

THE RUTHERFORD INSTITUTE

Post Office Box 7482
Charlottesville, Virginia 22906-7482

JOHN W. WHITEHEAD
Founder and President

TELEPHONE 434 / 978 - 3888
FACSIMILE 434/ 978 – 1789
staff@rutherford.org
www.rutherford.org

May 5, 2016

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, D.C. 20510

**Re: Proposed Amendments to Federal Rule of Criminal Procedure 41 /
Authorization of Remote Access Searches**

Dear Senator Wyden:

The Rutherford Institute¹ would like to offer its assistance in challenging proposed changes to Federal Rule of Criminal Procedure 41 (regarding applications for search warrants).

These proposed changes to Rule 41 threaten to further erode individual privacy by giving law enforcement and intelligence agencies the power to remotely hack into personal computers and mobile devices,² implant malicious software on computers, and rummage through the personal contents of those computers, even if their owners are not suspected of criminal activity.

If approved by Congress, the proposed changes to Rule 41 would constitute a significant expansion of the surveillance power the government may use to spy on its citizens.

This expansion must be resisted.

¹ The Rutherford Institute is a national nonprofit civil liberties organization dedicated to the defense of constitutional freedoms.

² By freeing government agents of the obligation to show that the computer or other electronic storage media they want to search is located in the district where the warrant application is made, the suggested amendments to Rule 41(b)(6) grant government investigators from anywhere in the United States the ability and legal authority to conduct remote access surveillance of private and sensitive information located on computers and mobile devices anywhere in the world.

These proposed Rule 41 changes present surreptitious and invasive governmental threats to the privacy of citizens by:

- **Subjecting innocent persons to hacking and indiscriminate searches:** The proposed changes allow remote surveillance of computers that are suspected to have been damaged without authorization by a criminal scheme³ to distribute malware or to gain unauthorized access to the computer.⁴ Thus, investigators would be allowed to hack into computers and other devices which they suspect have been infected by a virus or malware, which would apply to countless computers and devices. Moreover, the proposed change would allow investigators to conduct remote surveillance of the infected computer or device *even if the owner is not suspected of criminal activity*. Additionally, the Committee Notes to the proposed change make clear that computers that have been the *targets of criminal activity* would be subject to a search under the amended Rule. This proposed change to Rule 41 opens the door to unprecedented government access to the personal information of innocent people.
- **Failing to establish any time limits on remote surveillance:** The remote surveillance the government seeks to expand involves the surreptitious installation of software on a computer which allows the government unlimited access to the computer.⁵ However, nothing in the changes to Rule 41 imposes a limit on how long the software may remain on the target computer or requires the government to remove or delete the software once any investigation is complete. Once the software is on the computer, even a computer of an innocent person, it is subject to ongoing remote surveillance by the government. The prospect of this kind of ongoing government access to the digital information of citizens undermines significant constitutional protections and must not be allowed.
- **Not requiring government officials to notify citizens that a search has been or will be conducted:** The Fourth Amendment generally requires that the targets of a search under a warrant be informed that their property and

³ 18 U.S.C. § 1030(a)(5).

⁴ The proposed rule, Fed. R. Crim. P. 41(b)(6)(B), applies to “protected computers.” This is defined in 18 U.S.C. § 1030(e)(2) as and computer used in or affecting interstate commerce, and so would include virtually any computer that is connected to interstate communications facilities.

⁵ As described in one case which found such surveillance illegal, “[o]nce installed, the software has the capacity to search the computer’s hard drive, random access memory, and other storage media; to activate the computer’s built-in camera; to generate latitude and longitude coordinates for the computer’s location; and to transmit the extracted data to FBI agents within this district.” *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013).

The Honorable Ron Wyden

May 5, 2016

Page 3

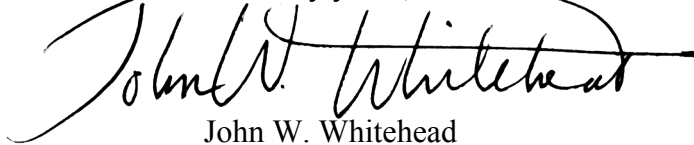
privacy is being invaded by the government.⁶ However, the proposed Rule 41 changes fail to require that notice of the search and seizure be given to the targeted citizen or entity at *any* time, much less at or before the time of the search. By relying on a surreptitious invasion of privacy in order to advance remote surveillance,⁷ this will only foster the kind of secret surveillance of citizens the government has been moving toward over the last decade.

Contrary to the government's claims as expressed in the Advisory Committee's report, the proposed changes to Federal Rule of Criminal Procedure 41 are not simply procedural in nature, affecting only the manner in which remote surveillance is authorized. Absent the authority to issue a remote surveillance warrant without regard to the presence of the computer within the district, the government is unable to conduct this kind of search because of the anonymity provided by technology.

Despite the U.S. Supreme Court's rubberstamped approval of the government's requested expansion of its surveillance powers, the proposed changes to Rule 41 fly in the face of the fundamental principles of individual security and privacy embodied in the Fourth Amendment and must be disallowed.

To this end, we look forward to working with you to ensure that these grave threats to citizen privacy do not come to pass.

Sincerely yours,

A handwritten signature in black ink that reads "John W. Whitehead". The signature is written in a cursive style with a long horizontal flourish extending to the right.

John W. Whitehead
President

⁶ *Wilson v. Arkansas*, 514 U.S. 927 (1995) (affirming that the Fourth Amendment generally requires officers knock and announce themselves before entering a premises to search).

⁷ *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d at 755.