BOTNET TAKEDOWNS AND THE FOURTH AMENDMENT

SAM ZEITLIN*

The botnet, a group of computers infected with malicious software and remotely controlled without their owners' knowledge, is a ubiquitous tool of cybercrime. Law enforcement can take over botnets, typically by seizing their central "command and control" servers. They can then manipulate the malware installed on private computers to shut the botnet down. This Note examines the Fourth Amendment implications of the government's use of remote control of malware on private computers to neutralize botnets. It finds that the government could take more intrusive action on infected computers than it has previously done without performing a search or seizure under the Fourth Amendment. Most significantly, remotely finding and removing malware on infected computers does not necessarily trigger Fourth Amendment protections. Computer owners have no possessory interest in malware, so modifying or removing it does not constitute a seizure. Additionally, even if the government's efforts cause some harm to private computers, this will rarely produce a seizure under the Fourth Amendment because any interference with the computer will be unintentional. Remotely executing commands on infected computers does not constitute a search under the Fourth Amendment unless information is returned to law enforcement.

 J.D., 2014, New York University School of Law. Many thanks to Andrew Weissman, Samuel Rascoff, Katherine Strandburg, Helen Hershkoff, Luke Dembosky, and Ethan Arenson for guidance and input during the development of this piece. I also owe thanks to the members of the *New York University Law Review* who worked on editing this piece, particularly my indefatigable note editor, Monte Frenkel.

INTRODUCTION

By the middle of April 2011, the Coreflood botnet had infected 2.3 million computers worldwide, including nearly 800,000 in the United States alone.[1] Compromising computers in homes, businesses, hospitals, and governments, the malware extracted online banking credentials and other sensitive personal information, then relayed the data back to a central "command and control" (C&C) server. 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.[2] By the end of April, however, Coreflood infections had dropped by nearly ninety percent in the United States and seventy-five percent abroad.[3] What happened? On April 11, the FBI obtained a court order authorizing them to seize twenty-nine domain names used to control Coreflood and redirect traffic intended for its operators to FBI servers.[4] The order also allowed the FBI to begin sending commands to infected computers, instructing thousands of infected machines to disable the malicious software.[5]

The government's tactics in the Coreflood case raise the question of how the Fourth Amendment should regulate botnet takedowns: If the FBI cleans up a botnet by remotely executing commands on

---

[1] *Coordinated Law Enforcement Action Leads to Massive Reduction in Size of International Botnet*, U.S. DEP'T OF JUSTICE (Apr. 27, 2011), http://blogs.justice.gov/main/archives/1320 [hereinafter *Coordinated Law Enforcement*]; *Fortinet Threat Landscape Research Shows Two New Malware Variants Targeting Facebook Users*, FORTINET (May 5, 2011), http://www.fortinet.com/press_releases/110505.html; Kim Zetter, *FBI vs. Coreflood Botnet: Round 1 Goes to the Feds*, WIRED (Apr. 26, 2011, 2:46 PM), http:///www.wired.com/2011/04/coreflood_results/.

[2] *See* Brian Krebs, *Online Crime Gang Stole Millions*, WASH. POST (Aug. 7, 2008, 3:05 PM), http://voices.washingtonpost.com/securityfix/2008/08/online_crime_gang_stole_millio.html ("By gaining access to an online server used to control the Coreflood network, ... [a researcher] found more than 500 gigabytes of stolen banking credentials and other sensitive data."); *Coordinated Law Enforcement*, *supra* note 1 ("[V]ictims of Coreflood have included 17 state or local government agencies; . . . approximately 20 hospital or health care companies; . . . and hundreds of businesses."); Kim Zetter, *With Court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal*, WIRED (Apr. 13, 2011, 6:17PM), http://www.wired.com/2011/04/coreflood/ ("[O]ne Coreflood command-and-control server held about 190 gigabytes of data . . . . The botnet allowed criminals to loot $115,000 from the account of a real estate company in Michigan . . . as well as $78,000 from a South Carolina law firm.").

[3] *Coordinated Law Enforcement*, *supra* note 1; Gregg Keizer, *Court Order Cripples Coreflood Botnet, Says FBI*, COMPUTER WORLD (Apr. 26, 2011, 5:32 PM), http://www.computerworld.com/s/article/9216190/Court_order_cripples_Coreflood_botnet_says_FBI.

