, in fact, prohibit and prosecute foreign searches. For example, Russia has charged an FBI agent who conducted a remote search of one of its citizens with hacking, and German courts have held that their constitution prohibits the practice.\(^{15}\)

**PROBLEMS WITH SURREPTITIOUS REMOTE SEARCHES**

With the exception of national security investigations that do not result in evidence used in court, under US 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 90 days after conclusion of the wiretap. Yet the surreptitious remote searches being proposed in the Rule 41 changes conflict with the openness lying at the heart of US jurisprudence.

Surreptitious collection of evidence by compromising computers (and computerized devices such as mobile phones) 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 can be expected to continually evolve, often quite rapidly, to adapt to new target devices as well as to circumvent new countermeasures. Law enforcement naturally resists disclosing the specific tools and techniques it uses to obtain access to target systems so it can deploy them against other targets in the future, but this goal must be balanced against several risks.

First, to meaningfully analyze the scope of an authorized intrusion and the dangers of exceeding that scope, judges—who might have little or no technical training—must understand certain aspects of the specific technology to be employed. This is especially important when, as is often the case, the target device is used for real-time communication (whose content is covered by wiretap statutes) as well as for processing and storing information.

In addition, a criminal defendant will often request detailed technical information about how a remote search was conducted to raise challenges as to whether it improperly exceeded legal authorization. Forensic analysis of a hacked computer is difficult,\(^{16}\) and bugs in the examination process can affect the results. The Federal Rules of Evidence state that “the [forensic] expert may be required to disclose those facts or data on cross-examination” and that expert testimony must be “the product of reliable principles and methods.”\(^{17}\) It is impossible to verify that the conditions were met without making the tools that extracted that data available to the defense.

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 methods used. Other fields of forensic examination have been plagued by bad science;\(^{18,19}\) the best assurance of justice in the US court system is the adversarial process.

US courts have not always recognized the importance of defendants’ ability to view source code—for example, of breathalyzers used to help secure drunk driving convictions.\(^{20,21}\) However, we believe that as much information as possible about the technology used to conduct a remote search should 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.

**BREAKS IN THE CHAIN OF CUSTODY**

Just as US jurisprudence requires transparency, evidence must be uncorrupted: a defendant can challenge the authenticity of prosecution evidence if procedures are not properly followed or discrepancies are found. It is much harder to maintain the integrity of evidence during a remote search than in a search of a physically seized computer. Normal forensic procedures require that all analysis be done on a copy of data from seized hardware, such as a disk drive. This protects the original disk from accidental corruption—for example, opening a file can change the “last accessed” date—and makes it easier to examine memory blocks. The original disk and image file are cryptographically hashed to show authenticity, but that won’t be useful in a remote search.

A difference of a single bit anywhere in system input will, of course, change hash output (that is, indeed, part of the usefulness of hashing). However, 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 system image through normal
operating system activities, effectively making the file system a moving target. Current technology simply does not match evidentiary needs, and this is not likely to change in the foreseeable future. Making an image copy of a drive can take hours under ideal conditions and with the owner’s cooperation. Copying a nontrivial-size disk is generally infeasible for surreptitious remote search; disks are too big and communications lines are too slow. For example, copying a 2-Tbyte 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, and so on. The proposed Rule 41 changes ignore the difficulty of creating image copies, despite its importance.

**LACK OF PARTICULARITY**

Sometimes a difference in scale can be a difference in kind. We believe that is the case with botnet investigations. In most crimes there is a single victim, or perhaps a handful of victims, but a botnet can potentially infect millions of machines. Allowing the broad seizure of information from so many devices simply because they were the victims of computer crime seems wrong. We therefore suggest an explicit requirement that all remote search software be configured extremely narrowly when used on victim computers.

As noted earlier, the Fourth Amendment requires that a warrant specify the place to be searched. The meaning of this requirement in electronic searches remains the subject of continuing constitutional debate, and is especially thorny as it relates to mass remote searches, where the identity of the computers being examined is unclear. 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” is by no means clear under the proposed Rule 41 changes.

