The Rule 41 Amendments: A Proposal to Expand Government Hacking Authority

At the request of the Department of Justice (DOJ), the U.S. federal court system (with the approval of the Supreme Court) has proposed changes to Rule 41 of the Federal Rules of Criminal Procedure. Absent congressional action, the rule change will automatically go into effect on December 1, 2016.[i]

The proposed amendments to Rule 41 would add new exceptions to the general rule that magistrate judges may only grant warrants for searches within their district. Specifically, the amendments would:

(1) Explicitly allow magistrate judges to issue a warrant *to remotely search and seize* (i.e. hack) electronic storage media within or outside their district in cases involving certain internet crimes or if the location of a computer is being masked through "technological means," (for example, when a person uses a virtual private network or a privacy-protective service like Tor). Such a warrant could cover hundreds or even millions of computers.[ii]

(2) Dramatically expand the fora in which officials may apply for a warrant to "*any* district where activities related to a crime *may* have occurred (emphasis added)," in cases involving such remote searches; and

(3) Weaken notice requirements by, in some cases, permitting the government to choose between providing notice to the target of the search or the owner of the property being searched.

The ACLU, along with organizations including the Computer and Communications Industry Association (CCIA), Electronic Frontier Foundation, Google, National Association of Criminal Defense Attorneys, Niskanen Center, and Reporters Committee on the Freedom of the Press, oppose the proposed changes to Rule 41.[iii] The ACLU urges Congress to pass S.2952, "The Stopping Mass Hacking Act", proposed by Senators Wyden (D-OR), Paul (R-KY), Baldwin (D-WI), Daines (R-MT), and Tester (D-MT), which would halt the proposed Rule 41 changes from going into effect.[iv]

The proposed changes are substantive, not procedural. Thus, they must be authorized through a law passed by Congress, not a change to the Federal Rules of Criminal Procedure.

- The amendment explicitly permits remote electronic hacking of victims and suspects without *any* authorization from Congress regarding whether these searches should be permitted, what protections should apply, and what remedies should be available for impacted third parties. Congress has made clear that such changes which "abridge,

enlarge, or modify" a substantive right should not be made through a procedural criminal rule change.[v]

- Existing provisions in Rule 41 that permit out-of-district search warrants have been authorized through legislation. For example, Congress passed the Patriot Act to permit judges to issue warrants outside their jurisdiction in terrorism cases; similarly, the Electronic Communications Privacy Act (ECPA) contains provisions allowing judges to authorize tracking devices that may be used outside their jurisdiction.[vi]

The amendments would allow judges to issue one warrant to potentially search millions of computers, raising significant constitutional and policy concerns.

- The proposed rule does not limit who can be the target of a search; a single warrant could be used to authorize the seizing of personal information involving thousands or millions of individuals, including potential victims of internet crimes. Such warrants may violate the Fourth Amendment's particularity requirement, which requires that a warrant "particularly describ[e] the place to be searched," and have serious cybersecurity implications.

- By expanding the number of investigations where law enforcement engages in remote computer hacking, the amendments increase the risk of law enforcement bypassing the requirements of ECPA when seeking information held on the cloud. Instead of requesting this information from the provider, law enforcement may try to access it directly via the hacked computer, potentially exposing large amounts of data that may be unrelated to the crime under investigation.

The proposed changes weaken Rule 41's existing notice requirements by permitting the government to unconstitutionally deny notice to the target of a search.

- Individuals have a constitutional right to be notified in cases where law enforcement searches or seizes their information. In cases falling under the new changes, the proposal would allow government to choose between providing notice to either the owner of the property being searched (i.e. the owner of a server) *or* the target of the search (i.e. the individual whose information was seized).

The proposed amendments encourage forum shopping and raise jurisdictional concerns by expanding the districts in which law enforcement can apply for a warrant.

- Generally, magistrate judges may only issue a warrant to search or seize property located within their district. The proposed change would permit law enforcement to apply for a warrant in "*any* district where activities related to a crime *may* have occurred (emphasis added)."

    - Most federal criminal investigations and prosecutions rely on the impact or effect on interstate commerce for their federal jurisdiction.[vii] Thus, as a practical matter, this means that the proposed amendment will give federal

agents the ability to cherry-pick among multiple jurisdictions when filing a warrant application.

- For example, if a suspect in an investigation had sent fraudulent emails to computers located in twenty different districts, the proposed rule would allow a judge in any of those twenty districts to issue a search warrant. If initially denied, law enforcement could subsequently file the same warrant application in any of the other jurisdictions.

