Written Statement

Of

The Center for Democracy & Technology

Before

The Judicial Conference

Advisory Committee on Criminal Rules

Friday, October 24, 2014

Members of the Committee, thank you for allowing the Center for Democracy & Technology (CDT) to testify on proposed changes to Rule 41 of the Federal Rules of Criminal Procedure (FRCrmP).[1] CDT is a nonprofit public interest organization dedicated to promoting policies and technical standards that protect civil liberties such as privacy and free expression globally.

CDT recognizes that law enforcement faces legitimate challenges in determining how to issue search warrants for computers with concealed locations in investigations. We also recognize the negative impact of malware, botnets, and illicit online activities undertaken using anonymity techniques that may obfuscate location. However, we believe the solution to this complex problem should arise through public and legislative debate. The proposal before the Advisory Committee on Criminal Rules to modify Rule 41 of the FRCrmP has significant implications for open legal and policy issues, as well as broad technological consequences affecting the privacy of computer users worldwide. We believe the Judicial Conference should withdraw the proposed changes to Rule 41 from its rulemaking process, and that the proposal should instead be deliberated in Congress.

I. The Proposed Amendment

Rule 41 of the FRCrmP is of fundamental importance to how the Fourth Amendment warrant requirement for government search and seizure applies in practice. Any changes to the Rule should be viewed in this context and carefully avoid creating new risks to privacy and security. However, the proposed modifications to FRCrmP Rule 41 would have significant legal and technical implications, described below, that merit open consideration by Congress, rather than a rulemaking proceeding of the Judicial Conference.

Under the current FRCrmP Rule 41, magistrates with authority in a particular district can issue warrants for the search and seizure of property:

a. Located within the district at the time of the search;

[1] Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure, Committee on Rules of Practice and Procedure, Judicial Conference of the United States, pgs. 338-339, Aug. 2014, www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf.

b. Located within the district at the time the warrant is issued, but which may move outside the district prior to the search;
c. Located within or outside the district in terrorism cases if the magistrate has authority in a district in which activities related to terrorism may have occurred;
d. Via tracking device, if the tracking device is installed in the district, even if it continues to function outside the district; and,
e. Located outside the jurisdiction of any district, but within a U.S. territory, possession, commonwealth, or diplomatic mission.[2]

The proposed amendment to FRCrmP Rule 41 would provide magistrates with new powers to authorize warrants to remotely search and seize or copy electronic media located outside the magistrate's district.[3] Per the proposal, magistrates would be able to exercise this power in two circumstances:

a. When the physical location of the media or information is "concealed through technological means," or
b. In an investigation of 18 U.S.C. 1030(a)(5), when the damaged protected computers are located in five or more districts.[4]

II. Legal Implications

The proposed modification to FRCrmP Rule 41 would make policy decisions about important questions of law that are not currently settled and would best be resolved through legislation.

A. The proposed Rule 41 amendment would authorize searches that violate the particularity requirement of the Fourth Amendment.

If the physical location of the electronic media to be searched is unknown, the search may not satisfy the particularity requirement of the Fourth Amendment, which requires that the "place to be searched" be particularly described.[5] In *In Re Warrant to Search a Target Computer at Premises Unknown*, the magistrate judge rejected a government application for a warrant to search and copy information from a computer, the location of which was unknown at the time of the application. The court concluded that the application did not satisfy the particularity requirement of the Fourth Amendment because the application did not describe the place to be searched.[6] The court also noted that, because the computer's location and owner were

---

[2] Rule 41(b)(1)-(5), Search and Seizure, Federal Rules of Criminal Procedure.

[3] *Supra*, fn 1.

[4] Under 18 U.S.C. 1030(e), the term "damage" means any impairment to the integrity or availability of data or a system, and the term "protected computer" means any computer affecting interstate or foreign communication – including computers located outside the United States.

[5] "[...] no warrants shall issue, but upon probable cause [...] and particularly describing the place to be searched, and the persons or things to be seized." Fourth Amendment to the United States Constitution.

[6] *In Re Warrant to Search a Target Computer at Premises Unknown,* F. Supp. 2d , 2013 WL 1729765 (S.D. Tex. Apr. 22, 2013). "The court concludes that the revised supporting affidavit does not satisfy the Fourth Amendment's particularity requirement for the requested search warrant for the Target Computer."

unknown, the search could easily affect multiple innocent parties.[7] The court's determination that the application was insufficient on Fourth Amendment grounds was wholly independent of the court's consideration of whether the current text of Rule 41 allows for warrants that authorize searches of computers in unknown locations.

