THE CONVERSATION
Academic rigor, journalistic flair

# Don’t let cybercriminals hide from the FBI

May 8, 2016 8.49pm EDT

Criminals who hide their computers shouldn't go free. Computer criminal via shutterstock.com

Imagine that a criminal investigator has identified one or more computers that are part of ongoing criminal activity. Unfortunately, the people operating these computers are hiding them. The machines could be anywhere in the world, using anonymous email or tools like Tor to conceal their location.

The investigator also has a tool, a carefully engineered piece of software, which she calls a "Network Investigatory Technique," or NIT, that will cause a targeted computer to reveal itself. Once she sends the software to the computer she's investigating, it will reply with a message saying, "I am at this location." The rest of the security world calls the NIT "malicious code" ("malcode" for short) and deploying it "hacking," because the software exploits a vulnerability in the target's computer, the same way a criminal would.

Federal court rules currently say she can use this tool only if she gets an electronic search warrant from a judge. But the computer could be anywhere: to which court should she go to get the warrant?

This is not a hypothetical problem. Online investigations face this problem all the time, when tracking down fraudsters or those issuing threats using anonymous emails, botmasters who have compromised thousands of computers around the planet or purveyors of drugs or child pornography. The current federal rules of criminal evidence (in particular a section known as Rule 41) require investigators to seek warrants from a magistrate judge in the federal court district where the target computer is located.

But if investigators don't know where in the country, or indeed the world, the computer is, the existing rules effectively dictate that there is no judge who could approve a warrant to actually find out its specific location. In essence, the rule is, "The investigator can get a warrant to hack these computers to reveal their location only when she knows where they already are." That rule might have made sense before the digital age, but in today's digital world it forces an end to promising investigations.

## Author

**Nicholas Weaver**
Senior Researcher, Networking and Security, International Computer Science Institute, University of California, Berkeley

## Making an improvement to the rule

At the request of the FBI, the U.S. Supreme Court has proposed changing the rule to allow any magistrate judge in the country to approve an electronic search warrant under one of two conditions: either the targets are using technological tricks to conceal their location, or the crime being investigated involves a mass break-in, compromising computers in at least five separate federal judicial districts. Congress has until December to review the changes.

The Electronic Frontier Foundation has an excellent summary of the civil liberties objections. They include the potential for the government to seek warrants from sympathetic judges, who might not closely scrutinize requests, or who might accept more spurious definitions of concealment by "technological means," thereby undermining the law's protections. They also fear that the FBI may seek to hack computers outside the U.S., and that searches could reach beyond criminals' equipment and involve innocent people's computers that had been taken over by wrongdoers.

I am in the minority among my civil liberties colleagues, but I believe this change is necessary, reasonable and proportional. If a computer search would qualify for a warrant if its whereabouts were known, why should simply hiding its location make it legally unsearchable?

The need for these types of searches is not theoretical. The "Silk Road" case is a prime example. This website, hidden through Tor to make it supposedly impossible to locate, acted as an online eBay for drugs. Until the FBI obtained the server's location, investigators were stumped, unable to identify the person, called "Dread Pirate Roberts," who was operating the site.

Once agents identified the computer, all the pieces fell into place, quickly leading to the arrest and subsequent conviction of Ross Ulbricht. The FBI almost certainly hacked the server but never bothered to get a warrant to do so. This was a decision which, but for a bizarre tactical choice by the defense, might have lost the case. Under the revised Rule 41, it would be straightforward to obtain a warrant to hack the server: there was certainly enough probable cause.

## When the FBI takes over a criminal site

Another large set of cases involve child porn distributed through Tor. The FBI routinely takes over websites that do this, and may for a few days or even a couple of weeks deliver surreptitious software to visitors, software that tracks their location, before taking the site down for good. In cases involving notorious sites like PedoBook and Playpen, the FBI may hack hundreds or thousands of computers with a single warrant.

The FBI's experience in taking over the Playpen server is a particularly good example of the need for a revision to Rule 41. The warrant request established probable cause for each computer to be hacked; the malcode identified individual visitors for prosecution (and associated their identities with their user names on the site).

The FBI's malcode itself was almost certainly reasonable, doing the minimum necessary to identify the target computer to authorities and no more. Even defense experts in a previous case acknowledged that the FBI's malcode both operated as advertised and did not exceed the scope of the warrant. However, almost all of the targeted computers were outside the federal court district where the FBI ran the captured Playpen server. As a result, this critical violation of the current Rule 41 may very well result in hundreds of pedophiles going free.

## Measured changes are appropriate

Hence the need for the measured changes proposed to Rule 41. It doesn't enable the FBI to get a warrant that lets the agency hack just anywhere. It applies only when the FBI can't determine where the targets are or when there are simply too many known targets that getting a warrant in every district would result in an explosion of paperwork without actually protecting anybody's rights. Because if people accept that the FBI should have the right to hack with a warrant and probable cause, extending this authority to enable hacking a computer in an unknown location represents only a small expansion in authority, not some vast overreach.

Despite some people raising concerns, it is also highly unlikely to affect U.S. diplomatic relationships. It's true that it the rule change could result in the FBI hacking systems outside the United States if the computer's location is hidden. But no matter their location, target computers aren't hacked until the FBI has shown probable cause they're involved in criminal activity in the United States. When this happens the FBI will do what it has done in previous cases like the Playpen case: notify local law enforcement of the evidence collected, and let that country's authorities take over.

Overall, the change to Rule 41 seems reasonable. It addresses a real-world problem, it comes into play only when a computer's location is unknown or the targets are too numerous, and does not reduce the key protection and oversight that already limits such hacking: the need for probable cause presented for a judge's approval and search warrant which specify with particularity what the hacking should search for (with the ability to enforce these restrictions in the code).

**Cybersecurity** **Malware** **Cybercrime** **US Supreme Court** **FBI** **Tor** **Civil liberties** **search warrants**