The Impact of the New Rule 41 on VPN Users

John Norris Technology Researcher ⋮ 6-8 minutes ⋮ Invalid Date

Rules governing how U.S. law enforcement can conduct electronic searches and mass surveillance are on the brink of change. Privacy advocates see many red flags and are speaking out in a last-ditch effort to stop the Fed's designs. Share

A major debate is currently raging in the U.S. over changes to a rule that dictates how law enforcement can perform electronic searches on suspects' computers. In this FAQ, we dive deep into Rule 41, the upcoming changes, and how this will potentially affect VPN customers in the U.S. and abroad. Click here to see what you can do to stop the change.

What Is the Current Rule 41?

Rule 41 of the Federal Rules of Criminal Procedure stipulates the procedures law enforcement must follow to perform searches and seizures. In its current form, the rule says magistrate judges can only authorize electronic searches within their own jurisdictions.

What Are the New Changes?

The U.S. Supreme Court has approved a change in Rule 41, providing judges across the country with the authority to issue warrants for remote electronic searches outside their district. The judge can also grant a warrant to perform "network investigative techniques" (i.e. hacking) on suspects' computers, even if the suspect uses tools such as VPNs or Tor browsers to hide his/her identity anywhere in the world.

Why Is the U.S. Government Seeking the Changes?

The U.S. Justice Department (DOJ) has pushed for the rule change since 2013. Painting it as a procedural tweak, the changes would enable FBI agents to seek a warrant from one judge to perform an electronic search, even if the target has computers in separate states and/or countries.

"This rule change would permit agents to go to one federal judge, rather than submit separate warrant applications to each of the 94 federal districts," the DOJ told Politico. "That duplication of effort makes no sense."

The DOJ also says the protections offered by the 4th Amendment of the Constitution (protection against "unreasonable" searches and seizures) are not threatened. The department sees the issue as a matter of venue streamlining; law enforcement agents still need to prove probable cause to get a judge to issue a warrant, even if the warrant's power is increased. In addition, the rule only applies in situations when a suspect can be shown to be using technology to conceal the location of his or her computer or for an investigation into a network of hacked or infected computers, such as a botnet.

In application, the rule changes would help the FBI avoid negative rulings like recent decisions in Massachusetts and Oklahoma. In these cases, important evidence against child pornographers was dismissed because it was gained through Tor exploits on computers out of the warrants' jurisdictions.

Will the New Rules Affect Internet Users Outside the U.S.?

Indeed, the recently approved rule change will grant the FBI the authority to seek authorization from a single judge to search and seize any computer belonging to a suspect located anywhere in the world if they are found to be utilizing privacy tools.

Do the Rule Changes Just Affect Criminal Suspects?

No, it has the potential to impact innocent users as well. Thanks to the FBI's efforts to clean up botnets, a warrant issued under the new rule could give access to victims' computers as well. As the Electronic Frontiers Foundation (EFF) said:

"Victims of malware could find themselves doubly infiltrated: their computers infected with malware and used to contribute to a botnet, and then government agents given free rein to remotely access their computers as part of the investigation."

When Will the Rule 41 Changes Go into Effect?

Unless the U.S. Congress takes legislative action, the rule changes will go into effect in December of 2016.

And there is a chance Congress will act. Sen. Ron Wyden (D-Oregon) recently said:

Sen. Ron Wyden; Source: http://www.finance.senate.gov/

"These amendments will have significant consequences for Americans' privacy and the scope of the government's powers to conduct remote surveillance and searches of electronic devices."

In addition, powerful tech companies are not sitting still. Google issued a statement, saying:

"The proposed change threatens to undermine the privacy rights and computer security of Internet users. For example, the change would excuse territorial limits on the use of warrants to conduct 'remote access' searches where the physical location of the media is 'concealed through technological means.'"

In mid-May, Wyden proposed legislation called the *Stopping Mass Hacking Act*. This one-page bill seeks a Senate vote to block the changes ahead of the December 1 deadline. The bill's co-sponsors are a mix of Democrats and Republicans, including Rand Paul (R-Ky.), Steve Daines (R-Mont.), Tammy Baldwin (D-Wisc.) and Jon Tester (D-Mont.).

By late May, Congress members introduced a companion bill in the House of Representatives. To succeed, the opposition will need a majority vote of both houses in Congress as well as President Obama's signature.

What Do the Rule 41 Changes Mean for VPN and Tor Users?

On the surface, the impending changes do not impact the protections VPN services and the Tor browser offer general users. However, users employing these services to perform illegal actions or hide from the U.S. government will be at greater exposure risk.

Also, if the opposition to the new rules fails, the government will gain an ability to gather data about innocent users without their knowledge. The DOJ denies it will do so, but this topic makes the changes worthy of more debate.

Are Other Countries Enacting Similar Legislation?

Yes. In the UK, the Investigatory Powers Bill, also knowns as "The Snooper's Charter," has almost finished its progress to royal assent. The draft bill has generated significant debate about balancing mass surveillance protections and privacy with the needs of law enforcement to gain targeted access to information during investigations.

Leaving on a Funny Note

The *Stopping Mass Hacking Attacks Act* is generally short-handed to the SMH Act. Hopefully, innocent computer users won't be SMH after the FBI accesses their private information.

What Can You Do?

Share this article, or this one, on Facebook and Twitter.