Washington and Lee Journal of Civil Rights and Social Justice

Volume 27 | Issue 1 Article 10

Fall 2020

Keeping the Zombies at Bay: Fourth Amendment Problems in the Fight Against Botnets

Danielle Potter
Washington and Lee University School of Law, potter.d21@law.wlu.edu

Keeping the Zombies at Bay: Fourth Amendment Problems in the Fight Against Botnets

*Danielle Potter**

Abstract

You may not have heard of a botnet. If you have, you may have linked it to election shenanigans and nothing else. But if you are reading this on a computer or smartphone, there is a good chance you are in contact with a botnet right now.

Botnets, sometimes called "Zombie Armies," are networks of devices linked by a computer virus and controlled by cybercriminals. Botnets operate on everyday devices owned by millions of Americans, and thus pose a substantial threat to individual device owners as well as the nation's institutions and economy.

Accordingly, the United States government has been fighting back vigorously against botnets. As botnets advance in sophistication, the government's methods for taking them down have become more intrusive. In executing a botnet takedown, the government collects IP addresses of the computers interfacing with the botnet. Because botnets are camouflaged in personal computers and devices, the government is unable to know which devices are infected until the takedown is effectuated.

But what about the Fourth Amendment rights of innocent owners, whose devices are enabling the botnet without their consent or knowledge? Takedowns are beneficial to the owners because they

* Candidate for J.D., May 2021, Washington and Lee University School of Law. I would like to thank my father, Jonathan Potter, for inspiring me with his brilliance and humor, and my mother, Teresa Potter, for her never-ending kindness and love. I would also like to thank my sister and best friend, Kaitlyn Potter, for being a constant source of wisdom and laughter, and my dear friend, Charlie Hallinan, for encouraging me every step of the way. I also want to express my gratitude to Professor Timothy C. MacDonnell for his invaluable insight. Finally, I would like to thank my faculty advisor, Professor Andrew Christensen, for lending me his guidance, knowledge, and support. I was very lucky to have him in my corner.

liberate devices, but should we acquiesce to a government cyber-invasion simply because of this benefit? This Note argues no.

Although the Fourth Amendment is implicated in botnet takedowns, this should not mean the government cannot perform the search; it simply means that the government needs to get a warrant authorizing the search first. This Note argues that the 2016 amendment to Rule 41 of the Federal Rules of Criminal Procedure, which allows multi-district warrants to be issued by one judge, is a positive development for the Fourth Amendment and for the fight against cybercriminals. But Rule 41 must be implemented in a way that protects Fourth Amendment rights. To address this concern, this Note argues that judges should be trained regarding cybercrime, botnets, and the government's takedown efforts so that judges can do their jobs: Make sure the warrants are reasonable and protect the Fourth Amendment rights of innocent victims.

Table of Contents

I. Introduction

During the 2016 presidential campaign, Russian hackers commanded legions of social media bots that posed as individual American social media users.[1] These bots were used to spread fake news, promulgate conspiracy theories, post unflattering photographs of the opposing candidates, or "simply muddy discussions."[2] For example, one Russian bot, disguised as "Melvin Redick of Harrisburg, [Pennsylvania], a friendly-looking American with a backward baseball cap and a young daughter," encouraged Facebook users to visit a website in order to learn the "hidden truth about Hillary Clinton, George Soros, and other leaders of the US."[3] The website, DCLeaks.com, was in fact a Russian-created site peddling stolen emails and conspiracy theories.[4] Facebook reported that it closed hundreds of accounts believed to have been created by a Russian company.[5] According to Twitter officials, during the

---

1. *See* Gabe O'Connor, *How Russian Twitter Bots Pumped Out Fake News During the 2016 Election*, NAT'L PUB. RADIO (Apr. 3, 2017, 4:53 PM), https://www.npr.org/sections/alltechconsidered/2017/04/03/522503844/how-russian-twitter-bots-pumped-out-fake-news-during-the-2016-election (last visited Oct. 10, 2020) (explaining that Russian Twitter bots were disguised as "Midwestern swing-voter Republicans" in order to enhance the credibility of the information proffered by the bots) [perma.cc/JHB8-CXDC].

2. *See* John Markoff, *Automated Pro-Trump Bots Overwhelmed Pro-Clinton Messages, Researchers Say*, N.Y. TIMES (Nov. 17, 2016), https://www.nytimes.com/2016/11/18/technology/automated-pro-trump-bots-overwhelmed-pro-clinton-messages-researchers-say.html (last visited Sept. 27, 2020) (explaining the purposes of the "automated army of pro-Donald J. Trump chatbots") [perma.cc/7TPQ-55LV].

3. Scott Shane, *The Fake Americans Russia Created to Influence the Election*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html (last visited Oct. 10, 2020) [perma.cc/W577-LWWC].

4. *See* Hamza Shaban, *Twitter Suspends Guccifer and DCLeaks After Mueller Links them to Russian Hacking Operation*, WASH. POST (July 16, 2018, 3:35 PM), https://www.washingtonpost.com/technology/2018/07/16/twitter-suspends-guccifer-dcleaks-after-mueller-links-them-russian-hacking-operation/ (last visited Oct. 10, 2020) (noting that DCLeaks was a "digital front" created by Russian intelligence officers "to launder hacked information") [perma.cc/YH4R-PGAZ].

5. *See* Shane, *supra* note 3 ("Facebook officials disclosed that they . . . shut down several hundred accounts that they believe were created by a Russian company . . . .").

election, Russia created more than 50,000 fake Twitter accounts to push its political agenda.[6]

The 2016 election thrust botnets into the spotlight, causing newfound concern among politicians and private individuals.[7] But long before the 2016 election, botnets had been engaging in online mischief.[8]

A bot is an internet-connected device that has been compromised by a computer hacker's virus.[9] A botnet is an army of bots all infected with the same virus.[10] Botnets have been nicknamed "zombie armies" because, through the virus, the hacker can command the bots to act at her behest, without their owners' knowledge.[11] The term zombie army is also appropriate for another reason: These things are extremely hard to kill.[12]

The United States government had its first major victory in the fight against botnets in 2011.[13] Its target, Coreflood, was a

---

6. *See* Jon Swaine, *Twitter Admits Far More Russian Bots Posted on Election than It Had Disclosed*, GUARDIAN (Jan. 19, 2018, 7:46 PM), https://www.theguardian.com/technology/2018/jan/19/twitter-admits-far-more-russian-bots-posted-on-election-than-it-had-disclosed (last visited Oct. 10, 2020) ("Twitter has admitted that more than 50,000 Russia-linked accounts used its service to post automated material about the 2016 US election . . . .") [perma.cc/SQ2D-X897].

7. *See What Is a Botnet?*, PANDA SEC. (Dec. 5, 2017), https://www.pandasecurity.com/mediacenter/security/what-is-a-botnet/ (last visited Oct. 10, 2020) ("Facebook's fake ad controversy and the Twitter bot fiasco during the 2016 presidential election worry many politicians and citizens about the disruptive potential of botnets.") [perma.cc/M99A-2QYL].

8. *See 9 of History's Notable Botnets*, WHITE OPS (May 2018), https://www.whiteops.com/blog/9-of-the-most-notable-botnets (last visited Oct. 16, 2020) (describing several notable botnet attacks, and naming the first notable attack as EarthLink Spammer, a botnet that was created in 2000) [perma.cc/FJ5B-P83L].

9. *See What Are Bots, Botnets, and Zombies?*, WEBROOT, https://www.webroot.com/us/en/resources/tips-articles/what-are-bots-botnets-and-zombies (last visited Oct. 9, 2020) (defining the term "bot") [perma.cc/6RYL-7EST].

10. *See id.* (explaining what a botnet is).

11. *See id.* (explaining how botnets work).

12. *See* Lysa Myers, *Top 5 Scariest Zombie Botnets*, WELIVESECURITY (Oct. 23, 2014, 3:45 PM), https://www.welivesecurity.com/2014/10/23/top-5-scariest-zombie-botnets/ (last visited Oct. 10, 2020) ("A network of zombies is a bit like post-apocalyptic infection scenarios in the movies. Some of these things are virtually un-killable—there always seems to be that last undead creature lurking in the shadows, ready to start the next wave of trouble.") [perma.cc/H6NE-7CXE].

13. *See* David Sancho, *A Win for the Good Guys: The Coreflood Takedown*,

criminal botnet that had been lurking on the internet since the early aughts.[14] By 2011, it had infiltrated about 800,000 devices in the United States.[15] Globally, the number of infected machines was close to 2.3 million.[16] Coreflood operated by logging keystrokes in order to steal users' passwords and financial information.[17] The botnet was so successful in its criminal pursuits that Coreflood's operators had access to more accounts than they could possibly exploit, forcing them to comb through the collected data to find accounts worth stealing from.[18] In total, Coreflood caused at least twenty million dollars of damages.[19]

In April 2011, the U.S. District Court in Connecticut issued an order allowing the government to commandeer twenty-nine domain names that had been used to facilitate Coreflood's criminal

---

SEC. INTEL. BLOG (Apr. 14, 2011, 5:46 AM), https://blog.trendmicro.com/trendlabs-security-intelligence/a-win-for-the-good-guys-the-coreflood-takedown/ (last visited Oct. 10, 2020) (describing the Coreflood takedown as "a great victory for law enforcement and for all the good guys fighting against cybercrime") [perma.cc/ECS2-BTJ6].

14. *See* Matt Liebowitz, *Feds Shut Down Massive 'Coreflood' Botnet*, NBC NEWS, http://www.nbcnews.com/id/42596694/ns/technology_and_science-security/t/feds-shut-down-massive-coreflood-botnet/#.Xhd-X5NKjfY (last updated Apr. 14, 2011, 4:45 PM) (last visited Oct. 10, 2020) (stating that, in 2011, the Coreflood botnet was "believed to have been active for nearly a decade") [perma.cc/J79P-NHGW].

15. *See* Dan Goodin, *Feds Declare Victory over Notorious Coreflood Botnet*, REGISTER (June 23, 2011, 9:09 PM), https://www.theregister.co.uk/2011/06/23/coreflood_botnet_eradicated/ (last visited Oct. 10, 2020) (describing the 2011 Coreflood takedown and stating that Coreflood "enslaved almost 800,000 machines when the FBI commenced the operation in April") [perma.cc/KB69-TUYZ].

16. *See* Dan Kaplan, *Coreflood Takedown May Lead to Trouble*, ITNEWS (Apr. 18, 2011, 10:34 AM), https://www.itnews.com.au/news/coreflood-takedown-may-lead-to-trouble-254827 (last visited Oct. 10, 2020) (providing an estimate of the total size of the Coreflood botnet) [perma.cc/CD79-VK5U].

17. *See id.* (describing the Coreflood botnet); Janine S. Hiller, *Civil Cyberconflict: Microsoft, Cybercrime, and Botnets*, 31 SANTA CLARA HIGH TECH L.J. 163, 172–73 (2014) (describing the damage caused by the Coreflood botnet).

18. *See* Sam Zeitlin, Note, *Botnet Takedowns and the Fourth Amendment*, 90 N.Y.U. L. REV. 746, 747 (2015) ("The Russian cybercriminals who created Coreflood trawled through their ever-growing trove of financial data looking for bank balances big enough to be worth taking—they had access to far more accounts than they could ever exploit.").

19. *See* Hiller, *supra* note 17, at 173 ("Estimates of Coreflood damages exceeded $20 million.").

activity.[20] The order further allowed the government to substitute the seized servers with government-controlled servers.[21] When an infected computer contacted the substitute servers, the servers responded with commands instructing the infected computers to temporarily stop running Coreflood software.[22] The order also allowed the government to use a trap-and-trace device to learn the Internet Protocol (IP) addresses of infected machines.[23]

While Coreflood's malicious software was temporarily disabled, the government released the victims' IP addresses to their internet service providers (ISPs) so that the providers could alert the victims that their machines were infected and advise them how to remove the malware.[24] Within two months of the court order, "computers reporting to the botnet's command and control center fell by more than 95 percent."[25]

The takedown was a huge success for the government, but for private individuals it was a double-edged sword.[26] On one hand, the government had liberated thousands of victims' devices.[27] On

---

20. *See* United States v. John Doe 1, No. 3:11-CV-00561-VLB, at *5 (D. Conn. 2011) (granting a preliminary injunction).

21. *See id.* (granting a preliminary injunction).

22. *See id.* (granting a preliminary injunction).

23. *See* Kim Zetter, *With Court Order, FBI Hijacks "Coreflood" Botnet, Sends Kill Signal*, WIRED, https://www.wired.com/2011/04/coreflood/ (last updated Apr. 13, 2011, 7:30 PM) (last visited Oct. 10, 2020) (describing the Coreflood takedown) [perma.cc/YG3F-SLR8].

24. *See id.* (describing the Coreflood takedown).

25. Goodin, *supra* note 15.

26. *See* Jeff Mordock, *"Inherently Invasive": FBI Counter-Hacking Operations Raise Red Flags over Privacy*, WASH. TIMES (Jan. 31, 2019), https://www.washingtontimes.com/news/2019/jan/31/fbi-counter-hacking-operations-raise-privacy-red-f/ (last visited Oct. 10, 2020) (noting that law enforcement's success in defeating botnets by hacking back "is a double-edged sword, giving authorities a new tool to fight crime in an increasingly digital world, but also exposing sensitive and unrelated files to law enforcement") [perma.cc/65VP-3DW2].

