Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Main 650 253.0000
Fax 650 253.0001
www.google.com

February 13, 2015

TO: The Judicial Conference Advisory Committee on Criminal Rules

FROM: Richard Salgado, Google Inc.
Director, Law Enforcement and Information Security

RE: **Google Inc. Comments on the Proposed Amendment to Federal Rule of Criminal Procedure 41**

Google Inc. ("Google") writes in opposition to the proposed amendment to Federal Rule of Criminal Procedure 41. Google makes available a variety of Internet-related products and services for people and businesses around the world, including webmail, search, maps, news, and image storage and organization. Google's mission is to organize the world's information and make it universally accessible and useful. Google has a significant interest in protecting its users and securing its infrastructure. The proposed amendment substantively expands the government's current authority under Rule 41 and raises a number of monumental and highly complex constitutional, legal, and geopolitical concerns. Google urges the Committee to reject the proposed amendment and leave the expansion of the government's investigative and technological tools, if any are necessary or appropriate, to Congress.

I. The Proposed Amendment Is a Substantive Expansion of the Government's Search Capabilities That Should Be Left to Congress

A. The government cannot seize evidence outside the United States pursuant to a search warrant that permits remote access of servers abroad.

Under current Rule 41, federal prosecutors must generally seek a warrant in the judicial district to search for and seize a person or property located within the district.[1] This territorial limitation is subject to limited exceptions.[2] Yet, the proposed amendment to Rule 41 would permit a court

[1] Fed. R. Crim. P. 41(b)(1).
[2] *See* Fed. R. Crim. P. 41(b)(2)–(5).

within any district where activities related to a crime may have occurred to issue a warrant authorizing remote access searches of electronic information located within or outside the district in two circumstances: first, where the location of "the media or information . . . has been concealed through technological means," and second, where the search involves "an investigation of a violation of 18 U.S.C. § 1030(a)(5)" and "the media are protected computers that have been damaged without authorization and are located in five or more districts."[3]

Remote searches of media or information that have been "concealed through technological means" may take place anywhere in the world. This concern is not theoretical. A magistrate judge in the Southern District of Texas recently denied an application for a Rule 41 warrant to permit U.S. law enforcement agents to hack a computer whose location was unknown, but whose IP address was most recently associated with a country in Southeast Asia.[4] Such searches clearly violate the extraterritorial limitations of Rule 41. The Department of Justice ("DOJ") urges that "[i]n light of the presumption against international extraterritorial application, . . . [the proposed] amendment does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries."[5] But despite this weak assurance that the amendment does "not purport" to expand the current scope of Rule 41, in reality it will: the nature of today's technology is such that warrants issued under the proposed

---

[3] The proposed change in Rule 41 that permits extraterritorial reach of a Rule 41 search warrant is a different issue than the matter currently before the Second Circuit, which deals with whether a search warrant authorized under the Stored Communications Act ("SCA") and properly served upon a U.S.-based electronic communications service provider is valid where that service provider has custody or control of communications it stores on servers outside the United States. *In re Warrant*, No. 14-2985 (2d Cir. 2014). Here the Committee is seeking by rule to grant extraterritorial reach to Rule 41 warrants and authorize surreptitious searches of remote computers, potentially circumventing both Mutual Legal Assistance Treaties, and SCA procedures in some cases.

[4] *In re Warrant*, 958 F. Supp. 2d 753, 758 (S.D. Tex. 2013) ("But the Government's application would fail nevertheless, because there is no showing that the installation of the 'tracking device' (i.e. the software) would take place within this district. To the contrary, the software would be installed on a computer whose location could be anywhere on the planet.").

[5] Letter from Mythili Raman, Acting Assistant Att'y Gen., U.S. Dep't of Justice, to Reena Raggi, Chair, Advisory Comm. on the Criminal Rules 4 (Sept. 18, 2013), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2013-10.pdf.

amendment will in many cases end up authorizing the government to conduct searches outside the United States.

The government has previously offered the theory that a search or seizure does not occur pursuant to a Rule 41 warrant until the government examines the data.[6] Under this rationale, a remote search by the government of media or information located in another country would not violate Rule 41's extraterritoriality limitations because no search would occur outside U.S. borders. But this logic must be, and has been, rejected.[7] A search or seizure occurs at the moment when the government secures the data.[8] Therefore, where the government accesses servers located abroad to obtain information pursuant to a Rule 41 warrant, there is no doubt that a seizure of such data will occur outside U.S. territorial limits.

