June 2016

The Honorable Charles Grassley
Chairman
United States Senate Committee on the Judiciary

The Honorable Patrick J. Leahy
Ranking Member
United States Senate Committee on the Judiciary

The Honorable Bob Goodlatte
Chairman
House of Representatives Judiciary Committee

The Honorable John Conyers, Jr.
Ranking Member
House of Representatives Judiciary Committee

Chairman Grassley, Ranking Member Leahy, Chairman Goodlatte, Ranking Member Conyers, and esteemed members of the Senate and House Committees on the Judiciary:

We write today to urge you, as the committees of jurisdiction, to hold hearings on the pending change to Rule 41 of the Federal Rules of Criminal Procedure. The U.S. Supreme Court recently approved a change to Rule 41 that will expand the use of sophisticated hacking tools, euphemistically known as Network Investigative Techniques (NIT). The House and Senate Judiciary Committees have neither debated nor approved the use of NITs. While technical and legal experts cast doubt on the merits of the change, the Administration has circumvented Congressional process to implicitly authorize the use of these tools.[1] This substantive new rule will take effect on December 1, 2016 unless congress passes legislation to halt or postpone it, such as the Stopping Mass Hacking Act (S. 2952 / H.R. 5321).

The Department of Justice has argued that the change to Rule 41 is *procedural* and will be narrowly applied.[2] However, the widespread effects of the change are clearly *substantive* and within the jurisdiction of the judiciary committees.[3] The change to Rule 41 will expand law enforcement's ability to use NITs in ways that may endanger human rights. For example:

- The change to Rule 41 would enable law enforcement to obtain a warrant from any magistrate judge to remotely search (i.e. hack) a computer where the computer's user

[1] Steven M. Bellovin, Matt Blaze & Susan Landau, *Insecure Surveillance: Technical Issues with Remote Computer Searches*, Computing Now, 2016, https://www.computer.org/cms/Computer.org/ComputingNow/issues/2016/06/mco2016030014.pdf (last visited Jun 1, 2016).

[2] RULE 41 CHANGES ENSURE A JUDGE MAY CONSIDER WARRANTS FOR CERTAIN REMOTE SEARCHES, Justice Blog (2016), https://www.justice.gov/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches (last visited Jun 20, 2016).

[3] Leslie Caldwell, Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches United States Department of Justice (2016), https://www.justice.gov/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches (last visited Jun 24, 2016).

has taken steps to protect his or her location, such as by using a VPN. Such tools are commonly used by journalists, activists, and other at-risk users.

- The change would facilitate the issuing of warrants to search more than one computer and to search computers outside the jurisdiction of the court. The FBI claims that this process will serve to streamline investigations; however, this expansion of searches would also facilitate and magnify risks to computer users.[4]
- The change to Rule 41 would grant access to computers belonging to victims of malware attacks and whose computers, as a result of such attacks, are part of botnets or tangentially connected. There are millions of computers for which such a provision could be applicable, including computers outside of the United States. Such an overbroad application could potentially disrupt the *legal* and *constitutionally-protected* activities of many users.[5]
- The change would authorize electronic notice to subjects of a warrant.
- The vague language of the amendment could allow activity ranging from something as simple as IP address collection to a more invasive and complex technique utilizing sophisticated malware to activate a user's built-in computer camera and microphones.[6]

While law enforcement agencies seek to keep the internet safe from malicious actors, this substantive change would keep users exposed to cybersecurity risks. In order to hack into a device, the government would have to exploit discovered vulnerabilities -- the same vulnerabilities that malicious actors utilize to commit fraud, identity theft, and other crimes. The potential to exploit vulnerabilities to access devices will disincentivize law enforcement agencies from reporting these vulnerabilities and thus would maintain an unsafe environment for *all* computer users.[7] It is necessary and appropriate to establish safeguards for innocent users through a more transparent, fair process for determining when to disclose vulnerabilities, as recommended by former White House advisors.[8]

There is no guarantee that the tools utilized by law enforcement agencies would be "controllable." Documents obtained by Wired magazine through the Freedom of Information Act, for example, demonstrate that law enforcement agencies are unable to predict the behavior of

---

[4] Rainey Reitman, With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Government Electronic Frontier Foundation (2016), https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government (last visited Jun 27, 2016).