[4] Brian Krebs, *FBI Scrubbed 19,000 PCs Snared by Coreflood Botnet*, KREBS ON SECURITY (June 21, 2011, 6:39 PM), http://krebsonsecurity.com/2011/06/fbi-scrubbed-19000-pcs-snared-by-coreflood-botnet/.

[5] *See id.* (noting that the FBI was granted authority to remotely execute commands on infected computers to disable the malicious software).

infected computers, or by remotely deleting or modifying files on infected hard drives, is it performing searches or seizures? The problem is difficult because it is so unusual. Law enforcement rarely acts remotely on private computers without the owners' knowledge or consent and without any interest in collecting information. As a result, neither courts nor scholars have yet turned their attention to the issue.

This Note will show that what the FBI did in the Coreflood case was neither a search nor a seizure under the Fourth Amendment. In fact, even remotely disabling or removing malware on infected computers need not implicate constitutional rights under current Fourth Amendment doctrine. Part I of this Note describes what botnets do, how they work, and the methods used to dismantle them. Part II considers whether these botnet termination methods are seizures under the Fourth Amendment. This Part argues that remote commands targeting only malware will rarely be seizures. Users have no possessory interest in malware, and in the event that the commands damage their computer or other files, no seizure has occurred unless the damage was intentional. However, if law enforcement intentionally targets the user's legitimate software or files using remote commands, then any significant damage constitutes a seizure. Part III considers whether remote botnet cleanup techniques constitute searches under the Fourth Amendment. It argues that the government can remotely execute commands on infected computers without performing a search, as long as the computer does not report any information back.

I
BACKGROUND

A. Botnets

A botnet is a network of computers all infected with the same malware.[6] In a traditional botnet, a central C&C server sends commands to the malware, remotely controlling the infected machines without their owners' knowledge.[7] Individual infected computers are called "bots," and the cybercriminals who control them are called "botmasters."[8] Botnets can be extremely large. Networks of hundreds of thousands of infected machines are common, with the largest consisting of millions of bots.[9] Between sixteen and twenty-five percent of

---

[6] *See* CYBER FRAUD: TACTICS, TECHNIQUES, AND PROCEDURES 316 (James Graham et al. eds., 2009) [hereinafter CYBER FRAUD] (defining botnets).

[7] *See id.* (describing the general structure of a centralized botnet); HELI TIIRMAA-KLAAR ET AL., BOTNETS 3 (Sandro Gaycken et al. eds., 2013) (same).

[8] CYBER FRAUD, *supra* note 6, at 316.

[9] *See How Big Is Big? Some Botnet Statistics*, ABUSE.CH (May 23, 2011), http://www.abuse.ch/?p=3294 [hereinafter *How Big Is Big?*] (discussing botnet sizes); *see also,*

computers connected to the Internet are estimated to be part of botnets.[10]

Botnets grow by finding vulnerable computers and infecting them with malware. The easiest method is to scan networks for computers running software with known backdoors that can be automatically exploited.[11] To infect computers protected by firewalls and more up-to-date software, botnets employ social engineering—tricking users into compromising their own security.[12]

A social-engineering-based infection typically starts with an innocent-looking email that encourages the reader to open an attachment or click on a link.[13] These emails, disguised as communications from banks, news sites, social-networking sites, online retailers, and so on, are sent indiscriminately to large numbers of individual users.[14] The attachment will be a file that exploits a security vulnerability in the program that opens it—like Microsoft Word or Adobe Reader—

---

e.g., CYBER FRAUD, *supra* note 6, at 316 (noting that Dutch cybercriminals arrested in 2007 were operating a botnet with 1.5 million computers); Wei Meng et al., DNS Changer Remediation Study, Presentation at the Messaging, Malware, and Mobile Anti-Abuse Working Group 27th General Meeting 7 (Feb. 19, 2013), *available at* https://www.m3aawg.org/sites/maawg/files/news/GeorgiaTech_DNSChanger_Study-2013-02-19.pdf (stating that the DNS Changer botnet infected around 4 million computers at its height); Press Release, U.S. Dep't of Justice, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014), http://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware [hereinafter ZeuS Press Release] (putting the size of Gameover ZeuS at between 500,000 and 1 million infected computers).

