Testimony of Amie Stepanovich

Senior Policy Counsel, Access

on behalf of

Access and the Electronic Frontier Foundation

Before the Advisory Committee on Criminal Rules

on the Matter of Proposed Amendments to the Federal Rules of Criminal Procedure, Rule 41

I would like to thank the members of the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States for allowing me to testify in front of you today. My name is Amie Stepanovich and I am Senior Policy Counsel with Access, an international digital rights non-governmental organization.[1] Founded in the wake of the 2009 Iranian post-election crackdown, Access seeks to defend and extend the digital rights of users around the world.[2] Today I am also testifying on behalf of the Electronic Frontier Foundation.[3] The Electronic Frontier Foundation, or EFF, was founded in 1990 and champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development.[4]

Introduction

[1] Access, https://www.accessnow.org (last visited Oct. 29, 2014).

[2] *About Us*, Access, https://www.accessnow.org/about (last visited Oct. 29, 2014). I would like to thank Access Junior Policy Counsel Drew Mitnick, Access Policy Intern Jack Bussell, and Access Tech Policy and Programs Manager Michael Carbone for their contributions to this testimony.

[3] Electronic Frontier Foundation, https://www.eff.org (last visited Oct. 29, 2014).

[4] *About EFF*, Electronic Frontier Foundation, https://www.eff.org/about (last visited Oct. 29, 2014). EFF Staff Attorney Hanni Fakhoury, Senior Staff Technologist Seth Schoen, Senior Staff Attorney Jennifer Lynch, and Senior Staff Attorney Lee Tien contributed to this testimony.

My testimony today will focus on the second proposed change to Federal Rule of Criminal Procedure 41.[5] Specifically, the proposed change I would like to discuss grants magistrate judges authority to issue warrants within an investigation under the Computer Fraud and Abuse Act to remotely search protected computers that have been damaged without authorization and to seize or copy electronically stored information on those computers when the computers are located in five or more districts and are not otherwise within that magistrate's jurisdiction.[6] As discussed in the relevant Committee Note, this change specifically involves the creation and control of "botnets."[7] Today, I will provide to the committee some technical background on botnets, the unique natures of botnets that would cause the rule change to have an overbroad, substantive impact on computing, and how the Department of Justice's interpretation of the Computer Fraud and Abuse Act,[8] or CFAA, could compound these impacts. I will end discussing how the proposed change could cause more harm than good in practice. Instead, we propose that a statutory solution is pursued to address the special challenges of unlawful botnets.

What are botnets?

The term "botnet" is short for "robot network." A botnet is a network of computers that have been linked together.[9] Botnets can consist of anywhere from a few computers to several million, as was the case with the Mariposa botnet, which was shut down in 2009,[10] as well as

[5] Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil and Criminal Procedure, 338-42 (August 2014), *available at* http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf.

[6] *Id.*

[7] *Id*.

[8] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2014).

[9] *Build you own botnet with open source software*, WIRED, http://howto.wired.com/wiki/Build_your_own_botnet_with_open_source_software#Business_Usages (last visited Oct. 29, 2014).

[10] John Leyden, *How FBI, police busted massive botnet*, The Register (Mar. 3, 2010), *available at* http://www.theregister.co.uk/2010/03/03/mariposa_botnet_bust_analysis/.

the most infamous botner, the Conficker, first discovered in 2008.[11] Unlawful botnets are created when computers are infected with malicious code, known as malware.[12] The type of malware that creates a botnet allows the infected computer to be remotely accessed and controlled by a third party, often without the owner's knowledge.[13] The infected computers in a botnet are sometimes known as "zombies."[14]

Botnet malware may sit stagnant on an infected computer for months or years without causing any additional harm to the computer itself or any other system, and without coming to the attention of the computer's owner or operator. Some botnets may never actually be utilized and may be patched without incident. In the case of Conficker, the botnet went largely unused despite its massive size, resiliency, and duration.[15]

Not all networked computers are intended for malicious or unlawful purposes. Lawful systems that closely resemble botnets in structure also exist and are used for communication and coordination.[16] In business contexts, these systems may be used to create a cloud computing system, to capitalize on spare computing resources, to balance application loads, and for testing purposes.[17] They may also be created and used to harness processing power in order to conduct scientific experiments or monitor emerging weather patterns.[18]

[11] *The 'Worm' That Could Bring Down The Internet*, NPR (Sept. 27, 2011 12:12 PM ET), http://www.npr.org/2011/09/27/140704494/the-worm-that-could-bring-down-the-internet.