[5] Testimony of Amie Stepanovich Senior Policy Counsel, Access on behalf of Access and the Electronic Frontier Foundation Before the Advisory Committee on Criminal Rules on the Matter of Proposed Amendments to the Federal Rules of Criminal Procedure, Rule 41, 4–7 (2014), https://www.accessnow.org/cms/assets/uploads/archive/docs/Rule41botnettestimony.pdf.

[6] Kim Zetter, So … Now the Government Wants to Hack Cybercrime Victims WIRED (2016), https://www.wired.com/2016/05/now-government-wants-hack-cybercrime-victims/ (last visited Jun 16, 2016).

[7] Bellovin et al., supra note 1 at 20.

[8] Ari Schwartz & Rob Knake, Government's Role in Vulnerability Disclosure; creating a permanent and accountable vulnerability equities process Government's Role in Vulnerability Disclosure; creating a permanent and accountable vulnerability equities process (2016).

their own software.[9] A computer system is not static like a building or a location for which warrants are usually granted for searches. There are many more variables at work to access information on a computer through malware. Thus, law enforcement agency efforts to access information through the proposed warrant amendments may end up causing damage to thousands of computers through mass hacking and exposing users to greater risk.[10]

The change to Rule 41 could also implicate international relations by allowing law enforcement agencies to conduct searches on computers that may be outside of the United States. The expanded use of NITs threaten laws protecting user privacy in other countries and could undermine international data protection agreements which are vital to the digital economy. The use of NITs as established within the change to Rule 41 would also circumvent the formalized Mutual Legal Assistance Treaty framework. A search of this nature would not only undermine well-established protocols but would also violate international laws of sovereignty.[11]

Importantly, Congress has never passed legislation on this sensitive issue. With the increased usage of computers, digital information has become crucial for investigations and this issue merits careful consideration by a democratic body.[12] Access Now recognizes that that 21st century law enforcement challenges necessitate 21st century methods. However, the changes to Rule 41 are not the appropriate method to address these challenges, as evidenced by the potential problems with substance of the change. Congress has already established the appropriate venues for these delicate discussions -- the Judiciary Committees in the House and Senate. Rather than allow the Administration to expand law enforcement's powers without debate, we urge you to hold hearings on the change to Rule 41 and the Stopping Mass Hacking Act.

Nathan White
Senior Legislative Manager

Amie Stepanovich
U.S. Policy Manager

---

[9] Solomon, Brett, *This Arcane Rule Change Would Give U.S. Law Enforcement New Power to Hack People Worldwide*, SLATE (May. 11, 2016, 2:00 PM), http://www.slate.com/blogs/future_tense/2016/05/11/the_rule_41_change_would_give_u_s_law_enforcement_power_to_hack_people_worldwide.html.

[10] Brett Solomon, *This Arcane Rule Change Would Give U.S. Law Enforcement New Power to Hack People Worldwide*, SLATE, 2016, http://www.slate.com/blogs/future_tense/2016/05/11/the_rule_41_change_would_give_u_s_law_enforcement_power_to_hack_people_worldwide.html (last visited Jun 23, 2016); Center for Democracy & Technology, ISSUE BRIEF: PROPOSED CHANGES TO RULE 41 INSIGHTS (2016), https://cdt.org/insight/issue-brief-proposed-changes-to-rule-41/ (last visited Jun 24, 2016).

[11] Center for Democracy & Technology, *supra* note 8.

[12] TESTIMONY OF AMIE STEPANOVICH SENIOR POLICY COUNSEL, ACCESS ON BEHALF OF ACCESS AND THE ELECTRONIC FRONTIER FOUNDATION BEFORE THE ADVISORY COMMITTEE ON CRIMINAL RULES ON THE MATTER OF PROPOSED AMENDMENTS TO THE FEDERAL RULES OF CRIMINAL PROCEDURE, RULE 41, *supra* note 7 at 8.

Drew Mitnick
Policy Counsel

--

Access Now defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all. Access Now's policy team works at the intersection of human rights and technology, furthering Access Now's mission by developing and promoting rights-respecting practices and policies. With staff placed strategically around the world, we seek to advance laws and global norms to affect long-term systemic change in the area of digital rights and online security, developing insightful, rights-based, and well-researched policy guidance to governments, corporations, and civil society.[13]

[13] About Us-Access Now, https://www.accessnow.org/about-us/ (last visited Jun. 20, 2016).