[10] Sergio S.C. Silva et al., *Botnets: A Survey*, 57 COMPUTER NETWORKS 378, 378 (2013).

[11] This style of botnet propagation is very similar to a worm or virus. *See* CYBER FRAUD, *supra* note 6, at 319 (explaining automated botnet propagation); Markus Koetter, *Know Your Enemy: Tracking Botnets—Introduction*, HONEYNET PROJECT (Aug. 10, 2008, 10:09 PM), http://www.honeynet.org/node/51 (same).

[12] *See* Rafael A. Rodriguez-Gomez et al., *Survey and Taxonomy of Botnet Research Through Life-Cycle*, 45 ACM COMPUTING SURVEYS art. 45 at 8 (2012), *available at* http://wdb.ugr.es/~rodgom/wp-content/uploads/Survey.pdf (describing how botnets spread through spam and malicious websites); *see also, e.g.*, Brett Stone-Gross, *The Lifecycle of Peer-to-Peer (Gameover) ZeuS*, DELL SECUREWORKS (July 23, 2012), http://www.secureworks.com/cyber-threat-intelligence/threats/The_Lifecycle_of_Peer_to_Peer_Gameover_ZeuS/ (describing how the Gameover ZeuS botnet spreads via spam emails).

[13] *See* ORG. FOR ECON. CO-OPERATION & DEV., MALICIOUS SOFTWARE (MALWARE): A SECURITY THREAT TO THE INTERNET ECONOMY 27 (2008), *available at* http://www.oecd.org/internet/ieconomy/40724457.pdf (last visited Mar. 24, 2015) (describing the spread of botnets through social engineering in the form of spam).

[14] *See* Rodriguez-Gomez, *supra* note 12 (noting that botnets send out millions of emails as a recruitment method); Sherly Abraham & InduShobha Chengalur-Smith, *An Overview of Social Engineering Malware: Trends, Tactics, and Implications*, 32 TECH. SOC'Y 183, 185–86 (2010) (describing how users are tricked into thinking they are interacting with trusted institutions and websites); Stone-Gross, *supra* note 12 (detailing the Gameover ZeuS botnet's use of spam emails).

and forces the computer to run hidden code.[15] Links in botnet emails will either directly download an infected file or lead to a malicious website.[16] Such websites exploit security vulnerabilities in browsers and related applications (like Javascript) to infect computers that visit them.[17]

Once a computer is compromised, malware can be downloaded and installed.[18] The malware then establishes contact with the botnet's C&C server to download more tools and send back information.[19] When this is done, the computer is a full-fledged member of the botnet. Most botnets are difficult for all but the most sophisticated users to remove from their computers.[20]

Botnets are the Swiss army knife of cybercrime, a ubiquitous tool used for many different purposes against both the users of infected machines and third parties. Coreflood is a perfect example of botnets' flexibility.[21] When Coreflood was first created sometime around 2002, its primary purpose was to be a tool for distributed denial of service

---

[15] CYBER FRAUD, *supra* note 6, at 113. Newly discovered security holes in widely used applications like Microsoft Word, Adobe Reader, and Java sell for large sums of money on the black market. *See* Violet Blue, *Hackonomics: Street Prices for Black Market Bugs*, ZDNET (Apr. 16, 2014, 9:15 AM), http://www.zdnet.com/hackonomics-street-prices-for-black-market-bugs-7000028490/ (describing online marketplace for exploits). These are called "zero-day exploits," because cybercriminals can take advantage of them on or before the day ("day zero") when the application's vendor becomes aware of the problem. *See* SYMANTEC CORP., INTERNET SECURITY THREAT REPORT 2014 58 (2014), *available at* http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf (describing zero-day vulnerabilities). Once the exploit becomes public, the vendor scrambles to release a patch. Although security-conscious users will immediately apply the update, anyone who continues to run the old, unpatched version of the software remains unprotected.

[16] *See* ORG. FOR ECON. CO-OPERATION AND DEV., *supra* note 13 (describing the use of email attachments and links to spread malware); Silva et al., *supra* note 10, at 383 (describing vectors for botnet infection).

[17] *See* CYBER FRAUD, *supra* note 6, at 113–14 (discussing malicious sites).

[18] *See id.* at 320–21 (discussing methods of malware propagation).