Because remotely examining a victim computer for botnet malware subjects a person not suspected of any wrongdoing to an unwitnessing search, the reasons for such a search should be limited to demonstrating that a crime has indeed taken place, finding pointers to the individual responsible for the botnet, and ascertaining the extent of the damage. There are two cases here, depending on whether or not the botnet’s behavior is understood.

When dealing with known botnets, law enforcement should be able to ascertain exactly how the malware in question works. Through so-called “honeypots,” carefully monitored machines instrumented to become infected by mimicking the behavior of other victim systems, the security community has had great success locating botnets’ command-and-control nodes without hacking into victim computers. Honeypots are less intrusive than remote computer searches and should be used first in criminal investigations. Even if this approach does not yield enough evidence to prove a botnet operator’s guilt beyond a reasonable doubt, evidence will likely be in a very few, easy-to-locate places. It is feasible to construct search software that looks precisely and solely for the necessary indicia rather than rummaging through an entire computer.

In other botnet investigations, the necessary evidence might not lie in a single, easy-to-examine location. A sophisticated attacker could, for example, split a contraband file into several pieces and stash them in different places on a machine using Shamir’s Secret Sharing. Such a scenario would likely require a thorough, less-automated forensic examination.

THE BROAD SEIZURE OF INFORMATION FROM MILLIONS OF DEVICES SIMPLY BECAUSE THEY WERE VICTIMS OF COMPUTER CRIME SEEMS WRONG.

The complexity of a search involving many locations on a victim’s machine means it is advisable to inform the victim prior to downloading malware to track the attack. Given the attack’s sophistication and the extensive damage it might cause, most victims would likely be willing to cooperate with law enforcement—once it had properly authenticated itself—to rid their system of the infection.

An alternative to searching a victim’s machine for evidence is to consult the victim’s ISP. Using their ability to map IP addresses to billing data, some ISPs have experimented with notifying subscribers whose machines appear to be infected by a botnet; the ISPs use their knowledge of a machine’s IP address to associate this with a billing address and thus can send an out-of-band mailing. ISPs
could go one step further and detect infections in subscribers’ machines, though this raises privacy issues that deserve a thorough policy vetting.\textsuperscript{25}

We therefore suggest that any Rule 41 changes include language mandating narrow remote searches, especially of victim machines. Failure to do so could result in phishing attacks by criminals turning into fishing expeditions by law enforcement.

**TARGET NOTIFICATION CHALLENGES**

Search warrants generally require notifying the target, including a receipt for any items seized (Rule 41(f)(1)(C)). The proposed Rule 41 changes note that this is difficult in remote computer searches;\textsuperscript{7} we feel it is much harder than indicated. We can think of only four feasible mechanisms for notifying the target of a search: a file left on the target’s computer, an email message, a popup window, or a physical letter. All are problematic, especially for mass searches.

Users might not notice a file left on their computer and, more importantly, would have no way to determine the file’s authenticity or provenance. A hacker could easily deposit files that looked just like the real ones, including a malicious URL to click on “to acknowledge the message.” Email, of course, would pose similar problems. The FBI itself has warned of malicious spam email purporting to be from them (www.fbi.gov/scams -safety/e-scams). There are, at least in theory, technical solutions involving digitally signed messages and a public-key infrastructure, but experience suggests that these would only work with highly trained users.

Hackers can be expected to abuse popup messages generated by law enforcement, just as they have done so with similar mechanisms to serve ads. Furthermore, there is little evidence that people would pay attention to such boxes.

Physical mail might be more reliable but could be time-consuming and expensive. It also would not deal with the problem of unknown search targets. An extensive remote search might yield a physical address but would be extremely intrusive.

The proposed Rule 41 changes obligate law enforcement to make “reasonable efforts” to notify remote search targets, and, given the technical difficulties, we cannot improve upon this standard. However, we think such efforts will fail in too many cases and suggest that judicial authorities develop and, after suitable public comment, enact regulations on how notification will work in practice.

