



Written by [Joe Wolverton, II, J.D.](#) on November 9, 2014

FBI Covertly Requests Backdoor Access to Electronic Data Through Procedural Rule Change

It should come as no surprise that the FBI is trying to backdoor its way into greater computer surveillance power.

The Obama Justice Department has asked that a committee be empaneled to amend Rule 41 of the Federal Rules of Criminal Procedure (FRCP).

Section (b) of that provision begins:

Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:

- (1) a magistrate judge with authority in the district — or if none is reasonably available, a judge of a state court of record in the district — has authority to issue a warrant to search for and seize a person or property located within the district;
- (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed....

In plain terms, judges can only issue search warrants within the districts where they have jurisdiction. The FBI wants this restriction removed.

Specifically, the FBI wants a judge to be able to issue an electronic surveillance warrant authorizing the feds to search the contents of a computer, regardless of where that computer is physically located.

According to documents obtained by *The New American*, the FBI's proposal would amend Rule 41 by adding the following language:

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 electronically stored information located within or outside that district.

And:

For a warrant to use remote access to search electronic storage media and seize electronically stored information, the officer must make reasonable efforts to serve a copy on the person whose property was searched or whose information was seized. Service may be accomplished by any means, including [reliable]* electronic means, reasonably calculated to reach that person [ALT: any person whose information was seized or whose property was searched].** [Upon request of the government, the magistrate may delay notice as provided in Rule 41(f)(3).]

As the *National Journal* explains:

Law-enforcement investigators are seeking the additional powers to better track and investigate





Written by [Joe Wolverton, II, J.D.](#) on November 9, 2014

criminals who use technology to conceal their identity and location, a practice that has become more common and sophisticated in recent years. Intelligence analysts, when given a warrant, can infiltrate computer networks and covertly install malicious software, or malware, that gives them the ability to control the targeted device and download its contents.

Something interesting about the *National Journal's* summary of the FBI's request is its use of the word "criminal" to describe the owner of the computer that the government wants to track and tap.

In the United States, a person is not a "criminal" until he has been subject to the due process of law, specifically: a charge of committing a crime, a hearing by an impartial tribunal on the merit of those charges, an opportunity for the accused to answer those charges, and finally, conviction of having committed the crime.

Due process as a check on monarchical power was included in the Magna Carta of 1215. This list of grievances and demands codified the king's obligation to obey written laws or be punished by his subjects. Article 39 of the Magna Carta says: "No freemen shall be taken or imprisoned or disseised [dispossessed] or exiled or in any way destroyed, nor will we go upon him nor send upon him, except by the lawful judgment of his peers or by the law of the land."

Over the years, the Magna Carta was occasionally revised and amended. In 1354, the phrase "due process of law" appeared for the first time. The Magna Carta as amended in 1354 says: "No man of what state or condition he be, shall be put out of his lands or tenements nor taken, nor disinherited, nor put to death, without he be brought to answer by due process of law."

This fundamental restraint on the royal presumption of the power to lop off heads on command was incorporated by our Founders in the Bill of Rights, particularly in the Fifth Amendment that says in relevant part: "No person shall ... be deprived of life, liberty, or property, without due process of law."

That is the first of two constitutional objections to the FBI's secret plan to use a committee decision to bypass not only the Constitution, but also the exclusive legislative authority that that document grants to Congress.

Fortunately, there are those who are working to thwart the Obama administration's plan to deny due process and to grant the government greater (unconstitutional) access to computers and other electronic devices. Last Wednesday, witnesses testified in opposition to the scheme at a hearing conducted by the Advisory Committee on Criminal Rules, a group of legal experts tasked with considering proposals for changing the federal rules of criminal procedure. As quoted in the *National Journal* piece:

"I empathize that it is very hard to get a legislative change," said Amie Stepanovich, senior policy counsel with Access, a digital-freedom group. "However, when you have us resorting to Congress to get increased privacy protections, we would also like to see the government turn to Congress to get increased surveillance authority."

Stepanovich also warned that the rule change could be applied to large computer networks, such as botnets, and breach the privacy of all users communicating via that network. While botnets, which can sometimes involve millions of computers, are often viewed as sinister, not all of them are, Stepanovich said.

Others noted that the amendment could have dramatic and unintended consequences on foreign relations. Surveillance orders granted for computers located in another country or where the location is unknown would lack the Fourth Amendment's protection against unreasonable search



Written by [Joe Wolverton, II, J.D.](#) on November 9, 2014

and seizures, said Ahmed Ghappour, a computer law professor at the University of California's Hastings college of law.

"It's like turning on a switch, but instead of turning on a faucet, it's like turning on a fire hose," Ghappour, added, noting that the rule change could usher in unprecedented powers to spy on foreign computer networks.

It is likely that the impetus for this increased pressure to pry into the electronic "papers and effects" of suspected criminals was the move by tech giants — particularly Google and Apple — to protect the data stored on customers' devices from the prying eyes of the agents of the federal surveillance state.

At a conference on counterterrorism held in New York City last Monday, director of the FBI James Comey demanded that Google, Apple, and other Silicon Valley companies help the feds carry out criminal investigations, specifically by granting the government access to consumer data — email, texts, tweets, etc. — if such requests are received.

Comey made a similar demand during a closed-door meeting held last week at the White House.

"In one way or another, our entire lives — our social lives, our work lives — reside online and on these devices," Comey said during his remarks at the conference. "And that's a great thing. But that's also where the bad guys are."

Again, what the federal government fails to understand is that their word is not the law. The Constitution is the law and that document requires that a warrant be issued, and that such a warrant be "supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Furthermore, "bad guys" are not "bad guys" until the due process of law has determined them to be such. Until that time, they are just citizens whose rights must be protected if we are to remain a free republic ruled by law rather than the edicts of would-be despots.

The Advisory Committee on Criminal Rules will meet again in Nashville, Tennessee, on January 30, 2015. The group is scheduled to discuss the FBI's proposed amendment to Rule 41.

Joe A. Wolverton, II, J.D. is a correspondent for The New American. Follow him on Twitter @TNAJoeWolverton.



Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.

[Subscribe](#)