Accordingly, while the proposed amendment "purports" not to substantively expand the government's search powers under Rule 41, it in effect does so anyway. Such a change is for Congress to effect, not the Committee.

Moreover, as the Committee must understand, the United States has long recognized the sovereignty of nations.[9] To this end, it is well established that "[a]bsent a treaty or other agreement between nations, the jurisdiction of law enforcement agents does not extend beyond a nation's borders."[10] Stated differently, "[a] state's law enforcement officers may exercise their

---

[6] *In re Warrant*, 958 F. Supp. 2d at 756 ("Even though the Government readily admits that the current location of the Target Computer is unknown, it asserts that this subsection authorizes the warrant because information obtained from the Target Computer will first be *examined* in this judicial district.") (emphasis added) (internal quotation marks and citation omitted).

[7] *Id.* at 757 ("By the Government's logic, a Rule 41 warrant would permit FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until the agents haul it off to the issuing district.").

[8] *See, e.g.*, *United States v. Ganias*, 755 F.3d 125, 135–36 (2d Cir. 2014) (copying electronic data constitutes a seizure).

[9] *See, e.g.*, *The Schooner Exchange v. McFaddon*, 11 U.S. (7 Cranch) 116, 136 (1812) ("The jurisdiction of the nation within its own territory is necessarily exclusive and absolute. It is susceptible of no limitation not imposed by itself."), *superseded by statute as stated in Siderman de Blake v. Republic of Argentina*, 965 F.2d 699 (9th Cir. 1992).

[10] L. Song Richardson, *Convicting the Innocent in Transnational Criminal Cases: A Comparative Institutional Analysis Approach to the Problem*, 26 Berkeley J. Int'l L. 62, 80 (2008); *see also United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990) (seven justices endorsing the view that U.S. courts may not issue search warrants for foreign searches); *cf.*

functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state."[11] The U.S. has many diplomatic arrangements in place with other countries to cooperate in investigations that cross national borders, including Mutual Legal Assistance Treaties (MLATs).[12] Generally, these arrangements allow "for the exchange of evidence and information in criminal and related matters."[13] Google, and many other service providers, have long encouraged and supported the efforts of the Administration and Congress to improve these processes, but the proposed amendment undermines those efforts.[14]

B. The proposed amendment alters constitutional rights and violates the Rules Enabling Act.

The proposed amendment is a substantive change that imposes upon the constitutional rights of targets in violation of the Rules Enabling Act, which provides that rules of practice, procedure, and evidence may be adopted so long as they do not "abridge, enlarge, or modify any substantive right." 28 U.S.C. § 2072(b). Although the proposed amendment disclaims association with any constitutional questions,[15] it invariably expands the scope of law enforcement searches, weakens

---

Weinberg v. United States, 126 F.2d 1004, 1006 (2d Cir. 1942) ("With very few exceptions, United States district judges possess no extraterritorial jurisdiction.").

[11] Restatement (Third) of Foreign Relations Law § 432(2); *see also id.* § 433(1) ("Law enforcement officers of the United States may exercise their functions in the territory of another state only (a) with the consent of the other state and if duly authorized by the United States; and (b) in compliance with the laws both of the United States and of the other state.").

[12] *See, e.g.*, Bureau of Int'l Narcotics & Law Enforcement Affairs, U.S. Dep't of State, 2012 International Narcotics Control Strategy Report (INCSR) (Mar. 7, 2012), http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm.

[13] *Id.*

[14] *See, e.g.*, Reform Government Surveillance, *Global Government Surveillance Reform*, Principle 5, https://www.reformgovernmentsurveillance.com/ ("In order to avoid conflicting laws, there should be a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions, such as improved mutual legal assistance treaty — or "MLAT" — processes."); Exec. Office of the President, Office of Mgmt. & Budget, *Statement of Administration Policy on H.R. 4660 — Commerce, Justice, Science, and Related Agencies Appropriations Act, 2015* (May 28, 2014), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr4660h_20140528.pdf (MLAT improvement "is critical to investigating crimes, working with foreign partners, and prosecuting terrorists and other criminals. This funding will provide for an updated, improved, and accelerated process to handle foreign governments' requests for evidence as well as enhance mutual relationships.").