27. *See* Goodin, *supra* note 15 (explaining that the government takedown rid thousands of machines of Coreflood malware).

the other hand, the government had invaded those very same victims' devices.[28] And it had done so without a warrant.[29]

According to the judge who issued the court order, no warrant was necessary.[30] That determination was crucial because, at the time of the Coreflood takedown, under the Federal Rules of Criminal Procedure, no magistrate would have had the authority to grant a warrant for extra-district botnet takedowns.[31]

Since the Coreflood takedown, cybercriminals have upped the ante, creating more resilient botnets.[32] In turn, the government has developed more aggressive—and inherently more intrusive—takedown methods.[33] As botnets continue to evolve, so must the government's efforts to combat them.[34] It is a high stakes games of cops and robbers with a twist—both the cops and the robbers are invisible.

Speaking of an "invisible policeman," when does the government cross the line and enter Fourth Amendment territory?[35] Between 2011 and 2016, the government performed

---

28. *See* Letter from Peter J. Kadzik, Ass't Att'y Gen., U.S. Dep't of Just., to Ron Wyden, Senator, U.S. Senate (Nov. 18, 2016), https://assets.documentcloud.org/documents/3225184/DOJ-Rule-41-Response.pdf (admitting that "some courts might hold" that the techniques used to collect victims' IP addresses and disrupt a botnet implicate the Fourth Amendment) [perma.cc/QDE6-NY9J].

29. *See* United States v. John Doe 1, No. 3:11-CV-00561-VLB, at *5 (D. Conn. 2011) (granting the government's request for civil relief).

30. *See id.* (granting the government's request for civil relief).

31. *See* Letter from Mythili Raman, Acting Ass't Att'y Gen., U.S. Dep't of Just., to the Hon. Reena Raggi, Chair, Advisory Comm. on the Crim. Rules (Sept. 18, 2013), https://www.justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf (explaining Rule 41 of the Federal Rules of Criminal Procedure needs to be amended to permit warrants for botnet takedowns) [perma.cc/C54B-6UCN].

32. *See* Julian B. Gizzard et al., *Peer-to-Peer Botnets: Overview and Case Study*, USENIX, Jan. 2007, at 1, https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/grizzard/grizzard.pdf (explaining that, in response to successful takedowns, attackers began creating sturdier botnet structures) [perma.cc/CHJ5-ER7P].

33. *See id.* (describing the additional steps necessary to take down a stronger botnet).

34. *See id.* (explaining that, as botnets grow stronger, takedown methods will need to improve).

35. *See* Berger v. New York, 388 U.S. 41, 65 (1967) (Douglas, J., concurring) (noting that a statute authorizing electronic surveillance "in effect, places an invisible policeman in the home").

several major botnet takedowns.[36] Some of these operations were even more invasive than the Coreflood takedown, actually manipulating data on victims' devices.[37] Still, in each case, the government was able to convince a judge that there were no Fourth Amendment issues.[38]

In 2016, Rule 41 of the Federal Rules of Criminal Procedure was amended to allow magistrate judges to grant extra-district warrants in cases involving botnets.[39] Privacy enthusiasts lampooned the change,[40] but this Note argues that the amendment is a step in the right direction.

Before Rule 41 was passed, the government conducted botnet takedowns under civil rather than criminal law—obtaining court orders instead of warrants.[41] This Note argues that even those early takedowns indeed implicated the Fourth Amendment. But the author is sympathetic to the government's dilemma—it had to operate outside of the Fourth Amendment because the Federal Rules had not caught up with the times.

This Note argues that, without the amendment to Rule 41, the government would be forced to continue to convince courts that

---

36. *See* Memorandum of Law in Support of Motion for Temp. Restraining Ord. and Ord. to Show Cause, at 3 (W.D. Pa. Nov. 28, 2016) (listing several successful botnet takedowns since Coreflood).

37. *See* Lorenzo Franceschi-Bicchieri, *How the FBI Took Down the Botnet Designed to Be "Impossible" to Takedown*, VICE (Aug. 12, 2015, 7:00 AM), https://www.vice.com/en_us/article/539xy5/how-the-fbi-took-down-the-botnet-designed-to-be-impossible-to-take-down (last visited Oct. 10, 2020) (explaining that, to take down the GameOver Zeus botnet, the government needed to persuade bots to talk only to government servers and refrain from talking to servers run by the cybercriminals) [perma.cc/Y646-9JTU]; *see also* Julian B. Gizzard, et al., *supra* note 32 (describing methods used to take down peer-to-peer botnets).

38. *See* United States v. Ghinkul, No. 2:2015-CV-1315, 2020 WL 85256, at *1, *2 (W.D. Pa. Jan. 7, 2020) (granting civil relief); United States v. Bogachev, No. 2:14-CV-00685, at *4–8 (W.D. Pa. 2014) (same).

39. *See* Leslie R. Caldwell, *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches*, U.S. DEP'T OF JUST. ARCHIVES (June 20, 2016), https://www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches (last visited Oct. 10, 2020) (explaining the purpose of the 2016 amendment to Rule 41) [perma.cc/986V-4YR2].

40. *See, e.g.*, Mordock, *supra* note 26 (discussing criticism of the Rule 41 amendments).

41. *See Ghinkul*, 2020 WL 85256, at *2 (granting civil relief); *Bogachev*, No. 2:14-CV-00685, at *4–8 (same).

takedown methods do not implicate the Fourth Amendment. These decisions could lead to dangerous precedents. One possibility is that botnet takedowns will become an established form of exigent circumstances.[42] An exception to the warrant requirement, exigent circumstances have historically been applied to situations so urgent that there is no time to get a warrant.[43] Although this Note does not explore the application of exigent circumstances to botnet takedowns, the author suggests that such an expansion of the doctrine is untenable.[44]

Instead, this Note will focus on dangerous precedents within the confines of the warrant requirement. To demonstrate the possibility for the perversion of search law as it relates to technology, this Note will focus on the government's retrieval of IP addresses. This Note will argue that such retrieval is a search, despite some court decisions that hold otherwise.[45]

The purpose of this Note is not to campaign against the collection of IP addresses. In fact, in the author's view, this collection is one of the least intrusive steps that the government takes when fighting botnets. Instead, the purpose is to show that, because even the most innocuous step of a botnet takedown is a search, botnet takedowns inherently implicate the Fourth Amendment.

One day, the government will have to develop means to overcome even more fanciful botnet disguises: Malware that can embed in the smoke detector, the garage door opener, or the dog's implanted identity chip.[46] Of course, these attacks require a response. But that response must comply with civil liberties, including the Fourth Amendment. Rule 41 allows courts to apply the Fourth Amendment in the battle against botnets. When the

---

42. *See* Zeitlin, *supra* note 18, at 758–59 n.72 (noting the possibility that exigent circumstances could cover botnet takedowns).

43. *See* Kentucky v. King, 563 U.S. 452, 473–77 (2011) (Ginsberg, J., dissenting) (discussing the notion that exigent circumstances require urgency).

44. *See* Zeitlin, *supra* note 18, at 758–59 n.72 (outlining the dangers of applying the exigent circumstances exception to the warrant requirement in the context of botnet takedowns).

45. *See, e.g.*, United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010) (holding that the government's retrieval of an IP address is not a search).

46. *See* MARC GOODMAN, FUTURE CRIMES 287 (Anchor Books 2015) (explaining that, in the future, virtually everything will be connected to the internet and capable of sharing data).

government mass hacks—even for a good cause—it should be regulated by the Fourth Amendment.[47]

II. A Brief Explanation of Botnets

A botnet is a network of devices linked by a virus and controlled remotely by a computer hacker, known as a botmaster.[48] To create a botnet, a botmaster "writes a computer program that searches the internet for connected devices."[49] The program attempts to infiltrate the devices that it finds, and, if it is successful, it will install the botnet virus onto the devices.[50]

Botnets can attack any device connected to the internet.[51] Many commonly used smart devices are vulnerable because they

---

47. *See* Jonathan Meyer, *Government Hacking*, 127 YALE L.J. 570, 614 (2018) ("Courts should end their myopic focus on which data government malware retrieves and acknowledge that government hacking necessarily constitutes a Fourth Amendment search.").

48. *See* Nicole Hong, *Brooklyn Trial to Reveal the Inner Workings of 'Botnet' Hackers*, WALL ST. J. (July 22, 2017, 7:00 AM), https://www.wsj.com/articles/brooklyn-trial-to-reveal-inner-workings-of-botnet-hackers-1500721201 (last visited Oct. 10, 2020) (describing botnets as "a network of computers with malicious software") [perma.cc/H2ES-VZ5F]; *see also* Hiller, *supra* note 17, at 167 ("An essential aspect of a botnet is that another party, at a distance, controls the network of infected computers.").

49. Stephen Ornes, *Rise of the Botnets*, SCI. NEWS FOR STUDENTS (Feb. 21, 2019, 6:45 AM), https://www.sciencenewsforstudents.org/article/botnets-malware-cyberattack-increase (last visited Oct. 10, 2020) [perma.cc/886U-6Y6C].

50. *See id.* (explaining that, once the computer program has broken into a device, "the program can install malware").

51. *See Botnet Facts*, WASH. STATE OFF. OF THE ATT'Y GEN., https://www.atg.wa.gov/botnet-facts (last visited Oct. 10, 2020) ("All computers connected to the Internet are susceptible to malware infections.") [perma.cc/K5HD-982S]; *see also How the FBI Investigated and Dismantled the Mirai Botnet*, BIZTECH (June 19, 2019), https://biztechmagazine.com/media/video/how-fbi-investigated-and-dismantled-mirai-botnet (explaining that "the Marai botnet attack turned Internet of Things devices . . . into [a] bot[] that could be used as part of a botnet in large-scale network attacks") [perma.cc/RXJ9-3PL9]; *see, e.g.*, Shaquille De Bique, The Botnet Threat Against Smart Refrigerator Security, 1, 3 (May, 2019) (Ph.D. dissertation, Utica College) (ProQuest) (explaining that smart refrigerators "are very susceptible to botnet attacks"); *The Odd, 8-Year Legacy of the Conficker Worm*, WELIVESECURITY (Nov. 21, 2016, 1:30 PM), https://www.welivesecurity.com/2016/11/21/odd-8-year-legacy-conficker-worm/ (last visited Oct. 10, 2020) (describing the Conficker botnet which infiltrated "MRI machines, CT scanners and dialysis pumps" and police body cameras)

come with a default password that the user never bothers to change.[52] Cybercriminals can easily guess these passwords in order to hack into the device.[53] For example, in 2016, "a massive botnet composed of baby monitors, webcams, and other common devices" wreaked havoc on the internet.[54]

Computers with secure systems can also fall victim to a botnet.[55] Using email attachments and pop up ads containing malicious website links,[56] botnets "trick . . . users into compromising their own security."[57] Even when a device owner takes all of the possible precautions, botmasters can still find a way in.[58] Botnets often infiltrate devices through known security vulnerabilities in commercially available security systems.[59] For

---

[perma.cc/87Z6-ZHGX].

52. *See* Ornes, *supra* note 49 ("New devices like smart TVs, wi-fi routers and security cameras are sold with a default password in place. (It's often something easy, like 'password.') According to a survey conducted by a computer magazine in June and July 2018, more than one-third of people never change their passwords.").

53. *See id.* (explaining that, because of default passwords, it is "easier than you might think" for a cybercriminal to guess a device's password); *see also* Shane Harris, *Presidential Commission Sounds Warning over Botnet Threat*, WALL ST. J. (Dec. 3, 2016, 6:30 AM), https://www.wsj.com/articles/presidential-commission-sounds-warning-over-botnet-threat-1480764656 (last visited Oct. 10, 2020) (noting that the Commission on Enhancing National Cybersecurity recommended that a device should not be able to connect to the internet until its default password had been reset because default passwords "are often easy for hackers to guess") [perma.cc/TD8L-38L6].

54. *See* Harris, *supra* note 53 (describing an attack that resulted in "widespread outages and congestion").

55. *See* Zeitlin, *supra* note 18, at 749 (explaining that botnets "grow by finding vulnerable computers and infecting them with malware," but even "computers protected by firewalls and more up-to-date software" are susceptible to infection through "social engineering") (citations omitted).

56. *See Botnet Facts*, *supra* note 51 ("If you open an email attachment or visit a website that is distributing malware, your computer may become infected . . . ."); *see also What is a Botnet, supra* note 7 ("The strategy typically requires users to infect their own systems by opening email attachments, clicking on malicious pop up ads, or downloading dangerous software from a website.").

57. Zeitlin, *supra* note 18, at 749.

58. *See* Press Release, U.S. Dep't of Just., *Department of Justice Takes Action to Disable International Botnet* (Apr. 13, 2011), https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet (last visited Oct. 16, 2020) (explaining how Coreflood thrived) [perma.cc/7CW5-MJ9A].