The proposed FRCrmP Rule 41 modification includes a note that states: "The amendment does not address constitutional questions, such as the specificity of description that the Fourth Amendment may require in a warrant for remotely searching electronic storage media […] leaving application of this and other constitutional standards to ongoing case law development."[8] While we appreciate the fact that the Committee does not seek to address such questions in this rulemaking, the proposed modification to Rule 41 nonetheless does have direct bearing on these very questions since it specifically contemplates the issuance of warrants for computers in concealed locations.

B. The proposed Rule 41 amendment would authorize extraterritorial searches that circumvent the MLAT process and may violate international law.

If the physical location of a computer is concealed through technological means, the computer is potentially anywhere in the world. In commentary, the Department of Justice states that the proposed amendment does not purport to authorize courts to issue warrants that authorize the search of electronic media located in foreign countries.[9] However, given the global nature of both the Internet and anonymizing tools,[10] in practice the warrants will very likely be used to authorize searches of electronic media located outside the United States.

If the computer from which data is searched or copied is located abroad, then the search takes place abroad. Several cases hold that a seizure occurs when and where data is copied, even if the warrant to remotely search electronic media is issued in the United States, or if the agent reviewing data extracted remotely from electronic media is located in the United States. The Second Circuit, for example, held that the act of copying electronic data constitutes a seizure, even before an agent searches through the extracted data.[11] Other courts have held that a search or seizure of data occurs where the electronic storage media is located.[12]

---

[7] *Id.* "The Government's application offers nothing but indirect and conclusory assurance that its search technique will avoid infecting innocent computers or devices[...] What if the Target Computer is located in a public library, an Internet café, or a workplace accessible to others? What if the computer is used by family or friends uninvolved in the illegal scheme?"

[8] *Supra,* fn 1, at pg. 341.

[9] Letter from Mythili Raman, U.S. Department of Justice, to Reena Raggi, Advisory Committee on the Criminal Rules, Sept. 18, 2013. Available at http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2014-04.pdf (pg. 174).

[10] As an example, more than 85% of the users of Tor – a popular service that conceals computer location – are located outside the United States. Tor, Tor Metrics: Users, Top-10 countries by directly connecting users, https://metrics.torproject.org/users.html (last accessed Oct. 22, 2014).

[11] U.S. v. Ganias, 12-240-CR, 2014 WL 2722618 (2d Cir. June 17, 2014). See also U.S. v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010).

[12] U.S. v. Gorskhov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

Extraterritorial searches today typically take place in coordination with foreign governments under the Mutual Legal Assistance Treaty (MLAT) process.[13] The issue of whether U.S. magistrates may circumvent MLATs and issue warrants to search data stored abroad is still under litigation.[14] Yet the proposed amendment could be interpreted to authorize U.S. law enforcement to unilaterally search media located abroad, so long as the location is unknown at the time of the search. In practice, this will likely result in U.S. law enforcement agencies circumventing the MLAT process far more often than in present circumstances.

Unilateral extraterritorial searches may violate the international obligations of the United States. Established and binding customary international law provides that a state (i.e., a nation) may not exercise its power in any form in the territory of another state without that state's consent. As a corollary of this rule, U.S. law enforcement officers may only exercise their functions in the territory of another state with the consent of the other state, given by duly authorized officials of that state, and in compliance with the laws of both the United States and the other state.[15] The Restatement (Third) of the Foreign Relations Law of the United States describes this stricture as "universally recognized."[16] The proposed changes to FRCrmP Rule 41 could put U.S. law enforcement agencies at risk of violating this binding rule of sovereignty, as well as the principle of comity, when they unilaterally conduct searches of electronic media outside U.S. territory. Computer users abroad would have little or no remedy for an improper search by the U.S. government, including if that search or seizure damages the user's computer.

C. The proposed Rule 41 amendment would make changes through judicial rulemaking that have thus far occurred through legislation.

The proposed amendment to FRCrmP Rule 41 would authorize magistrates to issue warrants to search property that is located outside of their districts both when the warrant is issued and when the search occurs. Currently, Rule 41 grants magistrates limited authority to issue warrants to search property outside their districts. Only under subsections (b)(3) and (b)(5) of the Rule do magistrates have authority to issue warrants for property that is not located in the district both at the time when the warrant is issued and when the search is performed.[17] In comments, the Department of Justice has analogized the language of the proposed amendment to Rule 41 to the current language in subsections (b)(3) and (b)(5) of Rule 41.[18]

---

[13] MLATs and Mutual Legal Assistance Agreements (MLAA) allow for the exchange of evidence in criminal matters between nations party to the treaty or agreement. The United States has an MLAT or MLAA in place with a large number of foreign nations. See 2012 International Narcotics Control Strategy Report: Treaties and Agreements, Dept. of State, Mar. 7, 2012, available at http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm.