[19] *See* Moheeb A. Rajab et al., *A Multifaceted Approach to Understanding the Botnet Phenomenon*, *in* PROCEEDINGS OF THE 6TH ACM SIGCOMM CONFERENCE ON INTERNET MEASUREMENT 41, 42 (2006), *available at* https://www.cs.jhu.edu/~moheeb/webpage_files/imc06-aburajab.pdf (describing how infected computers download and install botnet binaries); Rodriguez-Gomez, *supra* note 12 (describing how bots register with a botnet).

[20] *See* David Dittrich et al., *A Case Study in Ethical Decision Making Regarding Remote Mitigation of Botnets*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY, FC 2010 WORKSHOPS, RLCPS, WECSR, AND WLC 2010 216, 221 (Radu Sion et al. eds., 2010), *available at* http://staff.washington.edu/dittrich/papers/wecsr2010-botethics-dlw.pdf (noting "the inability of the average computer user to either protect themselves against malware infection through social engineering attacks, or effectively respond when attacked").

[21] *See* Gary Warner, *Bold FBI Move Shutters COREFLOOD Bot*, CYBERCRIME & DOING TIME (Apr. 13, 2011, 9:25 PM), http://garwarner.blogspot.com/2011/04/bold-fbi-move-shutters-coreflood-bot.html (summarizing the history of Coreflood).

(DDoS) attacks.[22] When a botmaster gave the command, each bot would simultaneously try to contact the target website repeatedly, draining the site's bandwidth and knocking it offline.[23] Coreflood's owners then moved into selling anonymity to hackers who could use the bots as untraceable staging points for further cyberattacks.[24] By 2008, Coreflood's focus had moved to bank fraud, using credentials stolen from infected computers to empty their owners' bank accounts.[25] Other common uses for bots include sending spam emails, hosting malicious or illegal websites, "clickfraud" (manipulating the payment systems of online advertising), and bitcoin mining.[26] Botnets can also be used by governments for espionage, infecting and controlling sensitive systems, and extracting confidential data.[27]

B. Botnet Takedowns

Given the ubiquity of botnets and the mischief they cause, it is unsurprising that they have attracted hostile attention from cybersecurity researchers and law enforcement. The weak point of a traditional botnet is its centralized control structure. The malware installed on infected computers contains instructions for how infected computers should "phone home" to the C&C server—specifically, what web domain they should contact to receive orders.[28] The first step in a typical botnet takedown is to take control of one or more domain

---

[22] *See id.* (describing how Coreflood was at first used for DDoS attacks).

[23] *See* CYBER FRAUD, *supra* note 6, at 316–27 (describing the role of botnets in DDoS attacks).

[24] *See* Nick Clayton, *Where to Rent a Botnet for $2 an Hour or Buy One for $700*, WALL ST. J. (Nov. 5, 2012, 9:43 AM), http://blogs.wsj.com/tech-europe/2012/11/05/where-to-rent-a-botnet-for-2-an-hour-or-buy-one-for-700/ (commenting on how cybercriminals will rent out their botnets to other cybercriminals); Joe Stewart, *The Coreflood Report*, DELL SECUREWORKS (Aug. 6, 2008), http://www.secureworks.com/cyber-threat-intelligence/threats/coreflood-report/ (same); Warner, *supra* note 21 (describing how botnet functions varied over time).

[25] *See* Krebs, *supra* note 2 (noting the significant amounts of financial data that the cybercriminals behind Coreflood had pulled from victims' machines).

[26] *See* DANIEL PLOHMANN & ELMAR GERHARDS-PADILLA, CASE STUDY OF THE MINER BOTNET (2012), *available at* https://ccdcoe.org/cycon/2012/proceedings/plohmann_padilla.pdf (analyzing a botnet that mines bitcoins); Yury Namestnikov, *The Economics of Botnets*, SECURELIST (July 22, 2009, 8:52 AM), http://securelist.com/large-slider/36257/the-economics-of-botnets/?print?_mode=1 (listing different uses of botnets); *Uses of Botnets*, HONEYNET PROJECT (Aug. 10, 2008, 10:29 PM), http://www.honeynet.org/node/52 (same).

[27] *See* TIIRMAA-KLAAR ET AL., *supra* note 7, at 12–15 (detailing various instances of botnets facilitating espionage against western nations).