59. *See* Hiller, *supra* note 17, at 170 ("Ironically, releases of vulnerability

example, Coreflood targeted Microsoft computers in order to take advantage of a flaw in the Windows operating systems.[60]

Botnets are particularly nefarious criminal devices because they are difficult to eradicate.[61] The infection is discrete, so owners of the infected computers are generally not even aware of the virus's presence.[62] Even if a user is aware of the botnet's presence, only a highly skilled computer user would be to able remove the botnet without technical assistance.[63] Finally, it is difficult for law enforcement to identify the botnet operator.[64] And, even when the operator is identified, she may be from another country and out of law enforcement's reach.[65]

---

information and patches are known to sometimes create the opposite result; malware can be propagated seeking to exploit the weakness before computers are updated.").

60. *See* Press Release, U.S. Dep't of Just., *supra* note 58 (explaining that Coreflood "install[ed] itself by exploiting a vulnerability in computers running Windows operating systems").

61. *See* Bill Brenner, *Botnets: 4 Reasons It's Getting Harder to Find and Fight Them*, CSO (Apr. 15, 2009, 7:00 AM), https://www.csoonline.com/article/2123967/botnets--4-reasons-it-s-getting-harder-to-find-and-fight-them.html (last visited Oct. 25, 2020) (explaining why it is very difficult to defeat botnets) [perma.cc/95ZV-2K3P].

62. *See Botnet Facts*, *supra* note 51 (explaining that "[i]n the past, sluggish performance and annoying advertisements" alerted users that their computers were compromised, but "[t]hese days, there may be no outward signs you have malware"); *see also* Nicole Perlroth, *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*, N.Y. TIMES, (Oct. 21, 2016), https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html (last visited Oct. 10, 2020) (describing a botnet that infected "internet-connected devices . . . without their owners' knowledge") [perma.cc/P2LT-QZUY]; *see also* Mark Bowden, *The Worm that Nearly Ate the Internet*, N.Y. TIMES (June 29, 2019), https://www.nytimes.com/2019/06/29/opinion/sunday/conficker-worm-ukraine.html (last visited Oct. 10, 2020) (defining botnets as "networks of secretly linked personal computers controlled by an unseen hand") [perma.cc/T3E9-LATF].

63. *See* Zeitlin, *supra* note 18, at 750 ("Most botnets are difficult for all but the most sophisticated users to remove from their computers.") (citations omitted).

64. *See* Daniel Ramsbrock et al., A First Step Toward Live Botmaster Traceback, Presentation at International Symposium on Research in Attacks, Intrusions, and Defenses (Sept. 16, 2008), at 2 (explaining the various reasons why "[t]racking and locating the botmaster of a discovered botnet is very challenging").

65. *See What Is a DDOS Botnet?,* CLOUDFLARE, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/ (last visited Oct. 24, 2019) (explaining that botnet operation is a particularly successful

Botnet operators use botnets for a variety of cybercrimes, both against the infected devices' users and third parties.[66] Botnets are not always committed to just one criminal objective, and sometimes a botnet's primary goal will evolve over time.[67] Often, botnets are used for financial gain.[68] Cybercriminals can use botnets to steal data, which they can then use to steal the computer user's identity or financial information.[69] Alternatively, cybercriminals can install devices with ransomware, "which encrypts and hijacks files on a computer system and later demands money for decrypting them."[70]

Botnets have also frequently been used to launch denial of service attacks.[71] These attacks temporarily disable websites by flooding them with more traffic than they can handle.[72] Sometimes, the botnet controller will demand money from the

---

endeavor in "geographic locations where regulation and law enforcement are limited") [perma.cc/ZS2K-NTTF].

66. *See* Hong, *supra* note 48 ("[B]otnets . . . allow hackers to remotely control the computers and command them for criminal purposes, including to steal banking credentials, launch denial-of-service attacks and transmit viruses."); *see also* Zeitlin, *supra* note 18, at 750 ("Botnets are the Swiss army knife of cybercrime, a ubiquitous tool used for many different purposes against both the users of infected computers and third parties.").

67. *See* Zeitlin, *supra* note 18, at 750–51 (discussing the Coreflood botnet and explaining that when it "was first created sometime around 2002, its primary purpose was to be a tool for distributed denial of service . . . attacks," but "[b]y 2008, Coreflood's focus had moved to bank fraud, using credentials stolen from infected computers to empty their owners' bank accounts") (citations omitted).

68. *See What is a Botnet?*, *supra* note 7 (outlining the different goals of the cybercriminals who command botnets and providing that one of those goals is financial gain).

69. *See Botnet Facts*, *supra* note 51 (explaining that botnets can be used to steal personal information for identify theft and credit card fraud).

70. Hong, *supra* note 48; *see, e.g.*, Patricia Mazzei, *Another Hacked Florida City Pays a Ransom, This Time for $460,000*, N.Y. TIMES (June 27, 2019), https://www.nytimes.com/2019/06/27/us/lake-city-florida-ransom-cyberattack.html (last visited Oct. 16, 2020) (reporting on a city government's payout to cybercriminals who "launched a cyberattack that disabled the city's computer systems") [perma.cc/U6PW-X2B6].

71. *See What is A Botnet?*, *supra* note 7 (providing that botnet operators use botnets in denial of service attacks and explaining how these attacks are carried out).

72. *See* Perlroth, *supra* note 62 (describing a botnet attack that disabled "several websites, including Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud and The New York Times" by "command[ing] [infected computers] to flood a target with overwhelming traffic").

targeted organization in exchange for ceasing the attack.[73] Even if no ransom is demanded, a denial of service attack can take a financial toll on a company whose website is attacked because, while the website is under attack, customers cannot use the company's services.[74] Denial of service attacks often target companies,[75] but they can also target national infrastructures.[76] A denial of service attack "on critical national infrastructure could cause widespread disruption including large populations suffering major power outages, significant business or market disturbance, life threatening emergency service outages and long term economic damage."[77]

Furthermore, botnets can "be used by governments for espionage, infecting and controlling sensitive systems, and extracting confidential data."[78] For example, in 2019, a botnet

---

73. *See* Mathew J. Schwartz, *Cyber Extortion: Fighting DDoS Attacks*, BANK INFO SEC. (Jan. 26, 2016), https://www.bankinfosecurity.com/cyber-extortion-fighting-ddos-attacks-a-8828 (last visited Oct. 10, 2020) ("Attackers disrupt a site for a short period with a distributed denial-of-service attack, send a ransom note threatening further disruption, and if the ransom doesn't get paid, sometimes make good on that threat.") [perma.cc/C78L-VTMC].

74. *See* Ornes, *supra* note 49 (discussing an October 2016 botnet attack that "crippled dozens of websites . . . includ[ing] Amazon, PayPal, Spotify and Twitter" and explaining that "[a]ttacked businesses lost money when customers couldn't buy things").

75. *See* Blair Felter, *5 of the Most Famous Recent DDoS Attacks*, VXCHNGE (May 31, 2019), https://www.vxchnge.com/blog/recent-ddos-attacks-on-companies (last visited Oct. 10, 2020) (naming five famous denial of service attacks which targeted companies such as GitHub, Netflix, PayPal, Visa, Amazon, The New York Times, Bank of America, JP Morgan Chase, Citigroup, and PNC) [perma.cc/2ZBL-D43Y].

76. *See, e.g.*, Bradley Barth, *DDoS Attacks Delay Trains, Halt Transportation Services in Sweden*, SC MEDIA (Oct. 16, 2017), https://www.scmagazineuk.com/ddos-attacks-delay-trains-halt-transportation-services-sweden/article/1473963 (last visited Oct. 10, 2020) (describing a denial of service attack aimed at the Swedish Transport Administration that "crashed the IT system that monitors trains' locations and tells operators when to go or stop") [perma.cc/BJ93-STLL].

77. Ashley Stephenson, *Why Critical National Infrastructure Organizations Shouldn't Overlook DDoS Attacks*, CORERO NETWORK SEC. (Nov. 5, 2018), https://www.corero.com/blog/901-why-critical-national-infrastructure-organizations-shouldnt-overlook-ddos-attacks.html (last visited Oct. 10, 2020) [perma.cc/9DUZ-P6ZN].

78. Zeitlin, *supra* note 18, at 751 (citing HELI TIIRMAA-KLAAR, ET. AL., BOTNETS, at 12–15 (Sandro Gaycken et al. eds., 2013)); *see Tagging and Tracking Espionage Botnets*, KREBS ON SEC. (July 30, 2012),

unleashed malware that targeted United States utility companies.[79] The malware, nicknamed "LookBack," infiltrated the computers of employees working within the utilities industry sector in order "to steal data files and take operational screenshots."[80] Though the botnet's origins were never confirmed, APT10, a hacking group backed by China, "is the most likely culprit."[81]

Botnets can also be used to influence public opinion in favor of the botnet operator's agenda.[82] Russia's use of botnets to interfere with the 2016 presidential election is one prominent example of this use,[83] but that was not the first time that botnets have been used for propaganda.[84] The Islamic State in Iraq and Syria (ISIS) used botnets to "achieve[] name recognition."[85] After carrying out a terrorist attack, ISIS members used Twitter to claim responsibility for the attack.[86] Then, legions of ISIS-controlled fake

---

https://krebsonsecurity.com/tag/espionage-botnet/ (discussing "malicious software that was developed and deployed specifically for spying on governments, activists and industry executives") [perma.cc/5VK2-HKUE].

79. *See* Zak Doffman, *Chinese State Hackers Suspected of Malicious Cyber Attack on U.S. Utilities*, FORBES (Aug. 3, 2019, 2:31 AM), https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/#43aec8146758 (last visited Oct. 10, 2020) (describing the "cyber campaign [that] target[ed] U.S. utility companies") [perma.cc/VH3U-WTB7].

80. *Id.*

81. *Id.*

82. *See What Is a Botnet, supra* note 7 (referencing the use of botnets as "tools for influencing elections").

83. *See supra* notes 1–6 and accompanying text (discussing the influence of Russian botnets in the 2016 presidential election).

84. *See* Moustafa Ayad, *Twitter Has Been Flooded with ISIS Propaganda Since al Baghdadi's Death*, VICE (Nov. 1, 2019, 1:09 PM), https://www.vice.com/en_us/article/9kevpp/twitter-has-been-flooded-with-isis-propaganda-since-al-baghdadis-death (last visited Oct. 10, 2020) ("While most of the attention has been focused on Russian-backed botnet interference in the 2016 US elections and the 2016 Brexit vote, ISIS was one of the first terrorist groups to pioneer swarming social media with posts from automated and semi-automated accounts.") [perma.cc/8Q3E-GMVZ].

85. Aaron Delwiche & Mary Margaret Herring, *ISIS Botnet*, PROPAGANDA CRITIC (Aug. 8, 2018), https://propagandacritic.com/index.php/case-studies/isis-botnet/ (last visited Oct. 10, 2020) [perma.cc/KW7X-AXE4].

86. *See id.* (discussing how ISIS "leveraged Twitter as a way of taking responsibility for successful terrorist attacks").

Twitter accounts retweeted and favorited the messages.[87] In this way, ISIS "made it highly likely that mainstream media would see their content and amplify it even as they condemned it."[88]

III. Hacking Back

Because of the dangers posed by botnets, the government has a significant interest in fighting back against them.[89] Since the Coreflood takedown, the government has consistently gathered victims' IP addresses in order to enlist the victims' assistance in taking down the botnet by liberating their own machines.[90]

This section will describe two takedowns that typify the government's approach, but there are other takedown methods that would not require the government to gather IP addresses.[91] These methods, however, require more egregious invasions of the victims' devices.[92] For example, instead of contacting the victim in order to get her to remove the malware, the government could remotely instruct the malware to remove itself.[93]

---

87. *See id.* (citing Twitter Inc., *Combatting Violent Extremism*, TWITTER BLOG (Feb. 5, 2016), https://blog.twitter.com/official/en_us/a/2016/combating-violent-extremism.html (last visited Oct. 16, 2020) (explaining how ISIS used "an army of bots to create false consensus online")) [perma.cc/XT6W-RB22].

88. *Id.* (quoting Renee Diresta, *How ISIS and Russia Won Friends and Manufactured Crowds*, WIRED (Mar. 8, 2018, 7:00 AM), https://www.wired.com/story/isis-russia-manufacture-crowds/ (last visited Oct. 16, 2020) [perma.cc/82VS-7R2V].

89. *See* Hong, *supra* note 48 ("Justice Department officials have urged Congress in recent years to modernize the laws that fight cybercrime . . . ."); *see also Worldwide Threats: Hearing Before the Senate Homeland Security and Governmental Affairs Committee*, 116th Cong. 5–6 (2019) (statement of Christopher Wray, Director, Federal Bureau of Investigation) (discussing the FBI's efforts to combat security risks posed by botnets).

90. *See, e.g.*, Zetter, *supra* note 23 (noting that the government collected IP addresses in the Coreflood takedown).

91. *See* Zeitlin, *supra* note 18, at 752–54 (discussing methods for dismantling botnets).

92. *See id.* at 754 (explaining that the most intrusive method for fighting botnets "involves modifying not just the malware, but the user's personal software as well").

93. *See id.* at 753 (noting that law enforcement could hack back in order "to modify or delete the malware running on infected computers").