[15] *See* Fed. R. Crim. P. 41 committee note (proposed Apr. 21, 2014), *available at* http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf.

the Fourth Amendment's particularity and notice requirements, opens the door to potentially unreasonable searches and seizures, and expands the practice of covert entry warrants. The Committee asserts that "the proposed amendment's language speaks directly only to venue, and . . . the proposed commentary makes clear that the government must satisfy constitutional requirements with respect to any warrant."[16] But the two provisions of current Rule 41 that authorize the commencement of searches outside the issuing district were both the result of congressional action under the USA PATRIOT Act, and were not, as here, the unilateral work of the Committee.[17]

The substantive changes offered by the proposed amendment, if they are to occur, should be the work of congressional lawmaking. Such was the case with a slew of legislation providing law enforcement with the ability to use technological means to conduct invasive searches on targets, including the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1804, which provides law enforcement with the ability to legally surveil and collect foreign intelligence information; Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), 18 U.S.C. § 2518, which provides law enforcement with the ability to legally intercept wire, oral, and electronic communications; the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*, which provides law enforcement with the ability to legally access electronically stored communications; and the Pen Registers and Trap and Trace Act, 18 U.S.C. § 3123, and USA PATRIOT Act, 50 U.S.C. § 1842, both of which provide law enforcement with the ability to legally intercept real time telephony metadata. In passing this legislation, Congress was able to openly debate and weigh the various constitutional issues at play.

---

[16] *See* Memorandum from Sara Beale & Nancy King to Criminal Rules Advisory Committee 1 (Mar. 17, 2014) ("Beale Memorandum"), *available at* http://www.uscourts.gov/uscourts/rulesandpolicies/rules/agenda%20books/criminal/cr2014-04.pdf.

[17] *See* 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. § 219 (amending Rule 41 to include the power to issue a search warrant for a person or property outside the district in a terrorism investigation); Fed. R. Crim. P. 41, advisory committee notes (2008) (noting that subsection (b)(5) is intended to authorize the issuance of a search warrant "in any of the locations for which 18 U.S.C. § 7(9) provides jurisdiction"); *see also* USA PATRIOT Act of 2001 § 804.

Legislation, not rule-making, is the proper way to balance legitimate law enforcement needs with serious constitutional and policy considerations.

II. The Proposed Amendment Is Vague and Fails to Specify How Searches May Be Conducted and What May Be Searched

It is unclear what types of searches are being authorized by the proposed amendment. The proposed amendment provides that the government may use "remote access" to search and seize or copy electronically stored data. The term "remote access" is not defined. Sample search warrants submitted by the DOJ to the Committee indicate that "remote access" may involve network investigative techniques, or NITs, which include, for example, the installation of software onto a target device to extract and make available to law enforcement certain information from the device, including IP address, MAC address, and other identifying information.[18] One sample warrant describes the deployment of an NIT onto a website to redirect certain information entered into the website to the government.[19] None of the sample warrants provide any details regarding the nature of the NIT being deployed, technical details specifying how the NIT will extract the specified information, or details regarding how the NIT will avoid collecting information belonging to non-targets who may innocently access the targeted website or share the targeted device or account. In short, "remote access" seems to authorize government hacking of any facility wherever located.

There are a myriad of serious concerns accompanying the government's use of NITs. These are outlined in detail in other comments submitted to the Committee and include, among other things, the creation of vulnerabilities in the target device thereby increasing the target's risk of

---

[18] *See* Memorandum from Jonathan Wroblewski, Office of Policy & Legislation, to Judge John F. Keenan regarding Proposed Amendment to Rule 41 of the Federal Rules of Criminal Procedure (Jan. 17, 2014) ("Wroblewski Memorandum"), *available at* http://www.uscourts.gov/uscourts/rulesandpolicies/rules/agenda%20books/criminal/cr2014-04.pdf.

[19] *Id.*

exposure to compromise by other parties, actual damage to the target device, the creation of a market for zero-day exploits, and unintended targets' exposure to malware.[20] Additionally, the remote facilities accessed by the government may in fact identify and disclose the "hack" or take action to prevent it or retaliate against its use. These are serious concerns that are more appropriately considered and balanced by Congress than by the Committee.

In addition to failing to specify or limit how searches may be conducted, the proposed amendment also fails to specify or limit what, precisely, may be searched once the media or information is accessed. The proposed amendment would allow the government to "use remote access to search electronic storage media and to seize or copy electronically stored information" where "the district where the media or information is located has been concealed through technological means." The phrase "concealed through technological means" is not defined and, as written, can be used to justify searches of widespread and legitimate Internet use. For example, this language extends to those who use Virtual Private Networks (VPNs) (as do businesses across the country), which provide a secure connection to sensitive data but also obscure a user's actual network location.[21] Therefore, routine use of lawful encryption technology would appear to satisfy the standard.[22] Moreover, the proposed amendment contains no "intent" element to the concealment, which would require probable cause to believe that the

---

[20] *See* ACLU Memorandum to the Advisory Comm. on Criminal Rules (Oct. 31, 2014) ("ACLU Memorandum"), *available at* https://www.aclu.org/files/assets/aclu_comment_on_remote_access_proposal.pdf.

