CENTER FOR
DEMOCRACY
& TECHNOLOGY

May 2016

Issue brief: Proposed Changes to Rule 41

The Rule Change: Under the **old Rule 41** of the Federal Rules of Criminal Procedure, magistrates with authority in a district may only issue warrants for search and seizure of property located within that district, with limited exceptions. Under the **new Rule 41**, magistrate judges would be able to grant warrants to search and seize electronic media located outside of their districts in two additional circumstances: 1) When the physical location of the information is "concealed through technological means"; and, 2) When, in an investigation of a violation of the Computer Fraud and Abuse Act (CFAA) (18 U.S.C. §1030(a)(5)), computers in five or more districts have been "damaged without authorization."

Privacy and Cybersecurity Concerns: *The new Rule 41 . . .*

- . . . violates the **particularity requirement of the Fourth Amendment**, which requires that the place to be searched be specifically described. Without the particularity requirement, multiple innocent parties could be affected by a remote search.
- . . . authorizes extraterritorial searches that **circumvent the MLAT process** and may **violate international law**. If a computer's location is unknown, it could be located anywhere in the world, which means that a remote search could violate well-established rules of sovereignty and comity with other nations.
- . . . creates new risks of **forum shopping**. Allowing agents to obtain warrants from any district would incentivize them to seek out and re-use districts that are more inclined to approve warrant applications, districts that may authorize overly-invasive or unnecessary technical means, or districts that are prohibitively inconvenient for the individual whose items are searched or seized.
- . . . contains very few restrictions. The new rule can reach practically **any computing device in the world**, and implicates many **common (and lawful) methods of using the internet**. "Concealed through technological means," for example, may encompass any use of computers that may change the route their network traffic takes to reach a destination (such as the use of VPNs). "Damaged" computers may include all computers infected with any virus or other damaging code, a vast number of computers.
- . . . **endangers** all devices, data, and dependent systems. Intrusion methods necessarily exploit weaknesses in the defenses of a device in order to gain access. Therefore, any remote searches and seizures could result in damage due to vulnerabilities introduced into the system or exacerbated by the technical act of gaining entry.

Suggested Reforms

- **Limit the scope of information that may be gathered.** To ensure that concealment of the location of information cannot make that information beyond the reach of the law, it would be appropriate to limit the scope of remote searches and seizures to the collection of information that can be used to identify the location of the target device (*e.g.*, a device identifier or network address). Once investigators pinpoint the location of the information, they may then go to the appropriate jurisdiction and obtain a warrant through means that comply with the Fourth Amendment and any international obligations.
- **Remove the exception for "damaged" computers.** Any government intrusion may further damage computers that have been infested by a botnet. These could be poorly maintained computers in critical systems in health care, power infrastructure, and other governments. The risk of potential damage to brittle and unknown computing devices are too great to permit this exception to the Fourth Amendment's particularity requirement.
- **Require additional details.** Given the unique risks that come with remote searches and seizures, magistrates should be able to make informed decisions about what, exactly, they're being asked to approve with each warrant application. To the extent feasible, warrant applications should 1) disclose the specific techniques that will be used throughout the remote search, including gaining entry and searching media; 2) establish that such techniques will be technically well-tailored to minimize intrusion, harm, and collateral damage; 3) provide the approximate number of devices that will be hacked; and 4) demonstrate exhaustion of other alternatives.

CDT's detailed analysis of the Rule 41 changes: https://cdt.org/?p=74296

CDT blog post, "U.S. Supreme Court Endorses Government Hacking": https://cdt.org/?p=78357

For more information, please contact Joseph Lorenzo Hall, CDT Chief Technologist, at joe@cdt.org.

Center for Democracy & Technology