A. Centralized Botnets: Coreflood

Traditional botnets are centered around one or a few central servers, which are identified in the virus's code.[94] In its early efforts to fight against botnets, the government generally partnered with ISPs in order to remove these servers.[95] By shutting down a botnet's domains, the government was able to freeze out the operator for a while.[96] But the devices comprising the botnet remained infected,[97] and to regain control, the botnet's operators need only rewrite the botnet's virus to answer to a new set of domain names.[98]

In 2011, instead of just shutting down Coreflood's central servers, the government created a "sinkhole."[99] Sinkholing reroutes bot "traffic from its original destination to one specified by the sinkhole [operator]."[100] The revised destination is called a

---

94. *See* Gizzard, et al., *supra* note 32 (explaining the centralized structure of traditional botnets); *see also* Zack Whittaker, *The Sinkhole that Saved the Internet*, TECHCRUNCH (July 8, 2019, 3:47 PM), https://techcrunch.com/2019/07/08/the-wannacry-sinkhole/ (last visited Oct. 16, 2020) (noting that a botnet was stopped by registering a "web domain found in the malware's code") [perma.cc/B72Q-MPD9].

95. *See* Kaplan, *supra* note 16 (describing the difference between the Coreflood takedown and prior botnet takedowns).

96. *See id.* (describing the difference between the Coreflood takedown and prior botnet takedowns).

97. *See* United States v. John Doe, No. 3:11-CV-00561, at *3 (D. Conn. 2011) (acknowledging that the seizure of Coreflood's servers would "leave the infected computers still running Coreflood").

98. *See* Kaplan, *supra* note 16 (explaining that, using the pre-Coreflood takedown method, botnets became temporarily defunct, but operators could resurrect the botnet by creating "a new hub"); *see also* Lily Hay Newman, *Hacker Lexicon: What Is Sinkholing?*, WIRED (Jan. 2, 2018, 7:00 AM), https://www.wired.com/story/what-is-sinkholing/ (last visited Oct. 16, 2020) (describing a sinkhole that "couldn't block the malware from being rewritten" in a way that would allow the malware to evade the sinkhole) [perma.cc/ZY89-2QDS].

99. *See* Lucian Constantin, *FBI Remotely Uninstalled Coreflood Malware from 19,000 Computers*, SOFTPEDIA NEWS (June 22, 2011, 4:29 PM), https://news.softpedia.com/news/FBI-Remotely-Uninstalled-Coreflood-Malware-from-19-000-Computers-207635.shtml (last visited Oct. 10, 2020) (noting that, in the Coreflood case, the judge "authorized the bureau to set up a sinkhole server") [perma.cc/J94W-YBXK].

100. Margaret Rouse & Matthew Haughn, *Definition: Botnet Sinkhole*, TECHTARGET, https://whatis.techtarget.com/definition/botnet-sinkhole (last updated June 2014) (last visited Oct. 10, 2020) [perma.cc/D3K7-V2MS].

sinkhole.[101] To prevent the infected machines from continuing to run Coreflood's malware, the government used the sinkhole to respond to bots with commands to stop running the malware.[102] Additionally, in order to facilitate the permanent liberation of the infected computers, the government used the information gathered from the sinkhole to collect the IP addresses of infected computers in order to independently locate and notify victims.[103]

B. Peer-to-Peer Botnets: Kelihos

A traditional botnet's centralized infrastructure makes it easy and efficient for botnet operators to "push commands to, and receive information from, infected bots."[104] But, as demonstrated by the Coreflood takedown, the centrality of a traditional botnet is also its Achilles heel.[105]

Cybercriminals have responded to this vulnerability by creating peer-to-peer botnets.[106] In a peer-to-peer botnet, infected computers communicate with each other rather than checking in with central servers.[107] To facilitate this communication, bots regularly exchange "peer lists," updating each other when new bots are added, and warning each other about suspicious bots.[108] If a

---

101. *See id.* ("The altered destination is known as the sinkhole.").

102. *See Doe*, No. 3:11-CV-00561 at *3 (allowing the government to use its substitute servers to send stop commands to infected computers).

103. *See* Zetter, *supra* note 23 (describing the Coreflood takedown).

104. Declaration of Special Agent Elliot Peterson in Support of Application for an Emergency Restraining Ord. and Ord. to Show Cause Re Preliminary Injunction, United States v. Bogachev, No. 2:14-CV-00685 (W.D. Pa. 2014); *see* Gizzard, et. al, *supra* note 32 (explaining that centralized structures "provide[] the attackers with very efficient communication").

105. *See* Gizzard, *supra* note 32, at 1 ("The threat of [a centralized] botnet can be mitigated and possibly eliminated if the central [server] is incapacitated.").

106. *See id*. at 1–3 (explaining that peer-to-peer architecture was developed in response to centralized botnet takedowns).

107. *See* Michael Mimoso, *Peer-to-Peer Botnets Resilient to Takedown Attempts*, THREAT POST (May 31, 2013, 2:15 PM), https://threatpost.com/peer-to-peer-botnets-resilient-to-takedown-attempts/100851/ (last visited Oct. 16, 2020) ("In Peer-to-Peer botnets, compromised bots talk to each other rather than to a central server.") [perma.cc/5EYP-LSY3].

108. Christian Rossow et al., *Modeling and Evaluating the Resilience of Peer-to-Peer Botnets*, 2013 IEEE SYMPOSIUM ON SECURITY AND PRIVACY, https://christian-rossow.de/publications/p2pwned-ieee2013.pdf (last visited Feb.

particular bot is compromised, "the gaps in the network are closed and the network continues to operate under the control of the attacker."[109]

To take down Kelihos, a peer-to-peer botnet, the FBI infected its own machines with Kelihos malware and then manipulated those newly infected machines into "supernodes."[110] The supernodes acted as mini-sinkholes.[111] When an infected machine contacted a super node, the super node responded with the IP address and routing information of an FBI controlled server.[112] Again, the FBI server then recorded the IP addresses of infected computers so that the FBI could release that information to the victims' ISPs.[113] The ISPs then told victims about the infection and helped them remove the malware.[114]

IV. The Privacy Implications of Hacking Back

Despite the dangers posed by botnets, the invasiveness of takedown efforts raises privacy concerns.[115] When private parties use sinkholes, many of these concerns are addressed by the Computer Fraud and Abuse Act (CFAA).[116] The CFAA is a federal

---

20, 2020) ("All [peer-to-peer] botnets implement the concept of *peer lists* to keep track of neighboring peers.") [perma.cc/7CJU-BRST].

109. Gizzard, *supra* note 32.

110. *See* Aliya Sternstein, *FBI Allays Some Critics with First Use of New Mass-Hacking Warrant*, ARS TECHNICA (Apr. 24, 2017, 2:44 PM), https://arstechnica.com/tech-policy/2017/04/fbi-allays-some-critics-with-first-use-of-new-mass-hacking-warrant/ (last visited Oct. 11, 2020) (describing the Kelihos takedown) [perma.cc/N6GW-3CN6].

111. *See id.* (describing the Kelihos takedown).

112. *See id.* (describing the Kelihos takedown).

113. *See* Affidavit in Support of an Application Under Rule 41 for a Search Warrant at 2, No. 3:18-MJ-0024-DMS (D. Alaska Apr. 5, 2017) (explaining the government's method to take down Kelihos).

114. *See id.* (explaining the government's method to take down Kelihos); *see also* Sternstein, *supra* note 110 (same).

115. *See* Zeitlin, *supra* note 18, at 756 (noting that government takedown efforts "intrude on private computers," and thus "raise[] legal and ethical concerns").

116. *See* 18 U.S.C. § 1030(a)(2)(C) (2018) (prohibiting individuals from "accessing a computer without authorization" in order to gain information from the computer's user); 18 U.S.C. § 1030(a)(5)(B)–(C) (2018) (establishing criminal liability for individuals who "intentionally access a protected computer without

statute that criminalizes intentional, unauthorized access to computers and networks.[117]

However, the CFAA does not apply to law enforcement agencies.[118] Instead, the privacy concerns implicated by government takedown efforts should be analyzed under the Fourth Amendment.[119] The Fourth Amendment provides that

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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.[120]

Often, the Fourth Amendment is contemplated through the prism of the suppression of evidence in criminal cases.[121] But the protections of the Fourth Amendment are not cabined to protecting individuals from having evidence used against them in courts.[122] Indeed, the "wrong condemned by the Amendment is 'fully

---

authorization" when that access causes damage or loss); *see also* Zeitlin, *supra* note 18, at 756–57 (explaining the CFAA's protections, which limit private uses of sinkholing).

117. *See* Kim Zetter, *Hacker Lexicon: What Is the Computer Fraud and Abuse Act?*, WIRED (Nov. 28, 2014, 6:30 AM), https://www.wired.com/2014/11/hacker-lexicon-computer-fraud-abuse-act/ (last visited Oct. 16, 2020) (describing the CFAA as "a federal anti-hacking statute that prohibits unauthorized access to computers and networks") [perma.cc/HY2E-7GFD].

118. *See* 18 U.S.C. § 1030(f) (2018) ("This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.").

119. *See* U.S. CONST. amend. IV. ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."); Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (specifying that the Fourth Amendment's "protection applies to governmental action").

120. U.S. CONST. amend. IV.

121. *See* Adam M. Gershowitz, *The Post-Riley Search Warrant*, 69 VAND. L. REV. 585, 590 (2016) ("In standard Fourth Amendment caselaw, the question of whether a search warrant is properly executed is litigated after the search is conducted.").

122. *See* U.S. CONST. amend. IV. (protecting "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"); United States v. Leon, 468 U.S. 897, 906 (1984) (explaining that the Fourth Amendment is not merely a tool for suppressing evidence).

accomplished' by the unlawful [invasion] itself."[123] By suppressing the ill-begotten evidence, a court cannot "cure the invasion of the defendant's rights which he has already suffered."[124] Instead, suppression merely serves to deter law enforcement from future Fourth Amendment violations.[125]

Botnet takedowns offend the Fourth Amendment rights of the owners of infected devices. These owners are not suspects in the botnet investigation and will not face prosecution. Thus, any evidence procured from the Fourth Amendment violations would not be used against them in court.

At first glance, it may seem that an analysis of the Fourth Amendment implications of botnet takedowns is only an academic exercise. If the invasion does not result in evidence that could be used against the owner, maybe the invasion does not matter. Furthermore, owners generally have an interest in eradicating the infection because it may slow down their device or compromise their data.[126] Perhaps it seems harsh to limit law enforcement's ability to help owners by asserting the owners' Fourth Amendment rights.

But to turn a blind eye to such intrusions would sanction government overreach.

> Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.[127]

---

123. United States v. Leon, 468 U.S. 897, 906 (1984) (quoting United States v. Calandra, 414 U.S. 338, 354 (1974)).

124. *Id.* (citations omitted).

125. *See id.* (quoting *Calandra*, 414 U.S. at 348) (noting that the exclusionary rule "operates as a 'judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved'").

126. *See* Jonathan Strickland, *How to Fix Your Zombie Computer,* HOW STUFF WORKS, https://electronics.howstuffworks.com/how-to-tech/how-to-fix-zombie-computer1.htm (last visited Oct. 16, 2020) (explaining that botnets can slow down an infected computer) [perma.cc/W2XD-CYU2].

127. Olmstead v. United States, 277 U.S. 438, 477 (1928) (Brandeis, J., dissenting).

V. Search: The Collection of IP Addresses

A. "The Technology We Exalt Today Is Everyman's Master"

For purposes of the Fourth Amendment, government conduct is a search if it meets the criteria of either the *Katz*[128] "reasonable expectation of privacy" analysis or the trespass test.[129] Courts have not had occasion to consider the government's collection of IP addresses in the context of botnet takedowns. But courts have considered this question in another context: The government's use of Network Investigative Techniques (NIT).[130]

In the most prominent examples of these cases, the Playpen cases, the government embedded malware into a child porn site.[131] When a user visited the site, the malware would infect her computer and report her IP address to the government.[132] In many of the Playpen cases, courts determined that no search had occurred.[133] It is easy enough to accept those Playpen decisions because the defendants are unsympathetic as "victims" of a search. "But every person is the victim, for the technology we exalt today is everyman's master."[134]

---

128. *See* Katz v. United States, 389 U.S. 347, 353 (1967) (holding that "the 'trespass doctrine' can no longer be regarded as controlling").

129. *See* Florida v. Jardines, 596 U.S. 1, 5 (2013) (explaining that the *Katz* definition of search "add[s] to the baseline, it does not subtract anything from the Amendment's protections 'when the government *does* engage in a physical intrusion of a constitutionally protected area'" (quoting United States v. Knotts, 460 U.S. 276, 286 (1983))); United States v. Jones, 565 U.S. 400, 406–07, 409 (2012) (citing Kyllo v. United States, 533 U.S. 27, 34 (2001)); United States v. Knotts, 460 U.S. 276, 278 (1983); Alderman v. United States, 394 U.S. 165, 176 (1969) (explaining that the *Katz* "reasonable expectation of privacy test has been *added* to, not *substituted* for the common-law trespassory test").

130. *See* Kaleigh E. Aucoin, Note, *The Spider's Parlor: Government Malware on the Dark Web*, 69 HASTINGS L.J. 1433, 1449–50 (2018) (discussing motions to suppress evidence gathered through NIT).