[12] *Malware*, Norton by Symantec, http://us.norton.com/security_response/malware.jsp (last visited Oct. 29, 2014).

[13] *Bots and Botnets--A Growing Threat*, Norton by Symantec, http://us.norton.com/botnet/ (last visited Oct. 29, 2014).

[14] *Id.*

[15] One version of the botnet was eventually utilized to download and install additional malware. *Conflicker*, Wikipedia.org, https://en.wikipedia.org/wiki/Conficker#End_action (last visited Oct. 29, 2014).

[16] *About Eggdrop*, Eggsheads Development Team (Oct. 2, 2011), http://cvs.eggheads.org/viewvc/eggdrop1.6/doc/ABOUT?view=markup. Additionally, other lawful computer networks are encompassed under the terms of the proposed rule, namely systems of protected computers located in five or more districts. Examples are CDNs, P2P systems, and websites run on shared resources.

[17] *Build you own botnet with open source software*, WIRED, http://howto.wired.com/wiki/Build_your_own_botnet_with_open_source_software#Business_Usages (last visited Oct. 29, 2014).

[18] *ATLAS@Home*, CERN, http://atlasathome.cern.ch/ (last visited Oct. 29, 2014); Katherine Smyrk & Liz Minchin, *How your computer could reveal what's driving record rain and heat in Australia and NZ*, The

Substantive Impacts of the Proposed Rule 41 Amendment

On account of their distributed nature, investigations of unlawful botnets undoubtedly pose a significant barrier to law enforcement. Access and EFF empathize with these challenges and are willing to work with members of Congress and leaders in law enforcement to develop an appropriate and rights-respective response. However, due to the same considerations, the proposed rule change presented today as a procedural modification would have a significant substantive impact, including on rights otherwise guaranteed under the Fourth Amendment and international law. Accordingly, we urge the rejection of the proposed amendment to Rule 41 in favor of pursuit of a statutory solution promulgated democratically in an open, public, and accountable legislative process.

The CFAA, initially passed in 1986, has traditionally been used to prosecute the theft of private data or damage to systems by way of malicious hacking.[19] The CFAA was designed to provide justice for victims of these activities by offering a remedy against the perpetrators - the plain text of the relevant section of the CFAA clearly focuses on knowing or intentional malicious activity.[20] Using this authority, magistrate judges issue warrants against those who create and use unlawful botnets, controlling the infected computers of otherwise innocent users.[21] However, the proposed amendment unilaterally expands these investigations to further encompass the devices of the victims themselves - those who have already suffered injury and are most at risk by the further utilization of the botnet.[22] And, as noted, a single

Conversation (March 25, 2014, 11:24 EDT), http://theconversation.com/how-your-computer-could-reveal-whats-driving-record-rain-and-heat-in-australia-and-nz-24804.

[19] *See e.g.,* United States v. Norris, 928 F.2d 504, (2nd Cir. 1991); United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).

[20] *See* 18 U.S.C. § 1030(a)(5) for “knowingly” and “intentionally” language.

[21] *See* Microsoft Corp. v. Does 1-18, No. 1:13cv139 (LMB/TCB), 2014 WL 1338677, (E.D. Va. April 2, 2014).

[22] *Supra* note 5. The proposed amendment would permit law enforcement to “. . . use remote access to search electronic storage media [when] the media are protected computers . . . “

botnet can include millions (or tens of millions) of victim's computers, which may be located not only across the United States, but anywhere around the world.[23]

Victims of botnets include journalists, dissidents, whistleblowers, members of the military, lawmakers and world leaders, or protected classes. Each of these users, and any other user subject to search or seizure under the proposed amendment, has inherent rights and protections under the U.S. Constitution, the International Covenant on Civil and Political Rights, and/or other well-accepted international law.[24] Without reference to or regard for these rights and protections, the proposed change would subject any number of these users to state access to their personal data on the ruling of any district magistrate. This is a substantive expansion of the CFAA. Today we are in the midst of a national, not to mention global, conversation about the appropriate scope of government surveillance. The U.S. Congress is actively considering a number of proposals to reform both international and domestic surveillance activities.[25] The proposed amendment is an end run around this process.