[28] *See* CYBER FRAUD, *supra* note 6, at 321–22 (describing direct and indirect communication models for C&C servers). Note that modern botnets incorporate more complex methods for communication as part of their defenses. *See infra* note 49 and accompanying text.

names used by the C&C server to receive communications from bots, and then to redirect bot traffic to a server controlled by researchers or law enforcement.[29] This process of hijacking a botnet is called "sinkholing," and the new server set up to receive the redirected botnet traffic is a "sinkhole."[30]

Sinkholing temporarily prevents the botmaster from controlling infected computers.[31] Once a sinkhole has been created, the sinkhole's owners can observe as infected computers make contact with their servers and record the IP addresses of the infected machines.[32] Researchers use this method to measure a botnet's size, learn the general geographic location of infected machines, and otherwise analyze the workings of the malware.[33] Law enforcement and companies like Microsoft use information from sinkholes to contact victims (typically via their Internet service providers (ISPs)) and encourage them to remove malware from their computers.[34]

However, sinkholes can play a role in dismantling botnets that goes beyond simply locking out criminals and gathering information. By exploiting features or design flaws in the malware, a sinkhole's

---

[29] *See* DAVID SANCHO & RAINER LINK, SINKHOLING BOTNETS 1 (2011), *available at* http://www.trendmicro.com.tr/media/misc/sinkholing-botnets-technical-paper-en.pdf (defining sinkholing); *How Big Is Big?*, *supra* note 9 (same).

[30] *See* SANCHO & LINK, *supra* note 29 (defining sinkhole and sinkholing); *How Big Is Big?*, *supra* note 9 (same). Some botnets have no centralized control structure to take over, and pass commands from peer to peer. *See* Silva et al., *supra* note 10, at 384–85 (describing decentralized botnets). Although the logistics of neutralizing such botnets are different from what is described in this Note, the basic goal is the same: Law enforcement or security researchers must figure out how the botmasters are propagating instructions through the botnet, and get their own commands through instead. *See* Christian Rossow et al., *SoK: P2PWNED—Modeling and Evaluating the Resilience of Peer-to-Peer Botnets*, IEEE SYMPOSIUM ON SECURITY AND PRIVACY 11–13 (2013), *available at* https://www.christian-rossow.de/publications/p2pwned-ieee2013.pdf (discussing techniques for sinkholing and otherwise attacking peer-to-peer botnets).

[31] *See* BRETT STONE-GROSS ET AL., YOUR BOTNET IS MY BOTNET: ANALYSIS OF A BOTNET TAKEOVER 2 (2009), *available at* https://seclab.cs.ucsb.edu/media/uploads/papers/torpig.pdf (describing how sinkholing denies access to the botnet administrator); Warner, *supra* note 21 (same).

[32] *See* SANCHO & LINK, *supra* note 29, at 1 (using this technique to passively analyze a ZeuS botnet).

[33] *See id.* at 1 (listing the information that researchers can gather about a botnet by creating a sinkhole); STONE-GROSS ET AL., *supra* note 31 (same).

[34] *See* Press Release, Microsoft News Center, Microsoft, the FBI, Europol and Industry Partners Disrupt the Notorious ZeroAccess Botnet (Dec. 5, 2013), http://www.microsoft.com/en-us/news/press/2013/dec13/12-05zeroaccessbotnetpr.aspx ("Microsoft is working with ecosystem partners around the world to notify people if their computers are infected . . . ."); ZeuS Press Release, *supra* note 9 (stating that the FBI would provide IP addresses of victim computers to national computer emergency readiness teams and to private companies as a means of assisting "victims in removing the Gameover ZeuS malware from their computers").

operator can send commands to infected computers with the goal of crippling the botnet itself.[35]

There are three general approaches to this sort of counterbotnet activity. The first is to use the sinkhole to improve victim notification. Rather than locating victims and their ISPs independently and warning them one by one, a sinkhole operator can simply send a message directly to victims through the malware on their infected computers. Dutch police used this tactic successfully in 2010 when they took over Bredolab, an enormous botnet that at its height infected 30 million computers worldwide.[36]

A second option is to use the sinkhole to modify or delete the malware running on infected computers. When Microsoft targeted Citadel botnets in 2013, it used sinkholes to "update" the malware on infected computers.[37] The updates both notified victims and switched off features of the malware blocking users from accessing security websites to download antivirus software.[38] During the Coreflood takedown, the FBI used its sinkholes to remotely command the malware to disable itself.[39] The FBI then notified victims independently and remotely deleted the malware from those who gave written consent.[40] Unfortunately, this approach is not always sufficient to permanently deal with a botnet. Many botnets are spread by another kind of malware called a dropper (or downloader).[41] To fully clean a com-

---

[35] *See* Dittrich et al., *supra* note 20, at 7 tbls. 1 & 2 (describing the various ways in which a sinkhole could be used to destroy a botnet).