131. *See id.* at 1449 (explaining the FBI's tactics in Playpen and stating that, although the FBI had employed similar tactics before, the Playpen cases were particularly controversial "because a single warrant led to an estimated collection of IP addresses ranging somewhere in the thousands").

132. *See id*. at 1446 (explaining how malware infects a device).

133. *See id.* at 1442, 1450–51 (explaining how the government uses NIT and stating that the government "deploy[ed] a NIT to any person's computer who logged into Playpen regardless of where they logged in from").

134. United States v. White, 401 U.S. 745, 757 (1971) (Douglas, J.,

Online companies use IP addresses to "know exactly what devices (and users) are utilizing their services."[135] An IP address is more than simply the address where you receive an email.[136] It can be used to track your very movements.[137] In the future, in the interconnected world, almost all tangible items will have an IP address.[138] Not only cars and phones will be traceable, but children, dogs, books (if they still exist), food, almost everything will have an IP address.[139] To allow the government to have unfettered access to our every movement is unfathomable. Those judicial decisions that fail to recognize the centrality of the IP address to our every movement are relics of a pre-interconnected world.

This Note argues that, in cases of botnet takedowns, the government's collection of IP addresses is a search under both the *Katz* test and the trespass test. To demonstrate the inevitable dangers of a different conclusion, this section will trace Supreme Court jurisprudence as it pertains to technology.

B. Katz*: A Beacon of Hope?*

The rise of technology has exacerbated the already difficult question of what constitutes a Fourth Amendment search. In the first era of search law, courts held that there could be no Fourth Amendment search without a physical intrusion of a constitutionally protected area.[140] In 1967, faced with a case of

---

dissenting).

135. GOODMAN, *supra* note 46, at 66.

136. *See id.* at 54 (explaining that IP addresses are "exploited to give internet companies and their advertisers a clear and persistent look at you and your online activities").

137. *See id.* at 209 (explaining how IP addresses aid in the surveillance of online activities).

138. *Id.* at 287; *see What Is an IP Address?*, AVAST ACAD., https://www.avast.com/c-what-is-an-ip-address (last updated Feb. 6, 2020) (last visited Oct. 16, 2020) ("Every single device that is connected to the internet has an IP address.") [perma.cc/7DH3-U2Z6].

139. *See* GOODMAN, *supra* note 46, at 287 ("We can think of today's internet as the size of a golf ball. Tomorrow's will be the size of the sun.").

140. *See* JOSHUA DRESSLER & GEORGE C. THOMAS, CRIMINAL PROCEDURE: INVESTIGATING CRIME 95 (6th ed. 2017) (explaining that early search law used a property-based approach).

electronic eavesdropping, the Supreme Court kicked off a new era of search law.[141]

In *Katz*, government agents installed an electronic listening device to the outside of a telephone booth that the defendant used to place his calls.[142] The government asserted that no search had occurred because the phone booth was not a constitutionally protected area and agents had not physically penetrated the phone booth.[143]

Eschewing a strict adherence to the trespass doctrine, the Court instead focused on privacy.[144] The Court declined to decide whether or not the phonebooth was constitutionally protected, noting that

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[145]

Turning next to the issue of physical intrusion, the Court determined that "the reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[146]

The Court held that a Fourth Amendment search had occurred, and in his concurring opinion, Justice Harlan articulated a two-prong test that has since "become the primary standard for determining whether police conduct constitutes a search:"[147] "[F]irst, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[148]

---

141. *See id.* at 96 (noting that the "second period of 'search' law" began with *Katz*).

142. *See* Katz v. United States, 389 U.S. 347, 348 (1967) (providing the facts of the case).

143. *See id.* at 351–54 (noting the government's arguments).

144. *See id.* at 351 (noting that the government can violate an individual's Fourth Amendment right to privacy without committing a physical trespass).

145. *Id.* at 351.

146. *Id.* at 353.

147. DRESSLER & THOMAS, *supra* note 140, at 102.

148. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

The new approach was attractive in part because of its flexibility, which alleviated concerns about how the government could use technology to circumvent the stringent requirements of the trespass doctrine.[149] For example, in *Kyllo v. United States*,[150] a government agent used a thermal-imaging device to establish that the defendant was using heat lamps to grow marijuana in his home.[151] It has long been accepted that the Fourth Amendment's protections of the home are especially powerful.[152] Nonetheless, this egregious invasion slips through the cracks of the trespass doctrine.

Though the device was aimed at a constitutionally protected area (a private home), there was no physical intrusion.[153] The agent operated the device from a public street,[154] and the device picked up heat emanating from the outer surface of the house.[155] Noting that "in the case of the interior of homes . . . there is ready criterion, with roots deep in the common law, of the minimal

---

149. *See* United States v. White, 401 U.S. 745, 748 (1971)

> Until *Katz v. United States*, neither wiretapping nor electronic eavesdropping violated a defendant's Fourth Amendment rights 'unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house or curtilage for the purpose of making a seizure.

(quoting Olmstead v. United States, 277 U.S. 438, 466 (1928); Goldman v. United States, 316 U.S. 129, 135–36 (1942)).

150. *See* Kyllo v. United States, 533 U.S. 27, 41 (2001) (holding that "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant").

151. *See id.* at 29 (providing the facts of *Kyllo*).

152. *See* Payton v. New York, 445 U.S. 573, 589–90 (1980) ("[A]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." (quoting Silverman v. United States, 365 U.S. 505, 511 (1961))); Florida v. Jardines, 596 U.S. 1, 5 (2013) ("When it comes to the Fourth Amendment, the home is first among equals.").

153. *See Kyllo*, 533 U.S. at 35 (noting that "a thermal imager captures only heat emanating from a house").

154. *See id.* at 30 ("The scan of Kyllo's home . . . was performed from the passenger seat of Agent Elliott's vehicle across the street from the front of the house and also from the street in back of the house.").

155. *See id.* (noting that the device could not penetrate the surface of the house).

expectation of privacy that exists, and that is acknowledged to be reasonable,"[156] the Court held that the *Katz* reasonableness test is automatically satisfied if the government uses technology that is not widely available to the public in order to obtain information about the interior of the home.[157]

When viewed in light of the *Kyllo* holding, it seems as though the government has performed a search if it retrieves information from an individual's infected device. The precise language does cabin the rule to investigations aimed at private homes. But the government cannot ensure that a sinkhole will only capture public IP addresses.[158] The sinkhole will capture the addresses of any computer infected with the malware.[159] That could be a device located in a public area, but it could also be a home computer, a home's smart refrigerator, or a home's Echo device—anything that contains the botnet's malware.[160]

Furthermore, the Court has indicated that, because of the amount of information stored on cell phones and computers, privacy expectations on those devices are tantamount to those of a home.[161] Thus, it is reasonable to assume the *Kyllo* holding would extend to an individual's laptop or cellphone even if, at the time of

---

156. *Id.*

157. *See id.* at 34 ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where . . . the technology in question is not in general public use.").

158. *See* Rouse, *supra* note 100 (explaining how a sinkhole works).

159. *See* Markus Rauschecker, *Symposium Essays from the State of Cyberlaw: Security and Privacy in the Digital Age: 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*, 76 MD. L. REV. 1085, 1085 (2017) (explaining that, "if a target location of a computer is unknown," the government cannot know where the search will occur).

160. *See supra* notes 99–103 and accompanying text (defining sinkholing and explaining how it can be used to take down a botnet).

161. *See* Riley v. California, 573 U.S. 373, 396–97 (2014)

> [A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.

the government's hack back,[162] the individual had carried that device into a public area.

But, when it comes to technology, the *Katz* application is not as privacy-friendly as it seems. "[U]nsurprisingly, those 'actual (subjective) expectations of privacy' 'that society is prepared to recognize as 'reasonable," bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable."[163] In application, *Katz* birthed two doctrines that have not aged well in modern times.[164]

1. The Third-Party Doctrine

Under the third-party doctrine, "a person has no legitimate expectation of privacy in information that he voluntarily turns over to third parties."[165] Federal courts have frequently invoked the third-party doctrine to hold that an IP address does not meet the *Katz* test.[166] This section argues that the notion that an IP address is not subject to search because it falls under the third-party doctrine is dated, not only according to recent caselaw, but by technological advances.

The rationale behind the third-party doctrine is that, by conveying information to a third party, an individual assumes the risk that the third party will convey that information to the government.[167] This rationale takes on a particularly sinister vibe

---

162. Hacking back is a term that some cyber-savvy individuals use to describe retaliation efforts against hackers, such as those described in Section II.

163. Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring).

164. *See* discussion *infra* Sections IV.B.1, IV.B.2 (discussing the third-party doctrine and the binary search doctrine).

165. Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (citations omitted).

166. *See* United States v. Christie, 624 F.3d 558, 573 (3d Cir. 2010) ("Federal courts have uniformly held that 'subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation' because it is voluntarily conveyed to third parties." (quoting United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008))). *But see* United States v. Hachey, Criminal No. 16-0128, 2017 U.S. Dist. LEXIS 34192, at *18 (E.D. Pa. Mar. 7, 2017) (refusing to apply the third-party doctrine to the government's collection of IP addresses).

167. *See* Elspeth A. Brotherton, Comment, *Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine*, 61 EMORY L.J. 555, 574–75 (2012) (explaining the assumption of risk rationale behind the third-party

when considered in light of ever-advancing technology.[168] In early cases, the Court was generally apathetic to these concerns.

The roots of the third-party doctrine come from a line of "false friend" cases.[169] False friend cases can be divided into two categories: "[P]ure false friend" and "wired false friend."[170] In a pure false friend case, the defendant privately makes statements to an individual who turns out to be a government informant.[171] The false friend then relays that information to the government.[172] In a wired false friend case, the informant wears a device that records or electronically transmits the information to law enforcement.[173] Before *Katz*, the Court routinely found no Fourth Amendment violation regardless of whether the false friend was wired.[174] Under the pre-*Katz*, property-based approach to search law, it makes sense not to distinguish between wired and pure.[175] But the Court also articulated an additional rationale: Assumption of risk.[176]

In *United States v. White*,[177] a post-*Katz* wired false-friend case, a plurality of the Court seized upon that assumption of risk rationale and merged it into the objective prong of *Katz*: An

---

doctrine).

168. *See id.* at 577 ("Legal commentators generally disagree with the soundness of the doctrine, criticizing the Court's understanding of what constitutes 'reasonable' expectations of privacy as out of touch with reality.").

169. *See id.* at 574–75 (discussing the evolution of the third-party doctrine).

170. *See* JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE, VOL. 1: INVESTIGATION 81–82 (6th ed. 2016) (describing the two categories of false friend cases).

171. *See id.* at 82 (providing a basic "pure false friend" fact pattern).

172. *See id.* (providing a basic "pure false friend" fact pattern).

173. *See id.* (providing a basic "wired false friend" fact pattern).

174. *See id.* at 84 ("Prior to *Katz*, the fact that a false friend was 'wired' with a transmitter or tape recorder was irrelevant to 'search' analysis.").

175. *See id.* ("As long as the agent did not trespass, no search occurred.").

176. *See* Hoffa v. United States, 385 U.S. 293, 302 (1966) (holding that the defendant could not invoke the Fourth Amendment to prevent his false friend from testifying against him and noting that the Fourth Amendment does not "protect[] a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it"); Lopez v. United States, 373 U.S. 427, 438 (1963) (holding that the defendant's statements, which had been tape recorded by a false friend, were not the product of a search and noting that the defendant "knew full well" that those statements "could be used against him").

177. United States v. White, 401 U.S. 745, 750 (1971) (holding that *Katz* did not disturb the Court's previous false friend decisions).

individual cannot have a legitimate, constitutionally protected expectation that a person he speaks to will not reveal the conversation to the police.[178] According to the *White* Court, there is no constitutional difference between a pure false friend and a wired false friend.[179] Harlan, the author of the *Katz* test, wrote a fiery dissent.[180] Harlan agreed that *Katz* left pure false friend cases undisturbed, but, citing Orwellian concerns, he urged that wired false friend cases should be overturned.[181]

In *United States v. Miller*,[182] the seminal third-party case,[183] the Court extended the assumption of risk rationale to apply to information conveyed to a third-party entity.[184] Upholding the warrantless search of a defendant's banking records, the Court

---

178. *See id.* at 751

> If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant's constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others from transmissions received from the agent to whom the defendant is talking and whose trustworthiness the defendant necessarily risks.

179. The Court explains that the Fourth Amendment does not require the suppression of evidence in pure false friend cases and states that

> For constitutional purposes, no different result is required if the agent . . . either (1) simultaneously records them with electronic equipment which he is carrying on his person (2) or carries radio equipment which simultaneously transmits the conversations either to recording equipment located elsewhere or to other agents monitoring the transmitting frequency.

Id. at 751.

180. *See id.* at 769–95 (Harlan, J., dissenting) (urging that Fourth Amendment jurisprudence had moved away from the rationale of previous wired false friend cases).

181. *See id.* at 777 ("[I]t is one thing to subject the average citizen to the risk that participants in a conversation with him will subsequently divulge its contents to another, but quite a different matter to foist upon him the risk that unknown third parties may be simultaneously listening in.").

