Northeastern University

The DOJ's Trojan:

A Legal Analysis of Rule 41 and Remote Search and Seizure of Botnets

John Martin

CS 4170 The Law, Ethics, and Policy of Data and Digital Technologies

Professor Woodrow Hartzog

April 12, 2018

• • •

> Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent . . . the greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.[1]
>
> Supreme Court Justice Louis Brandeis

• • •

In one of the most controversial and influential privacy cases in history, Justice Brandeis dissented the decision of the 1927 case of *Olmstead v. United States*, warning that the government should not be permitted to surveil persons who have a reasonable expectation of privacy. Forty years later in 1967, *Katz v. United States* sided with Brandeis and overturned the Olmstead outcome, ruling that an individual's Fourth Amendment rights extend beyond her physical possessions. Today, the Fourth Amendment is understood to "protect people, not places."[2] And now, in the wake of new guidelines in the Federal Rules of Criminal Procedure regulating how the government can obtain search warrants, we may be wise to look to Brandeis again for guidance in protecting liberty.

The Federal Rules of Criminal Procedure stand as legal guidelines for how law enforcement may go about investigating criminal activity in the United States. These rules are written first by federal agencies and committees before being presented to the Supreme Court and Congress.[3] Recently, these rules were amended to give the government more power in

---

[1] Olmstead v. United States, 277 US 438 (1928).
[2] Katz v. United States, 389 US 347 (1967).
[3] Thomson II, Richard M., "Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure," Congressional Research Service (2016): 8.

prosecuting criminals in the wake of new computer technology, which has posed unique difficulties in warrant obtainment for law enforcement. These amendments have left academics,[4] congresspersons,[5] and several American companies and organizations[6] very concerned about the law's potential to negatively affect the civil liberties of non-criminal Internet users.[7] Critics point out that the amendments authorize broad, never before seen government hacking abilities without any checks of power that severely threaten the privacy of Americans and people worldwide.[8] Others are concerned that the amendments will amplify an existing problem known as "forum shopping," where law enforcement agents find sympathetic judges to approve searches in districts over which they otherwise do not have authority.[9] Some have even argued that these specific changes to Rule 41 regarding remote search and seizure are sensitive enough that they should not be delegated to a federal agency at all, and should instead be debated vigorously by elected representatives.[10] Although the rules ultimately passed the Supreme Court and a divided Senate, there was enough concern generated over the changes to Rule 41 to compel a bill proposal, the Stopping Mass Hacking Act, by Senator Ron Wyden of Oregon.[11]

---

[4] Orcutt, Mike, "Congress Is About to Expand Government Hacking Powers," MIT Technology Review (2016), https://www.technologyreview.com/s/602953/congress-is-about-to-expand-government-hacking-powers/. Specifically, Professor Woodrow Hartzog's worry that "the history of computer crime law shows that vague language can lead to unintended consequences as technology evolves."

[5] Wyden, Ron, "Wyden: Congress Must Reject Sprawling Expansion of Government Surveillance," Ron Wyden of Oregon (2016), https://www.wyden.senate.gov/news/press-releases/wyden-congress-must-reject-sprawling-expansion-of-government-surveillance.

[6] "Coalition Letter to House and Senate Leadership Opposing Proposed Changes to Rule 41 of FRCP," https://alair.ala.org/handle/11213/6145.

[7] Ibid.

[8] Ibid.

[9] Thompson II, "Digital Searches and Seizures," 7.

[10] Thompson II, "Digital Searches and Seizures," 7-8.

[11] H.R.5321. https://www.congress.gov/bill/114th-congress/house-bill/5321/text.

This paper will stand to analyze the legal implications of the 2016 additions to Rule 41 of the Federal Rules of Criminal Procedure. Among the many concerns over the Rule, the paper will focus specifically on the new legal implications law enforcement deploying Trojan techniques (often referred to as a Computer and Internet Protocol Address Verifier (CIPAV) or simply a Network Investigative Technique (NIT))[12] on botnet-like entities. The paper will first offer a literature review of existing opinions about controversial language and interpretations involving Rule 41 and digital search and seizure, will move on to an attempt to lay out and explain the new language of the Rule, its standing among other interpretations of existing law, and possible inferences that can be logically drawn from such cross analysis, and finally will conclude with a summary of discoveries from the analysis.