[14] See, e.g., Stipulation Regarding Contempt Order, *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, Case Nos. 13-MAG-2814, M9-150, S.D.N.Y. (Sep. 2014), available at http://media.scmagazine.com/documents/91/microsoft_contempt_filing_22623.pdf.

[15] Restatement (Third) of the Foreign Relations Law of the United States, §§ 432(2), 433.

[16] *Ibid.* at § 432, comment (b).

[17] Rule 41(b)(1)-(5), Search and Seizure, Federal Rules of Criminal Procedure.

[18] *Supra*, fn 9.

However, both (b)(3) and (b)(5) have legislative roots not present in the newly proposed amendment to Rule 41.

Subsection (b)(3) of Rule 41 allows magistrates in any district in which terrorism-related activities have occurred to issue warrants for a person or property outside the district during investigations of domestic or international terrorism. This subsection was a Congressional amendment to Rule 41 as part of the USA PATRIOT Act of 2001.[19]

Subsection (b)(5) of Rule 41 was adopted in 2008 by the Judicial Conference as a rulemaking to allow magistrates to issue warrants for searches in areas under U.S. jurisdiction but outside of federal judicial districts, such as U.S. diplomatic or consular missions, located in foreign nations. However, U.S. jurisdiction in the areas listed in subsection (b)(5) was authorized by Congress. The Committee Notes to subsection (b)(5) state: "The rule is intended to authorize a magistrate judge to issue a search warrant in any of the locations for which 18 U.S.C. §7(9) provides jurisdiction."[20] Accordingly, the language of subsection (b)(5) mirrors that of 18 U.S.C. §7(9), which was first codified through the USA PATRIOT Act of 2001.[21]

The Electronic Communications Privacy Act (ECPA) authorizes multi-district searches of computers.[22] However, this too was an explicit grant of authority from Congress, not an instance of judicial rulemaking.

The proposed changes to FRCrmP Rule 41 are not a Congressional amendment, nor do they implement a direct expansion of extraterritorial jurisdiction codified in statute. Congress has not authorized extraterritorial or multi-district searches for computers with concealed locations or during investigations under 18 U.S.C. 1030(a)(5), as the proposed modification to Rule 41 contemplates. The proposed modification attempts to expand magistrates' Rule 41 authority in a manner that has historically been accomplished by Congressional action. The proposed modification should be handled through Congress rather than judicial rulemaking.

D. The proposed Rule 41 amendment raises new risks of forum shopping.

Authorizing the government to obtain a warrant from any district to search or seize multiple computers located in any district raises a significant risk of forum shopping. The proposed change to Rule 41 would incentivize agents to seek out and reuse districts that were more inclined to approve warrant applications. In practice, this may frequently result in warrants issued in districts remote from the individual whose electronic media is searched or seized, making it prohibitively inconvenient or expensive for the individual to appear in the district to exercise her right to contest the warrant.

---

[19] Sec. 219, 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.

[20] Title 18, U.S. Code, Appendix, Federal Rules of Criminal Procedure, Title VIII, Rule 41, Committee Notes.

[21] *Id.*, fn 19, Sec. 804.

[22] 18 U.S.C. 2703(a), as modified by Sec. 220 of the USA PATRIOT Act of 2001.

III. Technological Implications

The proposed modification to Rule 41 would enable the U.S. government to gain authorization from any district in the United States to spread invasive malware – code that may penetrate, search, and copy electronic media without user authorization – to potentially any computer worldwide. This is essentially allows law enforcement to hack computers with few restrictions on where an intrusion can take place and how many devices to which they may gain entry. It is tailored poorly and can reach practically any computing device while it also implicates many types of common and lawful methods of using the Internet. Finally, the act of intrusion into these devices may substantially damage the devices, the data resident on them, or the functions the devices mediate.

A. "Concealed through technological means" is overly broad.

The trigger language in the proposed amendment that the location of a target device be "concealed through technological means" before a warrant can be issued is overly broad, encompassing legitimate Internet use globally, not just within the United States, on devices for which the primary function is unknown to the government.