[36] *See Dutch Police Use Unusual Tactics in Botnet Battle*, BBC NEWS (Oct. 27, 2010, 10:55 AM), http://www.bbc.com/news/technology-11635317 (describing how in 2010, Dutch police took down a botnet by notifying victims that the security of their computers had been compromised).

[37] *See* James Wyke, *Was Microsoft's Takedown of Citadel Effective?*, NAKED SECURITY (June 10, 2013), http://nakedsecurity.sophos.com/2013/06/12/microsoft-citadel-takedown/ ("Microsoft recently fought back against more than 1400 Citadel botnets by sinkholing their Command and Control (C&C) infrastructure.").

[38] *See id.* (showcasing the command that Microsoft used to notify victims of Citadel that their computers had been compromised and to allow victims to access tools to remove the malware on their own).

[39] *See* Krebs, *supra* note 4 (noting that the FBI sent computers infected with the Coreflood botnet a command telling the machines to stop running the bot software).

[40] *See id.* (noting that the FBI obtained written consent from the victims of Coreflood that it identified before removing the malware from their computers).

[41] Operators of dropper and downloader networks take payments from other cybercriminals to install new malware on computers the operators have compromised. *See* GUNTER OLLMANN, BEHIND TODAY'S CRIMEWARE INSTALLATION LIFECYCLE: HOW ADVANCED MALWARE MORPHS TO REMAIN STEALTHY AND PERSISTENT 2–6 (2011), *available at* https://www.damballa.com/downloads/r_pubs/WP_Advanced_Malware_Install_LifeCycle.pdf (describing dropper and downloader malware and the business model associated with them).

puter, the dropper must be removed from the computer as well—otherwise, the botnet will simply reinfect the machine.[42]

Lastly, the most aggressive use of a sinkhole would be to patch the security flaws on infected computers that made them vulnerable in the first place.[43] This might mean updating programs like Java or Internet Explorer to the latest version, or it could involve installing a custom-written patch. This is the most intrusive intervention because it involves modifying not just the malware, but the user's personal software as well.

Using sinkholes and remote commands to directly target malware on infected computers is important because the traditional victim/ISP notification method for dismantling botnets can be slow and ineffective. Tools that enable users to completely neutralize complex malware are not always readily available or easily used.[44] Providing effective worldwide notice that users will take seriously is also challenging, especially given the prevalence of fake malware alerts and antivirus scams.[45] A study of victim and ISP notification after the FBI sinkholed a botnet called DNS Changer in 2012 found that over the course of eight months, as many as seventy percent of infected computers were cleaned.[46] However, at the end of the study period, more than 200,000 computers remained infected.[47] This slow timescale is a problem because the control granted by sinkholes can be fleeting.[48] Modern botnets include measures to protect against sinkholing, including decentralized peer-to-peer communication and a variety of

[42] *See* Kelly Jackson Higgins, *'Mystery' Malware Files Often Missed in Cleanup*, DARK READING (Dec. 10, 2013, 5:59 PM), http://www.darkreading.com/attacks-breaches/mystery-malware-files-often-missed-in-cl/240164631 (explaining how malware cleanup fails when only the main malware and not the original dropper is removed).

[43] Although to my knowledge this has never actually been done, in most cases there would be no technical barrier to doing so, since the malware will include a means of downloading new software and updates. *See* Silva et al., *supra* note 10, at 383 (describing how infected machines download new binaries and updates). Furthermore, even if such action could not be accomplished using the botnet itself, Microsoft can remotely delete malicious software from many Windows computers. *See* Patrick Howell O'Neill, *Microsoft's Secret Battle Against the Tor Botnet*, THE DAILY DOT (Jan. 17, 2014), http://www.dailydot.com/technology/tor-botnet-microsoft-malware-remove/ (investigating Microsoft's use of this tactic against the Sefnit botnet).