Further complicating matters, the proposed change being considered here today will likely have ramifications for a large number of users who are not even a part of a botnet. These users may be tangentially connected to a botnet through any number of means, such

[23] Notably, the provision in the CFAA relevant to the rule change addresses harm to a single computer - each provision in 18 U.S.C. § 1030(a)(5) addresses access to a "protected computer" - that is, one single computer, or, perhaps in some circumstances, a small network of computers operated by a single entity. A "protected computer" has been, at its most expansive, a corporate or government computer network.

[24] *See, e.g., Scope: Extra-territorial Application of Human Rights Treaties*, Necessary and Proportionate, https://en.necessaryandproportionate.org/LegalAnalysis/scope-extra-territorial-application-human-rights-treaties (last vistited OCt. 29, 2014).

[25] *See, e.g.,* Kurt Opsahl & Rainey Reitman, *A Floor, Not a Ceiling: Supporting the USA FREEDOM Act as a Step Towards Less Surveillance*, Electronic Frontier Foundation (Nov. 14, 2013), https://www.eff.org/deeplinks/2013/11/floor-not-ceiling-supporting-usa-freedom-act-step-towards-less-surveillance; *The USA FREEDOM Act's Long Road*, Access, https://www.accessnow.org/pages/usa-freedom-act (last visited Oct. 29, 2014); Amie Stepanpovich, *Virtual Integrity: Three steps toward building stronger cryptographic standards* (Sept. 18, 2014 4:43am), https://www.accessnow.org/blog/2014/09/18/virtual-integrity-the-importance-of-building-strong-cryptographic-standards ("U.S. Representative Alan Grayson and other lawmakers have introduced legislation to remove the mandatory requirement for NIST to consult with NSA (though still permit the consultation) and strictly prohibit the NSA from artificially weakening standards.").

as the use of a common shared server or service provider. For example, earlier this year Microsoft applied to a federal judge for a court order to assist in dismantling a pair of botnets that encompassed a total of about 18,000 computers.[26] The resulting action led to the disruption of service for nearly 5,000,000 legitimate websites or devices on which 1,800,000 additional non-targeted users were engaging in legitimate, constitutionally protected speech.[27] These other users had no connection to the botnets nor were they known to have broken any law, and instead were only guilty of using the same service as the botnet operators, a fact that caused a public outcry among the public and civil society.[28]

While the Microsoft case was a civil action, and not pursued in a criminal context, it is a good example of the the unsettled legal nature of these issues and the difficulty in crafting narrowly-tailored and appropriate remedies. This potential for far-flung damage requires a careful balancing of rights and responsibilities that is best accomplished through the public legislative process.

Overbroad Application of the CFAA

The above problems are exacerbated by overbroad interpretations of the CFAA itself. Federal prosecutors have forcibly expanded the scope of the CFAA through the overuse of the "without authorization" prong to encompass a range of unanticipated, and patently

[26] The court order applied to 18,000 subdomains. Many of these were likely individual personal computers, though it is possible that a small percentage were actually not individual computers. Microsoft Corp. v. Mutairi et al., No. 14-cv-0987,
(D. Nev. June 19, 2014) (Brief in support of App. for TRO), *available at* http://www.noticeoflawsuit.com/docs/Brief%20in%20Support%20of%20Ex%20Parte%20Application%20for%20a%20TRO.pdf#page=9. For clarity, we will refer to each subdomain as an individual computer.

[27] Natalie Goguen, *Update: Detail on Microsoft Takeover*, noip.com (July 10, 2014), http://www.noip.com/blog/2014/07/10/microsoft-takedown-details-updates/?utm_source=email&utm_medium=notice&utm_campaign=microsoft-takedown-update.