Literature Review

Rule 41 of the Federal Rules of Criminal Procedure is titled "Search and Seizure." The Rule serves to provide more concrete interpretations of how the government must comply with the Fourth Amendment when applying for and executing warrants. As such, much existing literature involving Rule 41 comes largely as an analysis of the Fourth Amendment. This paper, though, is focused specifically on recent changes to Rule 41, and there are some recent pieces that analyze legal implications similar to those analyzed here. From these, there are two primary stances: those that are sympathetic to the Department of Justice, and those that worry that the additions to Rule 41 are too broad.

The former group points to cases where the DOJ has needed these expansions to stop truly harmful crime. The DOJ themselves wrote a letter to Senator Ron Wyden explaining their

[12] Lerner, Zach, "A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure," *Yale Journal of Law and Technology*, 38.

position on the changes to Rule 41. They argue, firstly, that "[t]he use of remote search and seizure is not new . . . [and] courts already permit the search of multiple computers pursuant to a single warrant."[13] They further argue that the changes relax the unreasonable requirement that officers seek warrants from a judge that has authority over the location of the computer. Via the Internet, computers involved in the same investigation can easily span several, and up to 94, districts.[14] Moreover, the DOJ argues that "this change would not permit indiscriminate surveillance . . . because other than identifying a court to consider the warrant application, the amendment makes no change to the substantive law governing when a warrant application should be granted or denied."[15]

Botnets do pose a threat to the Internet as well as individuals and businesses, so there is a real need to do something about them. Botnets are also criminal, so the DOJ has a legitimate interest in investigating them.[16] Parties on both sides of the Rule 41 debate agree on this point. The ACLU opposed the changes to Rule 41, but stated that it "is sympathetic to the goal of disabling botnets and strengthening the security of the Internet."[17] But ultimately disagreed that Rule 41 of the Federal Rules of Criminal Procedure is the correct way to go about dealing with botnets, claiming, "If the government is acting primarily in a cybersecurity capacity (analogous to the government's public health function), rather than in a primarily law enforcement capacity,

---

[13] Kadzik, Peter J., Assistant Attorney General U.S. Department of Defense to The Honorable Ron Wyden, 18 November 2016. https://www.wyden.senate.gov/download/2016-11-18-rule-41-doj-response-to-wyden, 1.
[14] Kadzik, Assistant Attorney General, 2.
[15] Ibid.
[16] Lerner, "A Warrant to Hack," 32.
[17] American Civil Liberties Union to Members of the Advisory Committee on Criminal Rules, 4 April 2014, "Re: ACLU Comment on the Proposed Amendment to Rule 41 Concerning Remote Searches of Electronic Storage Media," https://www.aclu.org/other/aclu-comments-proposed-amendment-rule-41, 14.

then Fourth Amendment concerns are less acute."[18] They further argue that in past cases involving NITs, the government has not sufficiently provided judges with an understanding of the technology, including an understanding of the possible damage it can cause. They point out the Rule 41 changes should address this, and judges should have a full understanding of the capabilities of the technology.[19] The opposing view rejects this, claiming that the specific details of these techniques are classified and their reveal could jeopardize investigations.[20]

After the amendments were passed by the Supreme Court, opponents like Ron Wyden and Markus Rauschecker concluded that Rule 41 gives law enforcement "new substantive authorities" to conduct searches.[21] For this reason, they believe that legislative bodies should have debated the Rule and its consequences, and that the Supreme Court acted beyond its authority in passing the amendments to the Rule.[22] And conversely, there are academics such as Orin Kerr who believe it is important to update rules surrounding warrants in response to changing technology, and that, "the [Federal] Rules Committee rather than the courts are best suited to address the problem."[23]

Legal Analysis

The Federal Rules of Criminal Procedure is updated regularly as the needs of government evolve. In 2016, the Rules were updated to define ways in which a magistrate judge is allowed to

---

[18] Ibid.
[19] American Civil Liberties Union to Members of the Advisory Committee on Criminal Rules, 14-15.
[20] Lerner, "A Warrant to Hack," 44.
[21] Rauschecker, Markus, "Rule 41 Amendments Provide for a Drastic Expansion of Government Authority to Conduct Computer Searches and Should Not Have Been Adopted by the Supreme Court," *Maryland Law Review*, 1101.
[22] Ibid.
[23] Kerr, Orin, "Search Warrants in an Era of Digital Evidence," *Mississippi Law Journal* (2005), 135.