The Internet and software that interacts with it – email clients, web browsers, apps, etc. – have developed many ways to conceal a user's location, either intentionally to protect privacy but often as a side effect of accomplishing another goal, such as confidentiality. The intent of this part of the rule amendment seems to be to allow agents of law enforcement to de-anonymize users of online anonymity tools, such as the Tor network. However, there is a much larger ecosystem of similar technologies that encompass technical methods that effectively re-route traffic over the Internet. Close to half of all U.S. businesses use Virtual Private Network (VPN) technologies or other forms of secure proxies.[23] VPNs and secure proxies seek to ensure that a user can interact with sensitive data – e.g., trade secrets, medical data, financial data – even when they are forced to use potentially hostile local networking environments, such as the unencrypted free wireless Internet access offered at hotels, airports, and coffee shops. These technologies establish an fully encrypted secure connection with a trusted server on the Internet, and that trusted server "proxies" their network activity – meaning it appears as if all network traffic comes from the proxy server instead of the user's real network location.

There exist additionally a set of techniques that are designed to misreport identifiers that may associate a user's identity with their activity online. For example, to protect the privacy of the hundreds of millions of users of Apple's iOS mobile operating system from forms of in-store retail tracking that can follow shoppers from store to store, Apple has begun randomizing a common network identifier – the MAC address.[24] This will have the effect of "concealing through technical means" the network location of a device. Finally, the proposed amendment

---

[23] 42% of U.S. business respondents across company size segments use VPNs. See, Nav Chander, "Choosing the Best Enterprise IP VPN or Ethernet Communication Solution for Business Collaboration," *International Data Corporation* (whitepaper produced for AT&T, Inc.), (June 2014), available at: http://www.business.att.com/content/whitepaper/vpn_ethernet.pdf (pg. 2).

[24] Lee Hutchinson, "iOS 8 stymie trackers and marketers through MAC address randomization," *Ars Technica* (June 9, 2014), *available at:* http://arstechnica.com/apple/2014/06/ios8-to-stymie-trackers-and-marketers-with-mac-address-randomization/ (last accessed October 23, 2014).

seems to reach somewhat trivial forms of location obfuscation that are not technically technical but could be construed as such. For example, if a user of a social network service such as Facebook misreports the city in which they live, or if a user of a web browser modifies how the browser reports their native language, these seem to qualify as "concealing through technical means" the user's location. Legitimate uses of technology that have the effect of "concealing through technological means" a user's location, e.g., using a VPN or Apple's iOS mobile operating system, should not trigger the ability for a judge to issue a Rule 41 warrant.

The pervasive nature of technical means that have the purpose or effect of concealing the user's location is indicative that concealment does not necessarily indicate a crime. In fact, the core technology this rule amendment seeks to reach, the Tor network and Tor Broswer software, was developed primarily for two purposes that are fundamentally legitimate: the need of law enforcement as well as military and civilian intelligence agencies to access information services in hostile environments and the need of dissidents in repressive regimes to communicate with the larger, outside world.[25] Additionally, users that may be concerned about their privacy or security given threats online or to their person also use proxy technologies that securely obfuscate their location; this can encompass stalking victims and public servants that face threats of physical harm. Employees of businesses that deal in sensitive data such as finance or medicine may be required to use these kinds of technologies within the scope of their employment; for example, some businesses require their employees to route all traffic through a proxy that can detect viruses or malware, examine traffic for attempts to exfiltrate valuable intellectual property, or even a "caching proxy" that seeks to ease the load on a network by storing commonly retrieved resources such as images, videos, or other large files. Finally, we cannot rule out the possibility that an attempt to conceal location could actually be a simple misconfiguration or other error such that details like a computer's Internet Protocol (IP) address may be misreported.

Of course, technically, a device that uses any of the techniques mentioned above can be anywhere in the world, and the context of the device's true function (or contents) will in general be uncertain. As we outline above in Section II.B, this legally extends U.S. law enforcement jurisdiction globally. To the extent U.S. law enforcement uses this rule to hack into devices around the world, we should not be surprised when law enforcement entities from other nations conclude they should have this ability as well. Outside the question of the compatibility of legal regimes that are best dealt with in formal MLAT processes, there are serious questions about the uncertain functional context of a target device. That is, if the location of a device is unknown, concealed, or uncertain, we should expect that the purpose of the device will also be equally if not more uncertain. Law enforcement will have little data from which to ascertain how careful they need be while executing the search and seizure, lest they irreversibly damage the device, connected devices, or critical functionality the device may mediate. Unlike in the physical world, where the implications of an intrusion into a premises are relatively certain and easy to understand, the consequences in cyberspace can be very difficult to estimate. By way of analogy, in the physical world, agents of law enforcement can be reasonably confident that breaking and entering into premises won't cause the entire building to fall down. Similarly, they can also be reasonably confident that such an intrusion won't also cause the collapse of a

[25] See, e.g., "Who uses Tor?" available at: https://www.torproject.org/about/torusers.html.en.

series of nearby buildings or, for that matter, that a building they thought was a typical family home isn't actually the control system for a nuclear power plant. In cyberspace we cannot be so confident.