182. *See* United States v. Miller, 425 U.S. 435, 443 (1976)

> The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

183. *See* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) ("The third-party doctrine largely traces its roots to *Miller*.").

184. *See* Brotherton, supra note 168, at 574–75 (tracing *Miller*'s assumption of risk rationale to the false friend cases).

stated that "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[185]

In *Smith v. Maryland*,[186] the Court extended the rationale even further. In that case, the government asked a phone company to install a pen register in order to record the numbers that the defendant dialed from his home telephone.[187] The Court determined that the defendant's privacy interest in outgoing phone numbers did not meet the objective prong of *Katz*.[188] To reach this holding, the Court reasoned that "all telephone users realize that they must 'convey' phone numbers to the telephone company," and thus those numbers are covered by the third-party doctrine.[189] According to the Court, the fact that the information was conveyed to a switchboard, rather than a telephone operator, was immaterial to a third-party doctrine analysis.[190]

Although *Miller* and *Smith* ostensibly rely on an assumption of risk rationale, those cases' broad conception of "voluntariness" seem to undermine that rationale's logic.[191] Can an individual really be charged with volunteering to provide information if providing such information is nearly a requirement of modern life?[192] This broad conception of the third-party doctrine is "ill suited for the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[193]

---

185. *Miller*, 425 U.S. at 443.

186. Smith v. Maryland, 442 U.S. 735, 744 (1979) (holding that the defendant had no legitimate expectation of privacy in the telephone numbers he dialed because he "voluntarily conveyed that information to the telephone company").

187. *See id.* at 737 (providing the facts of the case).

188. *See id.* at 744 ("[E]ven if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as reasonable.'" (quoting *Katz*, 389 U.S., at 361)).

189. *Id.* at 742.

190. *See id.* at 745 ("We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.").

191. *See id.* at 750 (Stewart, J., dissenting) ("It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.").

192. *See id.* at 749 ("Implicit in the concept of assumption of risk is some notion of choice.").

193. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J.,

In *Carpenter v. United States*,[194] the Court narrowed the scope of the third-party doctrine. In that case, the government obtained cell-site tracking information from the defendant's wireless carriers.[195] Rejecting the government's argument that the information was covered by the third-party doctrine, the Court articulated two rationales behind the doctrine and determined that neither rationale was satisfied.[196]

First, the Court stated that "[t]he third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another."[197] The Court stated that this rationale required an inspection of the nature of the information.[198] This notion, that there is a qualitative consideration embedded in the third-party doctrine, was not a proper application of *Miller* and *Smith*.[199] Although those cases indeed noted the quality of the information procured, "the fact that information was relinquished to a third party was the entire basis for concluding that the defendants in those cases lacked a reasonable expectation of privacy."[200] Nonetheless, the *Carpenter* Court focused on the accuracy and detail of cell site location information, noting that "when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."[201]

Next, the Court turned to the notion of "voluntary exposure" (i.e. assumption of risk).[202] The Court noted that the use of a cell

---

concurring).

194. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (holding that cell site location information is not covered by the third-party doctrine).

195. *See id.* at 2211 (providing the facts of the case).

196. *See id.* at 2210 (explaining the rationales behind the third-party doctrine).

197. *Id.*

198. *See id.* (emphasizing that the opinions in *Smith* and *Miller* took note of the nature of the information).

199. *See id.* at 2231 (Kennedy, J., dissenting) (arguing that the majority opinion misinterprets *Miller* and *Smith*).

200. Carpenter v. United States, 138 S. Ct. 2206, 2232 (2018) (Kennedy, J., dissenting).

201. *Id.* at 2217.

202. *Id.*; *see also* Brotherton, *supra* note 202 at 577–78 (discussing the

phone is "indispensable to participation in modern society."[203] Further noting that the data was recorded "without any affirmative act on the part of the user beyond powering up," the Court determined that the cell phone user had not meaningfully "assum[ed] the risk" of disclosing the data.[204]

Applying *Miller* and *Smith* would seem to indicate that, like the banking records and pen register information at issue in those cases, an IP address would not be the type of information that would require a warrant. By merely having an IP address, an individual has voluntarily turned her IP address over to her ISP, thus waiving her right to privacy of that information.

In a post-*Carpenter* world, however, the analysis is less clear. By focusing on the necessity of cell phones, the *Carpenter* opinion ostensibly revitalizes a true voluntariness requirement.[205] However, the opinion does not overturn *Miller*, and as the dissent points out, carrying a cell phone is no more of a necessity than having a bank account.[206] Thus, it is possible that the Court's primary concern was the sheer amount of information contained in the cell site data. Regardless, *Carpenter* illustrates that the Court is prepared to alter doctrine, and perhaps even abandon it, to stay current with the times, or at least to appear to do so.[207]

An IP address, like a cell phone, is a necessity of life in the modern world.[208] Thus, under a *Carpenter* analysis, the voluntariness requirement is not met.[209] Furthermore, although IP

---

relationship between "volunteered" information and assumption of risk).

203. *Carpenter*, 138 S. Ct. at 2220 (2018).

204. *Id.*

205. *Id.* (noting that cell phones are a necessity of modern life and refusing to hold that cell site location information, though held by a third party, is subject to the third-party doctrine).

206. *See id.* at 2232 (Kennedy, J., dissenting) (arguing that using a bank account is "no more or less necessary than the decision whether to use a cell phone").

207. *See id.* at 2220 (limiting the third-party doctrine by excluding cell site location information).

208. *See* GOODMAN, *supra* note 138 (discussing the operation and ubiquity of IP addresses).

209. *See* Carpenter, 138 S. Ct. at 2220 (2018) (noting that the third-party doctrine covers information that is voluntarily shared); *see also* Brotherton, *supra* note 202, at 577–78 (discussing the relationship between "volunteered" information and the third-party doctrine).

addresses are currently not as revealing as cell site locations, predictions about the interconnectedness of the future digital universe indicate that IP addresses would be more ubiquitous than cell phones—and provide abundant information about almost everything.[210] The new IP allows for so many internet connections "that within the coming years, not only will every computer, phone, and tablet be online, but so too will every car, house, dog, bridge, tunnel, cup, clock, pacemaker, cow, streetlight, pipeline, toy, and soda can."[211] Everything and everybody will be connected.[212] In that world the Justices will very likely blanche at the notion of the government possessing such information.

2. The Binary Search Doctrine

The Supreme Court has repeatedly emphasized that society is not willing to legitimize an individual's privacy interest in contraband.[213] And thus, under the binary search doctrine, "government conduct that *only* reveals the possession of contraband" is not a search because it does not compromise an expectation of "privacy that society is prepared to consider reasonable."[214]

When a botnet takedown reports a victim's IP address to the government, it tells the government only that that computer is infected with illegal malware.[215] Thus, it might seem alluring to slap the binary search doctrine onto the conduct and call it a day. But extending the binary search doctrine to "obtain identifying information" turns the doctrine on its head.[216]

---

210. *See* GOODMAN, *supra* note 46, at 288 (discussing the future interconnectedness of the Internet of Things).

211. *Id.* at 287.

212. *See id.* (noting that, in the future, virtually everything will be connected to the internet and capable of sharing information).

213. *See* Illinois v. Caballes, 543 U.S. 405, 408 (2005) ("We have held that any interest in possessing contraband cannot be deemed legitimate . . . ."); *see also* United States v. Jacobsen, 466 U.S. 109, 123 (1984) ("A chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy.").

214. *Caballes*, 543 U.S. at 408–09 (citing *Jacobsen*, 466 U.S. at 122, 123).

215. *See* Zeitlin, *supra* note 18, at 752 (describing the processes involved in a botnet takedown).

216. *See* Meyer, *supra* note 47, at 608 ("Government hacking to obtain

To illustrate, consider a dog sniffing luggage in an airport, the archetypal application of the binary search doctrine.[217] The dog alerts to a particular individual's luggage, letting the officer know that the individual has drugs in her bag.[218] Under the binary search doctrine, the individual has not been searched.[219]

Now, consider another example. A police officer, sitting at the police station, suspects that there are people in America walking down the street with marijuana in their pockets. Luckily for him, the police officer has a piece of technology which allows him to press a button and learn the location of every individual who is carrying marijuana. Does the binary search doctrine still apply?

The latter hypothetical seems absurd, but it demonstrates the dangers of contorting the binary search doctrine to cover the government's collection of IP addresses in botnet takedowns. What if the government could press a button and learn the IP address of every computer in America that contains illegally downloaded music files?[220] That is a very real possibility.[221]

To comport with the established application of the binary search doctrine, as demonstrated in the first hypothetical, the government would need to know a potential botnet victim's individual IP address, then use technology which simply reported back whether or not that individual's device was indeed infected.[222] In other words, a binary search can only answer one question: Yes or No? It should not be extended to cover: No or Yes—and here is where to find them.[223]

---

identifying information . . . does not implicate the Fourth Amendment's exception for contraband. There is nothing inherently unlawful about an IP address.").

217. United States v. Place, 462 U.S. 696, 687–68 (1983).

218. *Id.*

219. *See id.* at 707 (concluding that exposing someone's luggage to a drug sniffing dog does not constitute a search).

220. *See* Meyer, *supra* note 47, at 613–14 ("Are we prepared for a society in which, at the press of a button, the government could constitutionally hack and identify millions of Americans who have committed mundane misdemeanors?").

221. *See id.* at 614 ("This is no thought experiment: [T]he technology is straightforward and exists today.").

222. *See id.* at 608 ("Government hacking to obtain identifying information . . . does not implicate the Fourth Amendment's exception for contraband. There is nothing inherently unlawful about an IP address.").

223. *See id.* (explaining that the binary search doctrine applies only to "technique[s] that solely indicate[] the presence or absence of contraband").

C. It's Alive!: The Resurrection of the Trespass Doctrine

For a time, the *Katz* analysis seemed to have replaced the trespass doctrine entirely.[224] Fact patterns that satisfy the trespass test usually also satisfy the *Katz* analysis.[225] Take the paradigmatic trespassory search, in which a police officer breaks into a home looking for evidence: Such conduct would of course meet the trespass test, but it would also readily meet the *Katz* expectation of privacy analysis.[226] Thus, at first glance, it seems that *Katz* would cover any circumstance that the trespass doctrine would have covered and then some. But the binary search and third-party doctrine create opportunities for the government to use technology to collect information without meeting the *Katz* analysis.

Worry not. In 2012, forty-five years after *Katz*, the Supreme Court made an important clarification: *Katz* is a supplement to, and not a replacement of, the trespass doctrine.[227] This revelation comes courtesy of another electronic surveillance case, *Jones v. United States*.[228]

In *Jones*, the government put a tracking device on the defendant's car and monitored his movements for weeks.[229] The government arguably had precedent on its side. In two "beeper

---

224. *See* DRESSLER & THOMAS, *supra* note 140, at 160 (describing *Jones* as "the return of the trespass doctrine to the 'search' analysis").

225. *See* United States v. Jones, 565 U.S. 400, 407–08 (2012)

> We have embodied [the] preservation of past [property] rights in our very definition of 'reasonable expectation of privacy' which we have said to be an expectation that has a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.

226. *See* Zeitlin, *supra* note 18, at 771 (explaining that the trespass doctrine and the *Katz* analysis are often overlapping).

227. *Jones*, 565 U.S. at 406–07, 409.

228. *See id.* at 404 ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'").

229. *See id.* at 403 (providing the facts of the case).

cases," *Knotts*[230] and *Karo*,[231] the Court determined that no search had occurred when the government used an electronic beeper to track a defendant's movements on public roads.[232] In *Knotts*, the government implanted a beeper into a can that would be purchased by the defendant.[233] In *Karo*, the government agents "substituted their own can containing a beeper for one of the cans" that was to be shipped to the defendant.[234] Citing the "beeper cases," the government attempted to rely on the third-party doctrine, arguing that "Jones had no 'reasonable expectation of privacy' in the area of the Jeep accessed by Government agents (its underbody) and the locations of the Jeep on public roads, which were visible to all."[235]

Insisting that "Fourth Amendment rights do not rise or fall with the *Katz* formulation," the Court declined to address the government's *Katz* expectation of privacy argument.[236] Instead, the Court announced that "*Katz* did not narrow the Fourth Amendment's scope" and the trespass doctrine was alive and well.[237] The Court pointed out that there was one important distinction between *Jones* and the prior beeper cases: In *Jones*, the government trespassed.[238] In both *Knotts* and *Karo*, the government installed the beepers into the cans before they came into the defendants' possession.[239] On the other hand, the defendant in *Jones* owned his car at the time of the installation.[240]

---

230. *See* United States v. Knotts, 460 U.S. 276, 281 (1983) (holding that "a person traveling in an automobile on public thoroughfare has no reasonable expectation of privacy in his movements").

231. *See* United States v. Karo, 468 U.S. 705, 714 (1984) (holding that the information gained from the beeper when it was within the defendant's private residence was a search but that the evidence gained when he was on public streets was not a search).

232. *See Knotts*, 460 U.S at 281 (stating that the defendant did not have an "expectation of privacy" for his movements on public roads); *see also Karo,* 468 U.S. at 714 (noting that an individual cannot expect for his public actions to be private).