**A POLICY DILEMMA**

The proposed rule changes imply 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 numerous policy issues that will need to be addressed by the courts and lawmakers. We have recently discussed some of these issues elsewhere.\textsuperscript{26,27}

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 system “back door,” 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. The computer software, hardware, and devices used by criminals (and from which evidence is collected) are used by millions of innocent citizens to store, process, and communicate the most important and sensitive details of their lives and business operations. This means that any flaw used by law enforcement for laudable evidence collection purposes also represents a risk to innocent people. The use of vulnerabilities to catch criminals must be balanced against the need to protect citizens from criminals who might exploit the vulnerabilities themselves.\textsuperscript{27}

**RECENT DEVELOPMENTS**

The proposed Rule 41 changes were drafted by the Judicial Conference’s Advisory Committee on the Federal Rules of Criminal Procedure, which is composed of a cross-section of criminal law experts including judges, attorneys, a law professor, and an assistant attorney general from the Department of Justice (DoJ). The changes were submitted to the public for comment on 15 August 2014, with responses due by 17 February 2015.\textsuperscript{2} Many prominent organizations including Google, the EFF, the American Civil Liberties Union, the Center for Democracy & Technology, and the Electronic Privacy Information Center raised some of the same points discussed here and in our own public comments (see the sidebar), prompting rebuttals from a high-ranking DoJ official.\textsuperscript{28} Public hearings were held on 5 November 2014 in Washington, DC.\textsuperscript{29}

Objections notwithstanding, the changes—with only minor revisions—were approved 11–1 by the Advisory Committee on 16 March 2015\textsuperscript{30} and
A SAMPLING OF PUBLIC COMMENTS ON THE PROPOSED RULE 41 CHANGES

The proposed amendment substantively expands the government’s current authority under Rule 41 and raises a number of monumental and highly complex constitutional, legal, and geopolitical concerns. Google urges the Committee to reject the proposed amendment and leave the expansion of the government’s investigative and technological tools, if any are necessary or appropriate, to Congress.

—Richard Salgado, director of Law Enforcement and Information Security, Google

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

—Nathan Fred Wessler and colleagues, Speech, Privacy and Technology Project, American Civil Liberties Union

CDT recognizes that law enforcement faces legitimate challenges in determining how to issue search warrants for computers with concealed locations in investigations. We also recognize the negative impact of malware, botnets, and illicit online activities undertaken using anonymity techniques that may obfuscate location. However, we believe the solution to this complex problem should arise through public and legislative debate. The proposal has significant implications for open legal and policy issues, as well as broad technological consequences affecting the privacy of computer users worldwide. We believe the Judicial Conference should withdraw the proposed changes to Rule 41 from its rulemaking process, and that the proposal should instead be deliberated in Congress.

—Joseph Lorenzo Hall, Center for Technology & Democracy

The technologies involved are rapidly developing and poorly understood, as are the existing international legal norms that apply to them. It is critical that these issues be approached with comprehensive deliberation (between technologists, policy makers and lawyers) that looks beyond the operational frame...As it stands, the proposed amendment allows the FBI to use a wide array of invasive (and potentially destructive) hacking techniques where it may not be necessary to do so, against a broad pool of potential targets that could be located virtually anywhere.

—Ahmed Ghappour, director of the Liberty, Security & Technology Clinic, University of California, Hastings College of the Law

Allowing Law Enforcement the ability to distribute malware, pierce anonymity and/or circumvent encryption technologies sounds like a valiant effort to catch criminals, but that's assuming the persons acting that way ARE, in fact, criminals. I submit law abiding, peaceful citizens perform these same actions as part of being regular citizens on the Internet. Agencies should target individuals, not practices...I urge you to dismiss this proposal. For the same reasons the Supreme Court disallowed using technologies to look inside your home from outside, allowing technologies to look through your firewalls is just as intrusive and paves the way to negating the 4th amendment.

—Former FBI agent

COMMUNICATIONS AND PRIVACY UNDER SURVEILLANCE

unanimously approved by the Standing Committee on 28 May. The Judicial Conference approved the amended rule on 17 September 2015 and forwarded it to the Supreme Court, which has until 1 May 2016 to review it. If the Court approves the amended rule, Congress has seven months to reject, modify, or defer it. Opposition continues, but if Congress does not act the rule change will go into effect on 1 December 2016.