authorize the remote search of computers outside the judge's district. Before this change, magistrate judges were only authorized to grant remote searches of computers known by the government to be within the given judge's district, unless the search involved an investigation of terrorism.[24]

Rule 41(b) outlines the situations in which a magistrate judge can issue a warrant. Before the 2016 amendment, the section allowed for five cases: (1) for a person or property expressly in the judge's district, (2) for a person or property expressly in the judge's district which might be moved outside the district before the warrant is executed, (3) for a person or property inside **or outside** the judge's district in matters related to domestic or international terrorism, (4) to install on a person or property a tracking device that may or may not move outside of the district, and finally (5) for property located outside the judge's district but inside United States territories or diplomatic buildings.[25] With the amendment, one additional case with two subsections has been added to Rule 41(b):

> (6) 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 or copy electronically stored information located within **or outside** that district if:
>
> (A) the district where the media or information is located has been concealed through technological means; or

[24] Fed. R. Crim. P. 41(b) (2017).
[25] Ibid.

> (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.[26]

To break down (6)(B) one must understand 18 U.S.C. § 1030(a)(5), which is a violation definition clause of the Computer Fraud and Abuse Act (CFAA):

> Anyone who . . . (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
>
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[27]

Section (A) makes a reference to the term "protected computer." A "protected computer" is a term of art defined in the CFAA in section 1030(e)(2) as "a computer … which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States."[28] Every computer connected to the Internet affects interstate or foreign communications. This means, in effect, every computer connected to the Internet is subject to the definition of a "protected computer" falling under jurisdiction of the new Rule 41. Therefore, section 1030(a)(5)(A) defines, among other things, computers involved in botnets.[29] Botnets are generally comprised of computers owned by innocent, unknowing, and involuntarily involved

---

[26] Ibid.
[27] 18 U.S.C. § 1030(a)(5).
[28] 18 U.S.C. § 1030(e)(2).
[29] Lerner, "A Warrant to Hack," 30.

individuals. Botnets can involve hundreds of thousands to millions of computers.[30] Computers involved in these botnets would trivially be located in five or more districts. Per the new definition in Rule 41, any magistrate judge could issue a warrant to seize information from these millions of computers, and consequentially millions of individuals.

It is important to realize this shift in targeting when issuing such warrants. The individuals involved in botnets are not criminals, but victims of criminal activity. After being infected, the victims of these computers may "transmi[t] a program, information, code, or command" but not by their own volition. Importantly, these victims are not *intentionally* or *knowingly* participating in crime. The creator of the botnet, who is presumably unknown, has *intentionally* or *knowingly* violated section 1030(a)(5), but Rule 41 issues warrants against the criminal's victims.

Moreover, contacting the owners of these computers is exceptionally more challenging than in a traditional warrant execution. Copies of these warrants often cannot be delivered to the individuals that they have been issued against.[31] Rule 41 has long interpreted the Fourth Amendment as guaranteeing the right to an immediate copy of the warrant and a receipt of seized items from the executing officer: "The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property."[32] However, in the case of remote searches like those used for botnets, this right has been reduced to a requirement to "make reasonable efforts":

---

[30] Thomas, Karl. "Nine bad botnets and the damage they did." 25 Feb. 2015. https://www.welivesecurity.com/2015/02/25/nine-bad-botnets-damage/
[31] Lerner, "A Warrant to Hack," 33-34.
[32] Fed. R. Crim. P. 41(f)(1)(c) (2017).

> For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.[33]

"Reasonable efforts" that are "reasonably calculated to reach" all the millions of victims of a botnet could easily result in few to no warrants being successfully served. Moreover, courts have established if a warrant is not shown upon request the search is in violation of the Reasonableness Clause of the Fourth Amendment.[34] In 2008, officers executed a search at the private home of a certain Thomas. When asked to view a warrant, officers denied Mrs. Thomas and proceeded to search the home before ultimately leaving a copy of the warrant before departing. In 2009, Thomas sued the government for infringement of his Fourth Amendment right to be free from unreasonable searches and won.[35] What is one to make of the legality of a search where the individual does not know the search is happening, and thus has no grounds to voice a request for the warrant? Furthermore, without knowledge of the warrant or the search, no individual can ever generate a case to challenge the constitutionality of the warrant. Framed this way, a search of this nature appears unconstitutional.