B. "Damaged" computers, under 18 U.S.C. 1030(a)(5), covers a very large quantity of machines.

The proposed changes to Rule 41 would allow the government to obtain a warrant in any district to remotely search five or more "damaged" computers during investigations of 18 U.S.C. 1030(a)(5). The justification for this proposal has been discussed in context of law enforcement action against botnets – networks of private computers infected with malware that enables an unauthorized party to use or control all or parts of the infected computers remotely.[26] As the FBI notes, millions of infected computers can be part of a botnet.[27] However, 18 U.S.C. 1030(a)(5) does not only encompass botnets.

18 U.S.C. 1030(a)(5) prohibits causing "damage" to protected computers intentionally without authorization or recklessly. "Damage" is defined broadly under the statute to include any malware, virus, Trojan, or even benign code that impairs "the integrity or availability of data."[28] While botnets may involve using infected computers to commit additional crimes (such as distributed denial-of-service attacks), computers infected with viruses are not necessarily committing any subsequent crime – though the act of damaging the computer by infecting it with a virus is a crime under 1030(a)(5).

Because the proposed modification to Rule 41 would apply to investigations into any violation of 1030(a)(5), not just botnets, the proposed modification would enable the government to more easily remotely search computers infected with any virus or other damaging code. Approximately 30 percent of all computers worldwide, as well as in the United States, are estimated to be infected with some type of malware.[29] The number of computers that may therefore be subject to multidistrict searches under the proposed Rule 41 amendment is massive.

C. Data stored on devices is increasingly sensitive and intrusion may damage the device, its data, and/or dependent systems.

The language of the proposed amendment that allows law enforcement to "use remote access to search electronic storage media to seize or copy electronically stored information" will allow access to data of an exceedingly sensitive nature in many cases.

While the particularity of a warrant under the 4th Amendment requires the government to specify exactly the materials they seek to search for and seize, the proposed amendment would grant access to a panoply of sensors on modern computing platforms. Desktop

---

[26] *Supra*, fn 9, pg. 172.

[27] Botnets 101, Federal Bureau of Investigation, Jun. 5, 2013, available at http://www.fbi.gov/news/news_blog/botnets-101/botnets-101-what-they-are-and-how-to-avoid-them.

[28] 18 U.S.C. 1030(e)(8).

[29] Panda Security, Annual Report PandaLabs, 2013 Summary, pg. 5, available at press.pandasecurity.com/wp-content/uploads/2010/05/Annual-Report-PandaLabs-2013.pdf.

computers, laptop computers, tablet computers and mobile computing devices contain an increasing array of sensors capable of reading current environmental and personal data – for example, microphones, cameras, motion sensors, and more complex accessories such as fitness tracking devices that measure fine-grained body data. Using these sensors, these devices store a multitude of sensitive data over time – personal photographs and videos, financial data, medical records, educational materials. As the Supreme Court recognized recently, networked devices like smartphones increasingly hold "a digital record of nearly every aspect of [our] lives – from the mundane to the intimate."[30] As mentioned above, the target device can be potentially any device attached to the Internet from personal computing devices to industrial control systems to Internet voting systems. Allowing law enforcement a broad remit to remotely access such sensitive information systems will have grave consquences for personal privacy and liberty, as well as the integrity of critical systems.

The acts of intrusion onto a device and/or seizing data may result in impairment of the device or data resident on the device. Intrusion methods necessarily exploit weakness in the defenses of a device to gain access. Practically speaking, "network investigative techniques" employ flaws or bugs in software like web browsers such that law enforcement can gain access to the larger system. Vulnerabilities or flaws in a system are by definition features the designers of the system did not plan the system's functionality to take into account. "Network investigative techniques" used by law enforcement can vary from relatively simple Computer and Protocol Address Verifier (CIPAV) tools that seek to assess and report network identifiers and information back to law enforcement agents to deeper forms of persistent access where invasive methods like rootkits – i.e., programs designed to completely evade system defenses and be highly resistant to removal – which can potentially permanently damage a device. Further, it is unclear from the text of the proposed amendment and relevant jurisprudence if the extent of "seizing" data does not merely copy the data but may also render it unusable by the user. If seizing and copying are distinct in this manner, a seizure of data could potentially deprive the user of critical data or system functionality without due process before a finding of guilt has been made.