- The proposed rule does not fully consider court decisions which recognize that there are constitutional limits on the ability of magistrate judges to authorize searches outside their district - limits that may be particularly pronounced in cases where the nexus between the crime and the district is attenuated.[viii]

The proposed amendment is broader than necessary to address DOJ's stated needs.

- The government has asserted that this rule change is needed to address situations in which the location of a device is unknown. However, the rule does not limit searches to only the information necessary to ascertain the location of a device or to cases where all other investigative means have been exhausted.

The proposed changes fail to ensure that judges are provided the information necessary to appropriately review warrant applications submitted under the new rule.

- The proposed rule does not require government agents to include explicit details in the warrant application regarding how the remote access search will be conducted, the impact on third parties, and any protections that will be put in place to mitigate the impact on third parties. Without this information, judges cannot adequately assess constitutional concerns prior to granting a warrant application.

- This is at odds with DOJ policy in other contexts; for example, DOJ policy explicitly requires that information regarding the technology, minimization procedures, and impact on third parties be included in warrant applications for Stingrays.[ix]

[i] 28 U.S.C. §2074(a)

[ii] Final Package from John Roberts, Chrief Justice, U.S. Supreme Court to Paul Ryan, Speaker of the House of Representatives, April 28, 2016, at 208-09 ("Final Package"), *available at* http://www.uscourts.gov/file/document/2016-04-28-final-package-congress.

[iii] Heather Greenfield, *CCIA Applauds Senate Bill To Stop Surveillance Expansion*, COMPUT. & COMMC'NS INDUS. ASS'N. (May 19, 2016), http://www.ccianet.org/2016/05/ccia-applauds-senate-bill-to-stop-surveillance-expansion/; Hearing Before the Advisory Committee on Criminal Rules on the Matter of Proposed Amendments to Federal Rules of Criminal Procedure, Rule 41, (Nov. 5, 2014) (statement of Amie Stepanovich, Senior Policy Analyst, Access, on behalf of Access and the Electronic Frontier Foundation) *available at* https://www.accessnow.org/cms/assets/uploads/archive/docs/Rule41botnettestimony.pdf; Letter from Richard Salgado, Director of Law Enforcement and Information Security, Google Inc., to the Judicial Conference Advisory Committee on Criminal Rules (Feb. 13, 2015), *available at* https://www.regulations.gov/contentStreamer?documentId=USC-RULES-CR-2014-0004-0029&attachmentNumber=1&disposition=attachment&contentType=pdf; Letter from Samuel Guiberson, Peter Goldberger, and William Genego, the National Association of Criminal Defense Lawyers, to the Judicial Conference Advisory Committee on Criminal Rules (Feb. 17, 2015), *available at* https://www.regulations.gov/contentStreamer?documentId=USC-RULES-CR-2014-0004-0038&attachmentNumber=1&disposition=attachment&contentType=pdf; Ryan Hagemann, *No "lawful Systems Access" Via Rule 41*, NISKANEN CENTER (Apr. 25, 2016), https://niskanencenter.org/blog/no-lawful-systems-access-via-rule-41/; Letter from Bruce Brown, Katie Townsend, Hannah Blach-Wehba, and Jennifer Henrichsen, Reporters Committee for Freedom of the Press, to The Judicial Conference Advisory Committee on Criminal Rules (Feb. 17, 2015), *available at* https://www.regulations.gov/contentStreamer?documentId=USC-RULES-CR-2014-0004-0047&attachmentNumber=1&disposition=attachment&contentType=pdf.

[iv] Stopping Mass Hacking Act, S___, 114th Cong. (2016) a*vailable at* https://www.wyden.senate.gov/download/?id=959B9967-F666-404F-B2D5-2520586107C2&download=1.

[v] 28 U.S.C. §2072(b).

[vi] §219 & §804, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. Law 107-56, 107th Cong.; 18 U.S.C. §3117(a)

[vii] *See* 1 Wayne R. LaFave et al., Crim. Proc. § 1.2(c) (3d ed.) ("[T]he dramatic expansion of federal criminal law was based primarily on Congress' authority under the Commerce Clause . . . .").

[viii] *See* Weinberg v. United States, 126 F.2d 1004, 1006 (2d Cir. 1942). ("[E]ven though the statute . . . does not contain an express limitation of the district court's power to its own district, that seems clearly understood, in view of the constitutional provisions and the general rule of territorial limitation").

[ix] DEP'T OF JUSTICE, DEP'T OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECH (last visited May 25, 2016) *available at* https://www.justice.gov/opa/file/767321/download.