[21] *See, e.g.*, Written Statement of the Center for Democracy & Technology Before the Judicial Conference Advisory Comm. on Criminal Rules (Oct. 24, 2014) ("CDT Memorandum"), *available at* https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/10/CDT-Rule41-Written-Statement-final-20141024.pdf.

[22] A number of news outlets have reported that Attorney General Eric Holder has authorized the National Security Agency to collect and indefinitely retain encrypted data, regardless of its U.S. or foreign origin, "for a period sufficient to allow thorough exploitation" of that data. Andy Greenberg, *Leaked NSA Doc Says It Can Collect And Keep Your Encrypted Data As Long As It Takes To Crack It*, Forbes (June 20, 2013, 6:21 PM), http://www.forbes.com/sites/andygreenberg/2013/06/20/leaked-nsa-doc-says-it-can-collect-and-keep-your-encrypted-data-as-long-as-it-takes-to-crack-it/; *see also* Declan McCullagh, *NSA 'secret backdoor' paved way to U.S. phone, e-mail snooping*, CNET (Aug. 9, 2013, 11:16 AM), http://www.cnet.com/news/nsa-secret-backdoor-paved-way-to-u-s-phone-e-mail-snooping/. The government therefore considers the mere use of encryption as a red flag that raises the suspicion of criminal misconduct. Law enforcement's suspicion of perfectly lawful activity indicates that the amendment as drafted may be fertile grounds for abuse.

target was purposefully concealing its location. Title III, for example, authorizes roving wiretaps only when the government can show that a target is switching facilities to avoid interception.[23]

Likewise, the phrase "media" is not defined. This opens the door to law enforcement's unfettered access to whatever information is accessible on the device being searched—whether that information is stored locally, on a network drive, or in the cloud. Devices such as computers and cell phones locally store or provide access to vast amounts of information that the Supreme Court has recognized amount to "the privacies of life."[24]

III. The Proposed Amendment Raises Serious Constitutional Concerns, and Case Law Addressing the Same Will Be Slow to Develop

The serious and complex constitutional concerns implicated by the proposed amendment are numerous and, because of the nature of Fourth Amendment case law development, are unlikely to be addressed by courts in a timely fashion.

First, the proposed amendment raises serious questions as to how the Fourth Amendment particularity requirement will be satisfied in applications submitted under Rule 41. The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[25] In what ways will warrant applications specify what "storage media" will be searched? And how will law enforcement maintain certainty that only specified media is accessed? Will warrants issued under the proposed amendment provide any detailed assurances that non-targets will not be affected by the search? The sample warrant applications submitted

[23] 18 U.S.C. § 2518(11)(b)(ii) (requiring "probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility").
[24] *Riley v. California*, 134 S. Ct. 2473, 2494–95 (2014).
[25] U.S. Const. amend. IV.

by the DOJ, and case law addressing a similar warrant application, show that warrants issued under the new rules are not likely to satisfy the Fourth Amendment.[26]

Second, there are legitimate concerns that the use of NITs to conduct remote access searches may constitute an unreasonable search because of their destructive and unpredictable nature. As noted by the ACLU in its comments to the Committee, the use of various forms of NITs, including malware and zero-day exploits, are more invasive than other searches because they often have unknown, widespread, and sometimes destructive consequences.[27]

Third, the types of searches authorized by the proposed amendment may circumvent the "super warrant" requirements of Title III.[28] Title III applies to any government interception of wire, oral, or electronic communications.[29] Wiretap orders issued under Title III require protections absent from traditional warrants, including that the applicant show that it has exhausted other investigative techniques and that interception of non-necessary communications will be minimized.[30] Additionally, the DOJ Office of Enforcement Operations reviews each wiretap application before it is submitted to a court.[31]

The NITs deployed on target devices could in many instances have wide-ranging capabilities for accessing and engaging various features of the device, including the device's camera and microphone.[32] To the extent that a remote access search engages in techniques such as activating

---

[26] *See* Wroblewski Memorandum, *supra* note 17; *In re Warrant*, 958 F. Supp. at 759 ("The Government's application offers nothing but indirect and conclusory assurance that its search technique will avoid affecting innocent computers or devices," and the application fails to "explain how [the Government] will ensure that only those committing the illegal activity will be subject to the technology.") (internal quotations omitted).