Additionally, courts have long agreed that items in plain view during a search can be acceptably counted as evidence. The 1942 moonshining case of *Hester v. United States* ruled,

---

[33] Fed. R. Crim. P. 41(f)(1)(c) (2017).
[34] United States v. Thompson, 667 F. Supp. 2d 758 (S.D. Ohio 2009)
[35] Ibid.

"The special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers and effects,' is not extended to the open fields."[36] How might the plain view doctrine apply to these sweeping remote searches? Suppose the Trojan software turns up information about computers that goes beyond what was necessarily expected. For example, the record returned by the search contains, in addition to an Internet Protocol address, which is less unique and therefore less personal, a media access control (MAC) address, which is unique to a particular device and therefore more personal. This is just an example, but it is feasible that highly sensitive information could be uncovered this way. This information might be reasonably in "open field" and admissible as collectable evidence from the officer's vantage point when executing the remote search.

Officers might even suspect that their search could result in such evidence in advance. That is to say, it has been held that officers do not need to inadvertently come upon plain view evidence for it to be admissible. *Horton v. United States* determined that "the Fourth Amendment does not prohibit the warrantless seizure of evidence in plain view even though the discovery of the evidence was not inadvertent."[37] If officers believe it is possible that they could happen upon extra information they can categorize as not the primary target of the search, but reasonable to collect through plain view doctrine, they may not legally need to exercise much caution in designing techniques that often collect sundry information. Indeed, they may be incentivized to do so. When considering sweeping warrants like those sought for botnets, combined with the implications of plain view doctrine, one could reasonably conclude that the government may now be authorized to use Rule 41 to deploy tactics that resemble dragnet techniques.

---

[36] Hester v. United States, 265 U.S. 57 (44 S.Ct. 445, 68 L.Ed. 898) (1924).
[37] Horton v. United States, 496 US 128 (1990).

Warrants of this type that are also expansive may very well be unconstitutional. In *United States v. Bridges*, the Ninth Circuit Court of Appeals rejected the constitutionality of a warrant because it was not sufficiently specific to the property being seized, saying, "[warrants] are fundamentally offensive to the underlying principles of the Fourth Amendment when they are so bountiful and expansive in their language that they constitute a virtual, all-encompassing dragnet of personal papers and property to be seized at the discretion of the State."[38] Personal computers increasingly contain masses of sensitive information. If a government Trojan program collected even a single sensitive property was a side effect of executing a warrant on a botnet of millions of people, the privacy implications may be defined as an "all-encompassing dragnet" and run afoul of the Fourth Amendment.

Conclusion

Botnets are dangerous instruments. They are a growing problem in society, especially with the increase popularity in Internet of things devices.[39] Botnets make millions of innocent people victims, and have long been classified as illegal under the CFAA. None of this in controversial. What is controversial is how to deal with this reality. Like much of law, solving the problem comes down to a balancing act between the powers of government and the rights of people. In the midst of current fast-moving technological changes, we ought to heed Justice Brandeis' advice that, without understanding, even the best-intentioned individuals can make enormous mistakes.

It appears that the additions to Rule 41 of the Federal Rules of Criminal Procedure may very well have been such a case. The Rule's loosening of the requirement to serve a copy of the

[38] United States v. Bridges, (9th Cir. 2003).
[39] Arghire, Ionut, "New Botnet Is Recruiting IoT Devices," Security Week, 2 Feb 2018, https://www.securityweek.com/new-botnet-recruiting-iot-devices.

warrant strips rights that are traditionally granted to individuals by the Constitution. The individual is not guaranteed knowledge of the search, and as such is not guaranteed the possibility of requesting the warrant and is not guaranteed the ability challenge the search. Certain interpretations of the plain view doctrine might mean that files containing aggregate information collected in a Rule 41 warrant is admissible. The degrading of Fourth Amendment protections against unreasonable search and seizure, the lack of rights afforded in traditional warrant execution, the targeting of warrants against victims of crimes, and the sheer volume of individuals that can be affected by the issuance of a single warrant all suggest that the additions to Rule 41 lend themselves to, in Hartzog's words, "[a] dramatic expansion[] of power."[40]

[40] Orcutt, Mike, "Congress Is About to Expand."