SECURELY CONDUCTING LAWFUL SURVEILLANCE

Law enforcement’s primary role is solving crimes, with prevention of crime typically a secondary goal. This focus can be problematic for computer security, which generally focuses on prevention. When investigating particular crimes or classes of crimes, it is difficult to see beyond the immediate goal of catching those responsible. But short-term solutions—such as remotely implanting malware on numerous machines across multiple jurisdictions—can have long-term adverse implications. While we recognize that the policy questions raised by the recommended Rule 41 changes might be beyond the scope of the proposal itself, it is imperative that these questions be addressed comprehensively, especially the impact on cybersecurity. A piecemeal approach such as that offered here is likely to leave society more, rather than less, vulnerable.

In our view, the current proposal has not been thoroughly vetted by computer security professionals. From this perspective, we therefore make the following recommendations with respect to conducting remote searches.

› A single warrant should not be used to conduct multiple simultaneous searches on victims’ computers. Blanket warrants cover far too many machines, without the necessary specificity; they also pose a great risk of damaging some of them.

› A warrant issued to search a victim’s computer should precisely specify the area of the computer that is to be searched.

› Guidance to law enforcement, and perhaps Rule 41 itself, should stress the potentially serious repercussions of remote searches of computers located in other countries. Except in extremely serious cases, such searches should only be conducted with the host country’s approval.

› To satisfy the legal requirements of target notification, law enforcement should be provided with guidelines on what mechanisms to use and under what circumstances, as well as when such requirements might be waived. The DoJ should also engage the technical community to devise better notification mechanisms.

Depositing remote search malware on machines—particularly those belonging to people not suspected of any wrongdoing—is a very tricky business and should never be attempted lightly. Without sufficient regard for
the technical as well as legal issues involved, law enforcement could end up doing more harm than good.

To our knowledge, there is no explicit statutory authority for law enforcement to remotely hack into computers. Given the intrusiveness of such activities, and the risks of both damaging innocent victims’ computers and compromising criminal investigations, the proposed Rule 41 changes authorizing mass surreptitious searches raise numerous important constitutional and practical issues that should be addressed comprehensively. As we have argued at greater length elsewhere,27 Congress should carefully consider any investigative methods that involve hacking into systems. The legislative process is better suited to address issues impacting policy than the judicial rule-making process.

Although this article has focused on a specific proposal for criminal investigations that applies only to US law, the issues raised 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 stakes are global.

ACKNOWLEDGMENT
The authors thank Matthew Green for many helpful comments on an earlier draft of this article.

REFERENCES
18. S.S. Hsu, “FBI Admits Flaws in Hair Analysis over Decades,” The
COMMUNICATIONS AND PRIVACY UNDER SURVEILLANCE

ABOUT THE AUTHORS

STEVEN M. BELLOVIN is the Percy K. and Vida L.W. Hudson Professor of Computer Science at Columbia University’s School of Engineering and Applied Science and cochair of the Cybersecurity Center at the university’s Data Science Institute. He works on security, privacy, and related public policy issues. Bellovin has a PhD in computer science from the University of North Carolina at Chapel Hill. He is a member of ACM. Contact him at smb@cs.columbia.edu.

MATT BLAZE directs the Distributed Systems Laboratory at the University of Pennsylvania, where his research focuses on security, privacy, and scale in computing and communications systems. Blaze has a PhD in computer science from Princeton University. Contact him at blaze@cis.upenn.edu.

SUSAN LANDAU is a professor of cybersecurity policy at Worcester Polytechnic Institute, where her research focuses on cybersecurity, privacy, and public policy. She was previously a senior staff privacy analyst at Google and a Distinguished Engineer at Sun Microsystems. Landau has a PhD from MIT and is a member of IEEE, ACM, the American Association for the Advancement of Science, the American Mathematical Society, and the Association for Women in Mathematics. Contact her at susan.landau@privacyink.org.


Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.