[27] ACLU Memorandum, *supra* note 19, at 17–18.

[28] 18 U.S.C. § 2518.

[29] *Id.*

[30] *Id.*

[31] *See U.S. Attorneys Criminal Resource Manual* § 89, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00089.htm.

[32] *See, e.g.*, *In re Warrant*, 958 F. Supp. 2d at 755–56 (warrant application to install NIT software that would enable the government to take photographs using the target computer's built-in camera).

built-in cameras or microphones or collecting real-time ingoing or outgoing electronic communications, the heightened protections of Title III would be implicated.[33] It does not appear that the government has, to date, acknowledged the Title III implications of NITs with the Committee or offered a proposal for how it plans to address the issue. This raises the concern that the government will be reluctant to describe techniques to courts that may not always be sensitive to the possibility that Title III is implicated.

Fourth, the proposed amendment weakens Rule 41's notice requirement. Under current Rule 41, law enforcement must provide "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."[34] Under the proposed amendment, law enforcement need only "make reasonable efforts to serve a copy of the warrant on the person whose property was searched or whose information was seized or copied."[35] If the person whose property is seized is different from the person whose information was copied, only one person need be notified. The relaxed notice standard clearly indicates that warrants issued under the proposed amendment will in many instances be targeted at those to whom no notice can feasibly be given, such as when law enforcement is unsuccessful in ascertaining the target's physical location.

A search without notice is tantamount to a covert entry. Covert searches must be "closely circumscribed,"[36] and "the absence of any notice requirement in [a] warrant casts strong doubt on its constitutional adequacy."[37] The Ninth Circuit has held that a warrant is constitutionally

---

[33] 18 U.S.C. § 2518; *see also United States v. Torres*, 751 F.2d 875, 885 (7th Cir. 1984) (surveillance that "is identical in its indiscriminate character to wiretapping and bugging" requires Title III protections); *see also United States v. Cuevas-Sanchez*, 821 F.2d 248, 250 (5th Cir. 1987) (requiring Title III protections for video surveillance).
[34] Fed. R. Crim. P. 41(f)(1)(C).
[35] Proposed Amendment to Rule 41 revised draft – April 21, 2014, *available at* http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf.
[36] *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986).
[37] *Id.* (citing *Berger v. New York*, 388 U.S. 41, 60 (1967)).

defective where it fails "to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry."[38]

The nature of Fourth Amendment case law development will make it difficult for courts to address these constitutional concerns any time in the near future, casting serious doubt on the Committee's reliance on courts to address the numerous and significant constitutional issues raised by the proposed amendment. These issues are likely to evade review for a number of reasons.

First, warrant applications are considered ex parte and without the benefit of adversarial perspective by magistrate judges who may lack technical expertise or resources to comprehend the nature or the risks of the search proposed. This is especially true if the warrant applications do not provide the necessary description for the judge to understand the technique being used or to appreciate the constitutional consequences of that technique. This makes it unlikely that the issues will be caught in the warrant application phase.

Second, courts will often apply the good faith exception to the exclusionary rule prior to addressing the underlying constitutional issues implicated by the search, leaving any discussion of the Fourth Amendment challenge as dicta or, worse, foregoing any constitutional discussion at all.[39] Worse yet, law-abiding citizens who were the target of an unconstitutional search but are not charged with a crime will almost certainly never learn of the search and therefore will not be able to challenge the search.[40]

---

[38] *Id.*

[39] *See, e.g.*, *United States v. Clay*, 646 F.3d 1124, 1128 (8th Cir. 2011) (denying a motion to suppress on the basis of the good faith exception and declining to "reach the underlying question of probable cause").

[40] *Cf.* Stephen W. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 Harv. L. & Pol'y Rev. 313, 328 (2012) (discussing a target's ability to challenge an electronic surveillance order issued under the Electronic Communications Privacy Act ("ECPA")).