233. *See Knotts*, 460 U.S at 277 (providing the facts of the case).

234. *See Karo,* 468 U.S. at 708 (providing the facts of the case).

235. United States v. Jones, 565 U.S. 400, 406 (2012).

236. *Id.*

237. *Id.* at 408.

238. *See id.* at 408–10 (distinguishing *Jones* from *Knotts* and *Karo*).

239. *See id.* (distinguishing *Jones* from *Knotts* and *Karo*).

240. *See id.* (noting that *Jones* "is on much different footing" than *Knotts* and *Karo* because Jones owned the car "at the time the Government trespassorily

In *Florida v. Jardines*,[241] the Supreme Court considered whether a Fourth Amendment search had occurred when police officers brought a drug-sniffing dog onto the defendant's porch.[242] The dog alerted to the smell of drugs, and police used the information obtained from the dog to get a warrant to search the defendant's home.[243]

The only information sought through the use of the drug-sniffing dog was whether or not the defendant had illegal narcotics in his home.[244] Thus, the Court could arguably have applied the binary search doctrine and determined that no Fourth Amendment search had occurred. Instead, lauding the trespass doctrine for "keep[ing] easy cases easy," the Court stated that the fact that "the officers learned what they learned only by physically intruding on [the defendant's] property to gather evidence is enough to establish that a search occurred."[245]

Jones and *Jardines* clarify that when the government physically intrudes on a constitutionally protected area for the purpose of gaining information, a Fourth Amendment search has occurred, regardless of whether or not the information sought is "private."[246] Thus, even if an IP address is not "private" under a *Katz* analysis, the process the government uses to gather that information might be a search under the trespass test.

Obviously, the information-gathering requirement is satisfied by the collection of IP addresses. Furthermore, the infected devices are likely to be in homes or other constitutionally protected areas.[247] And, even if the device is not in a constitutionally

---

inserted the information-gathering device").

241. *See* Florida v. Jardines, 596 U.S. 1, 7 (2013) (determining that a Fourth Amendment search had occurred because the government had conducted an investigation in a constitutionally protected area and the investigation was "accomplished by an unlicensed physical intrusion").

242. *Id.* at 3–4.

243. *Id.* at 4.

244. *Id.*

245. *Id.* at 11.

246. *See id.* at 5, 9 (Brennan, J., concurring) (outlining the trespass test (citing *Jones*, 565 U.S. at 406–07 n.3; United States v. Knotts, 460 U.S. 276, 286 (1983))).

247. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) ("A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.").

protected area, the device itself is likely to be a cell phone or computer, and the Court has indicated that the constitutional protections extended to cell phones and computers are tantamount to the protections afforded to the home.[248]

The sticking point in a trespass-based analysis of a botnet takedown is whether or not there has been a physical intrusion.[249] The question of whether the government's use of malware to learn an IP address constitutes a search has generally been considered in NIT cases, where the government planted the malware in the computer in the first place.[250] In such cases, courts have been inconsistent in their trespass analysis, highlighting the difficulties of applying the trespass doctrine in the digital world.[251] But the best answer is that implanting malware is a physical intrusion, albeit a tiny one.[252]

In one NIT case, the judge noted that malware itself is computer code, which "ultimately consists of flipped bits on magnetic storage."[253] The judge concluded that a physical intrusion had occurred.[254] But the judge implicitly acknowledged that the trespass doctrine may be a poor fit for a "computerized search" and bolstered his decision that the government had conducted a search

---

248. *See* Riley v. California, 573 U.S. 373, 396–97 (2014)

> [A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.

249. *See* United States v. Hachey, Criminal No. 16-0128, 2017 U.S. Dist. LEXIS 34192, at *20 (E.D. Pa. Mar. 7, 2017) (determining that the government's hack back constituted a physical trespass but also noting that some may question that determination).

250. *See* Aucoin, *supra* note 130, at 1449–50 (discussing the government's use of NIT technology as it pertains to the Fourth Amendment).

251. *See, e.g.*, United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010) (determining that the government's use of NIT did not constitute search). *But see Hachey*, 2017 U.S. Dist. LEXIS 34192, at *20 (determining that the use of NIT software was a physical intrusion).

252. *See Hachey*, 2017 U.S. Dist. LEXIS 34192, at *18 (holding that "computer code . . . did indeed physically occupy Defendant's computer in his home").

253. *Id.*

254. *Id.*

by discussing non-trespass Supreme Court cases "where high-tech methods were at issue."[255]

Unlike NIT cases, when the government sinkholes a botnet it does not implant devices with malware.[256] Rather, it takes over the botnet's already existing malware, which is distributed throughout devices all over the world. Does the government physically intrude by taking over an already implanted physical object?

It is difficult to analogize this conduct to traditional, physical world applications of the trespass doctrine. In *Jones*, the government performed a trespassory search by planting a tracking device on the defendant's car.[257] In *Knotts* and *Karo*, however, there was no trespass because the tracking devices had already been implanted in the cans at the time that they came into the defendants' possession.[258] The government's takeover of malware does not fit neatly into either of these fact patterns. Unlike *Jones*, when the government takes over malware, the government does not originate the physical intrusion, it simply changes the character of that physical intrusion.[259] Before the sinkhole, the botnet reported to a hacker.[260] After the sinkhole, the botnet reports to the government.[261]

Consider the following alteration of *Knotts* and *Karo*: The government has an interest in tracking person A. The government learns that person B, a private citizen, has planted a tracking device on person A's car. Without person A's knowledge, the government electronically takes control of the tracking device. Has the government trespassed?

---

255. *Id.* at *20.

256. *See* Zeitlin, *supra* note 18, at 752–56 (describing the processes involved in a botnet takedown).

257. *See* United States v. Jones, 565 U.S. 400, 408–10 (2012) (distinguishing *Jones* from *Knotts* and *Karo*).

258. *See id.* at 409 (stating that, in *Karo* and *Knotts*, "at the time the beeper was installed the container belonged to a third party, and it did not come into possession of the defendant until later.").

259. *See* Zeitlin, *supra* note 18, at 752–56 (describing the processes involved in a botnet takedown).

260. *See id.* at 748 (explaining that botnets receive commands from botmasters).

261. *See id.* at 751–52 (discussing how "[s]inkholing temporarily prevents the botmaster from controlling infected computers" and gives the government control instead).

Answering this question in the negative is, quite simply, bad for business. Taken to its logical conclusion, such a finding could be extended to determine that no trespass has occurred if the government surreptitiously took over a smart speaker, such as an Alexa-enabled Echo device, in a private home.

One out of every five Americans has a smart speaker in their home.[262] Although these speakers are not always recording, they are always listening.[263] Even though they are not supposed to record until they hear a wake-up word, "contractors hired by device makers to review recordings for quality reasons report hearing clips that were most likely captured unintentionally, including drug deals and sex."[264] If there is no trespass in such a situation, the case would be analyzed under *Katz*, and therefore subjected to the unwieldy third-party doctrine.[265] After *Carpenter*, it is likely that the Court would determine that the application of the third-party doctrine in that case is a bridge too far.[266] But it seems risky to wait to find out.

VI. Rule 41

The Fourth Amendment protects individuals' privacy by requiring the government to obtain a warrant from a neutral and detached magistrate before it can perform a search.[267] Under Rule

---

262. *See* Kashmir Hill, *Activate This "Bracelet of Silence," and Alexa Can't Eavesdrop*, N.Y. TIMES (Feb. 14, 2020), https://www.nytimes.com/2020/02/14/technology/alexa-jamming-bracelet-privacy-armor.html (last visited Sept. 28, 2020) (explaining how ubiquitous smart speakers are) [perma.cc/8RXJ-G88Z].

263. *See id.* ("By design, smart speakers have microphones that are always on, listening for so-called wake words like 'Alexa,' 'Hey, Siri,' or 'O.K., Google.' Only after hearing that cue are they supposed to start recording.").

264. *Id.*

265. *See* United States v. Jones, 565 U.S. 400, 406–07, 409 (2012) (explaining that the *Katz* "reasonable expectation of privacy test has been *added* to . . . the common-law trespassory test").

266. *But cf.* United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) (suggesting that *Carpenter*'s impact on the third-party doctrine is limited to instances where only a small proportion of society would escape the electronic surveillance in question).

267. *See* Lo-Ji Sales v. New York, 442 U.S. 319, 326 (1979) ("We have repeatedly said that a warrant authorized by a neutral and detached judicial officer is 'a more reliable safeguard against improper searches than the hurried

41 of the Federal Rules of Criminal Procedure, a magistrate judge or district court judge can issue a warrant to search property only within her district.[268] The Rule enumerates a couple of exceptions,[269] but, before 2016, none of those exceptions "addressed the special circumstances that arise when officers execute search warrants, via remote access, over modern communications such as the internet."[270]

Thus, before 2016, treating the government's retrieval of IP addresses from infected computers as a search would have created the proverbial chicken and the egg dilemma: Law enforcement needed to know the locations of the infected computers in order to get a warrant to perform the search, but the identity of infected computers was unavailable to law enforcement until after the search had already been performed.[271] Adding to law enforcement's dilemma, botnets are often sprawled on devices throughout the country.[272]

Theoretically, the government could have requested a search warrant in every district in the United States.[273] But, in addition

---

judgment of a law enforcement officer engaged in the often competitive enterprise of ferreting out crime.'").

268. *See* FED. R. CRIM. P. 41(b)(1) ("[A] magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district.").

269. *See* Meyer, *supra* note 47, at 626–27 ("A magistrate can also issue a warrant for property outside her district, but only in exceptional circumstances. Until recently, those circumstances were: property currently within the district that might move outside the district, terrorism investigations, tracking device installation within the district, and crimes committed on certain federal property.").

270. Letter from Mythili Raman, Acting Ass't Att'y Gen., U.S. Dep't of Justice, to the Hon. Reena Raggi, Chair, Advisory Comm. on the Crim. Rules, *supra* note 31.

271. *Cf.* Meyer, supra note 47, at 621 (describing particularity issues associated with warrants to search unknown devices and noting that there is "a seeming chicken-and-egg problem: how can investigators describe, with particularity, the very electronic device that they are attempting to discover").

272. *See* Letter from Mythili Raman, Acting Ass't Att'y Gen., U.S. Dep't of Justice, to the Hon. Reena Raggi, Chair, Advisory Comm. on the Crim. Rules, *supra* note 31 ("[A] large botnet investigation is likely to require action in all 94 districts, but coordinating 94 simultaneous warrants in the 94 districts would be impossible as a practical matter.").

273. *Id.*

to being cumbersome for law enforcement,[274] that solution is fraught with legal peril. There are ninety-four districts in the United States.[275] Even if all ninety-four magistrates were served with nearly identical warrants, it is quite possible that there would not be a consensus among them.[276] In the physical world, allowing each magistrate judge to make her own determination as to whether to sign a warrant is a good thing.[277] However, because of the nature of botnet takedowns, allowing for individualized discretion poses a problem. If ninety-three out of ninety-four magistrates signed off on the search but one magistrate did not, the government could not perform the search because there is no way to make sure that the sinkhole does not retrieve information from the hold-out magistrate's district.[278]

To address these limitations, the Department of Justice campaigned for an amendment to Rule 41 that would allow magistrate judges to grant extra-district warrants in cases involving botnets and other cybercrimes.[279] The amendment was passed in December 2016 and it provides the following:

> [A] magistrate judge with authority in any district where

---

274. *See id.* ("At a minimum, requiring so many magistrate judges to review virtually identical probable cause affidavits wastes judicial and investigative resources and creates delays that may have adverse consequences for the investigation.").

275. *See Court Role and Structure, About Federal Courts,* U.S. COURTS, https://www.uscourts.gov/about-federal-courts/court-role-and-structure (last visited Sept. 27, 2020) ("In the federal court system's present form, 94 district level trial courts and 13 courts of appeals sit below the Supreme Court.") [perma.cc/8DLR-E3NB].

276. *See* United States v. Leon, 468 U.S. 897, 914 (1984) ("Reasonable minds frequently may differ on the question whether a particular affidavit establishes probable cause, and we have thus concluded that the preference for warrants is most appropriately effectuated by according 'great deference' to a magistrate's determination.").

277. *See id.* (noting that it is appropriate to give deference to magistrate's determinations).

278. *See* Rauschecker, *supra* note 159, at 1100 (explaining that, because law enforcement does not know where the infected devices are, it cannot ensure that it will only search computers in certain locations).

279. *See* Memorandum from Jeffrey S. Sutton, Comm. on Rules of Prac. & Proc, Jud. Conf. of the United States to Scott S. Harris, Clerk of the Supreme Court of the United States, Summary of Proposed Amendments to the Federal Rules (Oct. 9, 2015) (on file with the author) (discussing the proposed amendments).