[28] *Id.*; Nate Cardozo, *What Were They Thinking? Microsoft Seizes, Returns Majority of No-IP.com's Business*, Electronic Frontier Foundation (July 10, 2014), https://www.eff.org/deeplinks/2014/07/microsoft-and-noip-what-were-they-thinking; Brandon Moss, *So many botnets, so little time: U.S. Senate holds a hearing to combat "thing-bots,"* Access (July 18, 2014 4:03pm), https://www.accessnow.org/blog/2014/07/18/the-senate-holds-a-hearing-to-combat-thing-bots.

inappropriate, activities: users have been charged with violating the CFAA for violating online terms of service, researching website vulnerabilities, and lying on social media profiles.[29]

Aaron's Law - so named for technologist Aaron Swartz who was aggressively prosecuted under the CFAA eventually leading to his suicide - has been introduced in the House of Representatives by Representative Zoe Lofgren with six co-sponsors to restrict these overuses.[30] However, until either Congress or the U.S. Supreme Court are able to permanently rectify these mis-applications of the CFAA, there is a danger that the proposed amendment could be used in a shocking number of unintended instances. This is particularly concerning because, as explained above, there are several properly-established and otherwise lawful computer networks that the proposed rule would likely encompass. Increasing the potential impact of the proposed amendment, any small networked group of computers may be subject to invasive surveillance at the whim of an overzealous prosecutor and a compliant judge. Further, as also explained above, since the proposed amendment targets victim computers and not the devices of bad actors, it would be enough for a computer connected to a lawful network to carry a virus or to have violated a standard shrinkwrap agreement to justify this surveillance, a move that carries heavy implications for constitutional rights and rights under international law.

The Proposed Amendment in Practice

I have described how the proposal could bring an enormous number of computers belonging to innocent users into the purview of the CFAA and subject them to law enforcement surveillance. In applying the proposed amendment, it is likely that law

[29] *See e.g.,* United States v. Nosal, 676 F.3d 854 (9th Cir. 2012); United States v. Drew, 259 F.R.D. 449 (C.D. Ca. 2009); *see also* Declan McCullagh, *From 'WarGames' to Aaron Swartz: How U.S. anti-hacking law went astray,* C|NET (March 13, 2013 4:00 AM PDT), http://www.cnet.com/news/from-wargames-to-aaron-swartz-how-u-s-anti-hacking-law-went-astray/.

[30] Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (2013).

enforcement could cause more harm to these users than the botnet it has seeks to investigate. Specifically, the use of the word “seizure” in the proposal, an undefined term, could authorize any amount of invasive activity. For example, as in the Microsoft case described above, law enforcement could intercept and re-route legitimate internet traffic. Further, the ambiguity in the language could potentially be interpreted to encompass a level of government hacking into private networks. Even groups that are supportive of this type of government activity concede that it necessarily requires statutory authorization.[31]

The range of offensive cybersecurity measures available to law enforcement vary from passive measures like beaconing - causing files to broadcast back to a preordained location - to active and potentially harmful measures that interfere with the operation of the computer or its communications with other devices. The proper limits for use of offensive measures should be subject to public debate. While limits have been raised through various statutory vehicles in recent years, none have gained significant public support, and one has received not one, but two veto threats from the White House.[32] It is not the place to pre-empt these continued conversations through implementation of a procedural measure.

Conclusion

The proposed amendment before the Committee today is a substantive change to federal law masquerading as a procedural measure. Once again, I urge you to reject the

[31] The IP Commission Report, 82, (May 2013), *available at* http://ipcommission.org/report/IP_Commission_Report_052213.pdf “Statutes should be formulated that protect companies seeking to deter entry into their networks and prevent exploitation of their own network information while properly empowered law-enforcement authorities are mobilized in a timely way against attackers.”

[32] *See e.g.,* Hayley Tsukayama, *CISPA critics bolstered by veto threat*, Washington Post (April 17, 2013), *available at* http://www.washingtonpost.com/business/technology/cispa-critics-bolstered-by-veto-threat/2013/04/17/2c2f761e-a76b-11e2-8302-3c7e0ea97057_story.html. *See also*, Brandon Moss, *Access calls for President Obama to pledge to veto CISA*, Access (July 15, 2014 9:30 am), https://www.accessnow.org/blog/2014/07/15/access-calls-for-president-obama-to-pledge-to-veto-cisa; and Letter from Access and Civil Liberties Groups to President Obama (July 15, 2014), *available at* https://www.accessnow.org/page/-/Veto-CISA-Coalition-Ltr.pdf.

proposal and to, instead, support the exploration of appropriate statutory solutions for any legal gaps in the investigation, pursuit, and prosecution of those responsible for unlawful botnets. Thank you. I look forward to your questions.