Likewise, in those cases where the doctrine of qualified immunity applies, courts will often apply the doctrine first and forego a constitutional discussion altogether.[41] Qualified immunity "protects government officials from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known."[42] In other words, the doctrine "protects all but the plainly incompetent or those who knowingly violate the law."[43] Under the doctrine, where the government relies on a warrant issued by a magistrate judge, courts have held that the government generally "cannot be expected to" question the magistrate judge's determination that the warrant was proper.[44]

Therefore, without previously established precedent or statutory law on the constitutionality of the searches permitted under the proposed amendment, case law discussing the constitutionality of such searches will develop slowly at best.[45] The Committee acknowledges that "there have not yet been many published opinions dealing with the various scenarios that would be covered by the proposed amendment," but reasons that "these situations are likely to arise more frequently."[46] Because this is in fact not likely to be the case, leaving constitutional questions to the courts will be an ineffective means of addressing the serious constitutional issues raised by the proposed amendment.

Additionally, the Committee should not reject the opinion of the at least one court that *has* addressed the extraterritorial effects of Rule 41 warrants that purport to authorize searches of computers outside the U.S.[47] That court denied a warrant application to remotely search a target

---

[41] *See, e.g., Messerschmidt v. Millender*, 132 S. Ct. 1235, 1249 (2012) (foregoing a constitutional analysis after holding that qualified immunity applies).
[42] *Id.* at 1244 (internal quotation marks and citation omitted).
[43] *Id.* (internal quotation marks and citation omitted).
[44] *Id.* at 1245.
[45] *Cf.* Smith, *supra* note 39, at 326–31 (discussing the dearth of appellate case law addressing ECPA in the 25 years since its enactment, and citing the lack of incentive to appeal ECPA orders as a cause: "The inevitable result is that appellate courts are rarely presented with the opportunity to interpret and apply ECPA's complex provisions").
[46] *See* Beale Memorandum, *supra* note 15, at 1.
[47] *In re Warrant*, 958 F. Supp. 2d 753, 758 (S.D. Tex. 2013).

computer whose location was unknown, citing many of the same constitutional infirmities Google raises today.[48]

IV. The Proposed Amendment Would Authorize Remote Searches of Millions of Computers

The proposed amendment authorizes searches for investigations under § 1030(a)(5) of the Computer Fraud and Abuse Act ("CFAA").[49] As the Committee notes, "[t]he proposal would enable investigators to obtain warrants to search computers in many districts simultaneously."[50] Such search capabilities would enable law enforcement to investigate robot networks, or botnets, which are "automated malware program[s] that scan[] blocks of network addresses and infect[] vulnerable computers."[51] According to the FBI, a network of botnets can number "in the hundreds of thousands or even millions."[52] The implications of such searches should be left to Congress to weigh and to craft a statute that balances the privacy rights of affected network owners or operators with the investigative needs of law enforcement.

Subpart (B) of the proposed amendment extends beyond botnet searches, however. The definition of "damaged computer" under the CFAA is broad, encompassing "any impairment to the integrity or availability of data, a program, a system, or information."[53] "Damage" may encompass, for example, software infected with unwelcome code,[54] malware, or viruses. As

---

[48] *Id.*

[49] This provision makes it a crime to "(A) knowingly cause[ ] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[ ] damage without authorization, to a protected computer; (B) intentionally access[ ] a protected computer without authorization, and as a result of such conduct, recklessly cause[ ] damage; or (C) intentionally access[ ] a protected computer without authorization, and as a result of such conduct, cause[ ] damage and loss." 18 U.S.C. § 1030(a)(5).

[50] Beale Memorandum, *supra* note 15, at 3.

[51] Fed. Bureau of Investigation, *Botnets 101* (June 5, 2013, 7:00 AM), http://www.fbi.gov/news/news_blog/botnets-101/botnets-101-what-they-are-and-how-to-avoid-them.

[52] *Id.*

[53] 18 U.S.C. § 1030(e)(8).

[54] *See, e.g.*, *United States v. Sullivan*, 40 F. App'x 740 (4th Cir. 2002).

noted by another commentator, it is estimated that nearly thirty percent of computers in the United States are infected with some form of malware.[55]

Computers that have suffered "damage", therefore, encompass computers belonging to millions of average Americans, many of whom are the victims of cybercrime, and the proposed amendment would permit remote searches into those computers.

V. Conclusion

Google urges the Committee to reject the proposed amendment to Rule 41. As Google has explained above, the proposed amendment substantively expands the government's current authority under Rule 41 and raises a number of monumental and highly complex constitutional, legal, and geopolitical concerns that should be left to Congress to decide.

[55] *See* CDT Memorandum, *supra* note 20, at 8 (citing Panda Security, Annual Report, PandaLabs (2013), *available at* http://www.pandasecurity.com/mediacenter/wp-content/uploads/2010/05/Annual-Report-PandaLabs-2013.pdf).