The act of intrusion and installing a "network investigative technique" can not only harm the device but also potentially result in further follow-on damage due to vulnerabilities introduced into the system or exacerbated by the technical act of gaining entry. To the extent the intrusion technique causes damage or triggers malware that causes ancillary damage, the device itself may be no longer functional, along with any data it holds and any actions in the real world it performs. There are examples of adversarial network investigation that resulted in taking an entire country off the Internet[31] as well as buggy law enforcement intrusion code that left targeted devices seriously vulnerable to subsequent malicious attacks.[32]

---

[30] *Riley v. California*, 573 U. S. ____ (2014) at 19.

[31] Spencer Ackerman, "Snowden: NSA accidentally caused Syria's Internet blackout in 2012," *The Guardian* (August 13, 2014), available at: http://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war (last accessed October 23, 2014).

[32] Chaos Computer Club, "Chaos Computer Club analyzes government malware," (October 8, 2011), available at: https://www.ccc.de/en/updates/2011/staatstrojaner (last accessed October 23, 2014).

D. Concealment of the location of "information" can potentially reach even more devices.

The proposed amendment does not just trigger on concealing the location of a device with technical means but also concealment of the location of information. Similarly to the discussion above in Section III.A of the variety of activities that by their nature obscure the location of a device, there are a number of modern computing techniques that obscure the location of information, mostly for efficiency gains related to data mining and analysis.

For example, rather than keeping very large databases of information in a single location, many modern computing techniques rely on a technique called "sharding," or the process of breaking up individual pieces of a database and redistributing them across disparate computing facilities. If a target machine has information sharded across tens or hundreds of additional machines, the proposed amendment would appear to reach all of those devices as well. There are more exotic types of data structures – for example, hash tables and bloom filters – that do similar things from the perspective of technically concealing the location of information; some of these techniques are very difficult – by design – to map onto a physical location or the specific device on which the data may be stored.

IV. Practical implications

In addition to the legal and technical implications, we are concerned that a slew of negative practical implications may be relevant once law enforcement gains the abilities contemplated by the proposed rule.

First, the rule essentially eliminates existing practical limits on law enforcement search and seizure in networked computing. The Department of Justice indicated that under the current Rule 41, agents seeking authority to search computers in multiple districts must obtain warrants with magistrates in every district in which the computers are known to be located (except in cases of domestic or international terrorism).[33] As a practical matter, agents currently must be judicious in deciding which computers to remotely search. However, if the requirement to obtain warrants from each district in which the property is known to be located were removed, the likely effect would be for far more remote searches of far more machines. As we argue above, the number of computers for which location is concealed, or which are "damaged" may well run to many millions. The potential for abuse or overzealous and sloppy law enforcement hacking is very real.

Further, there are follow-on implications from this collapsing of practical limitations. Authorizing law enforcement to operate in this manner may lead to more intrusive methods being brought to bear. If malware that reveals computer location is easily bypassed or rendered ineffective, law enforcement may have to use more powerful techniques that are more likely to threaten the integrity of the target device or information. For example, a simple web beacon that can report a device's IP address back to law enforcement can be blocked by common software (e.g., Little Snitch) that prohibits network requests to unknown addresses. The government

[33] *Supra*, fn 9, pg. 173.

may then attempt more intrusive – necessarily less reasonable – searches of the contents of media to gather clues regarding location.

Finally, the proposed rule amendment and the law enforcement hacking that may result has the potential to spark a deadly arms race. Malicious hackers may begin to purposefully stage attacks from computers running critical infrastructure and applications. If an intrusion renders these devices inoperable – either by design or accident – the implications for just one such incident could be profound for society. We may very well see staging of malware on critical infrastructure coupled with "trip wires" that are armed to cause damage and havoc when an attempted intrusion is detected.

V. **This is an issue for Congress**

Law enforcement clearly faces challenges in remotely searching electronic media in concealed locations. However, the proposed rule has important technical, legal, and practical implications that necessitate the deliberation of Congress. We recommend that the Judicial Conference reject the proposed changes to Rule 41 and instead urge Congress to address the issue of remote searches of electronic media located in multiple districts or in unknown locations.

END