> 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 . . . in an investigation of a violation of [the CFAA], the media are protected computers that have been damaged without authorization and are located in five or more districts.[280]

Many opponents of Rule 41(b)(6)(B) are particularly enraged by the notion that it allows the government to invade the privacy of innocent individuals, who themselves are victims of a botnet.[281] Although this argument is perhaps effective on a visceral level, it has no legal ground to stand on. Under the Fourth Amendment, the government is allowed to search an innocent person's property for evidence of a crime.[282]

A more legitimate concern is how the amendment came to fruition. Instead of going through Congress, the Department of Justice pushed the Rule through the Supreme Court by way of the Advisory Committee.[283] Under the Rules Enabling Act of 1934, the Supreme Court has the authority to make procedural changes to the federal rules, as long as the changes do not "abridge, enlarge, or modify any substantive right."[284] Substantive amendments, on the other hand, must be initiated by Congress.[285]

Opponents of the Rule 41 amendment urge that Congress should have "initiated, debated, and enacted" the amendment because it is "drastic expansion of government authority."[286] Proponents of the change insist that the Rule is simply a "venue" provision.[287]

---

280. FED. R. CRIM. P. 41(b)(6)(B).

281. *See* Rauschecker, *supra* note 159, at 1096 ("[V]ictims of malware could find themselves doubly infiltrated: their computers infected with malware and used to contribute to a botnet, and then government agents given free rein to remotely access their computers as part of the investigation.").

282. *See id.* (admitting that the government is allowed to search innocent parties' property for evidence of a crime).

283. *See* Mordock, *supra* note 26 (noting that the Justice Department "pushed [this amendment] through the rules committee").

284. 28 U.S.C. § 2072(b) (2018).

285. *See* Rauschecker, *supra* note 159, at 1087 (noting that only Congress has the authority to make substantive changes to the Federal Rules).

286. *Id.*

287. *See* FED. R. CRIM. P. 41(b) advisory committee's minutes, at 3, 5 (Mar. 16–17, 2015) (presenting the notes from a discussion about the amendment in

In addition to the substantive versus procedural debate, some opponents of the Rule argue that Congress would likely have produced a "nuanced, detailed set of rules."[288] At the heart of this contention is the fear that the amendment, as written, is overbroad and that the government will take advantage of this breadth to collect data from victims' computers that is not necessary for the takedown efforts.[289]

The Kelihos takedown, described above, assuaged some of these fears.[290] That takedown was the government's first use of the new Rule 41 in the context of botnet takedowns.[291] Opponents of the Amendment were relieved that the government's takedown method in that case was quite similar to pre-Rule 41 peer-to-peer takedown methods.[292] But reliance on executive self-restraint is dangerous.[293]

This Note does not endeavor to address the debate as to whether the 2016 amendments to Rule 41 were an appropriate exercise of power under the Rules Enabling Act. This Note does, however, advocate that the Rule is vague and vulnerable to potential abuse. But, in the author's view, codifying a more detailed set of rules is not the best way to ameliorate these concerns. Botnets, and the methods used to combat them, are

---

which proponents of the amendment assert that the change is merely procedural); FED. R. CRIM. P. 41(b) advisory committee's note to 2016 amendment (insisting that the change is "not substantive" because it simply "identifies the courts that may consider the application for a warrant, not the constitutional requirements for the issuance of a warrant, which must still be met").

288. Mordock, *supra* note 26.

289. *See* Sternstein, *supra* note 110 (discussing the concerns surrounding the Rule 41 amendment).

290. *See id.* (stating that critics were relieved to see that the government had not exploited the Rule 41 amendments); Sara Sun Beale & Peter Berris, *Hacking the Internet of Things*, 16 DUKE L. & TECH. REV. 161, 188 (2018) ("Some critics of the Rule 41 amendments were impressed that the government had been protective of individual privacy: It collected only the victims' IP addresses and 'non-content' routing and signaling information so Internet Service Providers could notify the victims.").

291. *See* Beale, *supra* note 290, at 188 (discussing the Kelihos takedown).

292. *See id.* (noting that the Kelihos takedown was similar to previous takedowns).

293. *See* Aucoin, *supra* note 130, at 1463 ("Executive restraint, while a good thing, is not enough on its own.").

evolving constantly.[294] Thus, a more dynamic approach is appropriate.

A. Constitutional Uncertainty

Right now, the fate of botnet victims' privacy rights is at the mercy of "ongoing case law development."[295] But waiting for caselaw to address constitutional concerns regarding Rule 41(b)(6)(B) is dangerous for two reasons. First, because of the breadth of botnet takedowns and the "sheer amount of data" contained in smart devices, one overly invasive search could result in the exposure of a massive amount of private information.[296]

Second, courts are unlikely to scrutinize the constitutionality of warrants obtained under Rule 41(b)(6)(B). The owners of infected devices will not be prosecuted with evidence procured from their computers, so the constitutionality of warrants obtained under Rule 41(b)(6)(B) will not be challenged under motions to suppress. Thus, a judge would only consider whether a warrant granted under Rule 41(b)(6)(B) violated a botnet victim's Fourth Amendment rights if that victim filed a civil suit.

A civil suit is particularly unlikely because it is quite possible that a victim whose computer has been subjected to a hack back will never even know it.[297] The Rules require the government to make "reasonable efforts" to notify victims,[298] but it is unclear what "reasonable efforts" entail.[299]

---

294. *See supra* Section II (briefly explaining botnets).

295. FED. R. CRIM. P. 41(b) advisory committee's note to 2016 amendment.

296. *See* Gershowitz, *supra* note 121, at 590 ("[B]ecause of the sheer amount of data held on cell phones and the clear overbreadth, particularity, and good faith exception problems present in post-*Riley* search warrants, addressing the execution of the warrant ex post is extremely problematic."); *see also* Rauschecker, *supra* note 159, at 1091 ("The Rule 41 changes would enable the government to obtain a single warrant that would permit it to access and search the thousands or millions of computers involved in a botnet.").

297. *See* Rauschecker, *supra* note 159, at 1098 (discussing the likelihood that owners of hacked computers will never receive notice of the hack and noting that "owners of searched computers who do not get notice of a search may never find out that the search has occurred and will therefore never be able to contest the search warrant").

298. FED. R. CRIM. P. 41(f)(1)(C).

299. *See* Rauschecker, *supra* note 159, at 1098–99 ("It is unclear . . . what

The Department of Justice has suggested that it may ask ISPs to tell victims that their IP addresses have been recorded by the government.[300] When the government employs a takedown method that requires action on the part of the owner of the device, the government has independent incentive, outside of compliance with Rule 41, to provide such notice. However, the Rule gives the government freedom to remotely remove or manipulate the malware.[301] Under those circumstances, some have suggested that it is naïve to imagine that every victim will actually be notified.[302]

B. The Almighty Magistrate

When the government asks a magistrate judge to sign off on a warrant under Rule 41(b)(6)(B), it puts an incredible amount of power in her hands.[303] Because of the sheer breadth of the search and the sensitivity of the information that could potentially be obtained, one misstep could be devastating.[304] Furthermore, because botnet victims are unlikely to bring suit, it is likely that missteps will go uncorrected.[305]

---

notice attempts would constitute a reasonable effort.").

300. *See* Letter from Peter J. Kadzik, Ass't Att'y Gen., U.S. Dep't of Just., to Ron Wyden, Senator, U.S. Senate (Nov. 18, 2016), https://assets.documentcloud.org/documents/3225184/DOJ-Rule-41-Response.pdf (discussing how the government will attempt to notify a botnet victim that her device has been searched) [perma.cc/9D87-ZFUS].

301. FED. R. CRIM. P. 41(b)(6).

302. *See* Rauschecker, *supra* note 159, at 1098 ("It is unrealistic . . . to expect every computer owner of an affected botnet to be notified of a government search.").

303. *See* Sternstein, *supra* note 110 (noting that the Rule 41 Amendment "empower[s] judges to grant a single warrant for searching or seizing information on any number of devices, regardless of location").

304. *See* Gershowitz, *supra* note 121, at 590 ("[B]ecause of the sheer amount of data held on cell phones and the clear overbreadth, particularity, and good faith exception problems present in post-*Riley* search warrants, addressing the execution of the warrant ex post is extremely problematic."); *see also* Rauschecker, *supra* note 159, at 1091 ("The Rule 41 changes would enable the government to obtain a single warrant that would permit it to access and search the thousands or millions of computers involved in a botnet.").

305. *See* Rauschecker, *supra* note 159, at 1099 (explaining that many victims will be unaware of the search so courts will rarely review the warrant's legitimacy).

Thus, it is particularly important that the magistrate judge granting the warrant makes the proper decision in the first place.[306] This is no simple task: Botnets are technologically complex and ever evolving.[307] To satisfy the Fourth Amendment's "reasonableness" requirement, takedown methods should be as unintrusive as possible, while still being effective.[308] But if magistrates do not understand the technology, they cannot evaluate whether the government's request is reasonable.[309] To resolve this problem, magistrate judges should be required to attend Continuing Judicial Education programs focused on botnet technology and takedown methods.[310] Such programs would provide magistrates with the technological framework required to understand the government's Rule 41 takedown requests and determine if those requests are reasonable.[311]

VII. Conclusion

Rule 41 is indeed potentially dangerous. But the alternatives to that Rule are no better. Botnets are destructive and cannot be allowed to run amuck. The government's efforts to combat botnets are not only beneficial, but crucial, to private citizens.[312] Rule 41 allows the government to undertake those efforts within the

306. *See* Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. ONLINE 1, 10–12 (2011) (discussing the potential ramifications of an ill-advised digital search).

307. *See* Aucoin, *supra* note 130, at 1462 (explaining the complexities of the technology involved in applications for searches under Rule 41 and noting that "[a] potential issue here is that those authorized to issue searches . . . do not necessarily understand the technology that they are authorizing.").

308. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated . . . .").

309. *See* Aucoin, *supra* note 130, at 1462 ("If judges do not understand the technology then they cannot understand the government action that they authorize.").

310. *See id.* at 1462–63 (recommending mandatory Continuing Judicial Education in order to "ensur[e] competency in government hacking and surveillance technology as it pertains to the authorization of warrants").

311. *See id.* (explaining that technological Continuing Judicial Education requirements would ensure that magistrates have the "necessary foundation" to evaluate applications under the 2016 amendment to Rule 41).

312. *See supra* Section II (explaining botnets and the dangers posed by them).

confines of the Fourth Amendment.[313] If Rule 41 did not allow the government to apply for warrants in order to perform takedowns, quite frankly, the government would perform those takedowns anyway.[314] And the result would lead to the perversion of the Fourth Amendment's mandates.[315]

This Note demonstrates that potential for perversion by tracing Fourth Amendment jurisprudence as it pertains to technology. Many federal courts have recently invoked that jurisprudence to reach the conclusion that the government's retrieval of an IP address is not a search.[316] Most courts have reached this conclusion by applying the third-party doctrine, holding that an individual has no legitimate privacy interest in her IP address.[317] In this digital era, that understanding of the third-party doctrine is dangerous. *Carpenter* invites courts to walk back a bit on the third-party doctrine, before it becomes a black hole that swallows privacy rights.[318] Courts should accept that invitation.

Having established that the government's collection of IP addresses is indeed a search, this Note does not seek to eliminate the government's opportunity to perform that search. In fact, the collection of IP addresses from infected computers is one of the least intrusive steps the government can take in order to effectively combat botnets. That method ensures that the victim

---

313. *See supra* Section VI. Rule 41 (explaining how the amendment to Rule 41 allows a magistrate to issue a warrant for devices outside her district).

314. *See supra* note 41 and accompanying text (showing that, before Rule 41 was passed, the government obtained civil court orders, rather than search warrants, to combat botnets); *see, e.g.*, *supra* notes 28–31 and accompanying text (noting that, in the Coreflood case, the district court judge determined that the government's proposed action did not implicate the Fourth Amendment).

315. *See supra* Section V. Search: The Collection of IP Addresses (explaining that, to preserve the integrity of the Fourth Amendment, a botnet takedown must be considered a search).

316. *See* United States v. Christie, 624 F.3d 558, 573 (3d Cir. 2010) (noting that federal courts have generally held that an individual does not have a Fourth Amendment right to privacy of her IP address).

317. *See id.* ("Federal courts have uniformly held that 'subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation' because it is voluntarily conveyed to third parties." (quoting United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008))).

318. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (holding that cell site location information is not covered by the third-party doctrine).

will receive notice of the search and minimizes the government's need to muck around on her computer.[319]

Instead, the government should be able to collect IP addresses if it has a valid warrant. Thus, in the age of botnets, the amendment to Rule 41 is essential to ensure the proper balance of national safety and individual privacy. This Note concedes that the wording of the Rule is broad but argues that specific, detailed mandates are not a realistic solution because technology is rapidly advancing. In the context of botnet takedowns, it is dangerous and unrealistic to await caselaw that would reign in potential government oversteps.

Continuing Judicial Education for magistrates is the best way to ensure that the government does not exploit its Rule 41 powers.[320] There should be mandatory programs that provide magistrates with sufficient knowledge to understand the technology behind botnets and botnet takedowns. Armed with that basis of knowledge, magistrates can do their job: Provide a barrier between individual privacy and potentially overzealous policing.

---

319. *See supra* Section IV (explaining the collection of IP addresses).

320. *See* Aucoin, *supra* note 130, at 1462–63 (recommending mandatory Continuing Judicial Education in order to "ensur[e] competency in government hacking and surveillance technology as it pertains to the authorization of warrants").