[44] *See* ONLINE TRUST ALLIANCE, BOTNET REMEDIATION OVERVIEW & PRACTICES 7–9 (2013), *available at* https://otalliance.org/system/files/files/best-practices/documents/ota_2013_botnet_remediation_best_practices.pdf (describing difficulties in notifying and providing remediation tools to end users).

[45] *Id.*; *see also id.* at 12 (exploring the problem of anti-virus scams).

[46] *See* Meng et al., *supra* note 9, at 20 (graphing infections over time).

[47] *Id.*

[48] *See, e.g.*, STONE-GROSS ET AL., *supra* note 31, at 5 (explaining that, after a successful sinkhole, the authors controlled the botnet for only ten days before the botnet administrator regained control).

techniques to obscure and rapidly vary the location of the C&C server.[49] Sinkholing a botnet without dealing with all of the contingencies and defenses its creators have developed can allow criminals to quickly regain control.[50] Microsoft has experienced this problem repeatedly, engaging in high-profile strikes against botnets and achieving partial success, only to see botnet operators quickly roll back their gains.[51] The difficulty of successfully taking permanent control of a botnet has led Microsoft to stop describing their efforts as "takedowns," and to start referring to them instead as "disruption" efforts.[52]

Cleaning infected computers by targeting malware directly is also far quicker than notifying the owners of infected systems. In the DNS Changer example discussed above, the FBI and its partners used victim and ISP notification to reduce the botnet's size by seventy percent over eight months.[53] By contrast, when the FBI shut down the Coreflood malware directly from their sinkholes, they achieved a greater reduction in size in less than two weeks.[54]

Furthermore, remote cleanup is useful even when a botnet takedown goes wrong. Consider Microsoft's botched attempt to dismantle the ZeroAccess botnet.[55] Microsoft made two mistakes when it sinkholed ZeroAccess. First, it failed to deal with the botnet's peer-to-peer functionality, so setting up a sinkhole didn't fully prevent the botnet administrator from exercising control.[56] Second, even though

---

[49] *See* Rossow et al., *supra* note 30 (discussing peer-to-peer botnets); *How Criminals Defend Their Rogue Networks*, ABUSE.CH (July 28, 2011), http://www.abuse.ch/?p=3387 (explaining fastflux hosting, domain generation algorithms, and other tools).

[50] *See, e.g.*, Brian Foster, *Three Reasons Why Botnet Takedowns Are Ineffective*, THE DAY BEFORE ZERO, https://www.damballa.com/three-reasons-why-botnet-takedowns-are-ineffective-2/ (last visited Feb. 7, 2015) (describing why past botnet takedowns haven't succeeded in disabling botnets).

[51] *See* Yacin Nadji & Manos Antonakakis, *Microsoft DCU—Strike Three. Now What?*, THE DAY BEFORE ZERO, https://www.damballa.com/microsoft-dcu-strike-three-now-what-2/ (last visited Feb. 7, 2015) (discussing Microsoft's failure to deal with the peer-to-peer component of the ZeroAccess botnet during its takedown attempt); Wyke, *supra* note 37 (observing that many of the domains sinkholed by Microsoft as part of its attempt to takedown the Citadel botnet appeared to have been reclaimed by botnet administrators as of a week later).

[52] Mathew J. Schwartz, *Microsoft Fails to Nuke ZeroAccess Botnet*, DARKREADING (Dec. 10, 2013, 2:40 PM), http://www.darkreading.com/attacks-and-breaches/microsoft-fails-to-nuke-zeroaccess-botnet/d/d-id/1113008.

[53] *See supra* notes 46–47 and accompanying text.

[54] *See supra* notes 1–5 and accompanying text (describing ninety and seventy-five percent reductions in coreflood infections).

[55] *See* Richard Adhikari, *Microsoft's ZeroAccess Botnet Takedown No 'Mission Accomplished*,' TECHNEWSWORLD (Dec. 9, 2013, 9:44 AM), http://www.technewsworld.com/story/79586.html.

[56] *Id.*

the cybercriminals had been locked out and prevented from sending the botnet new orders, Microsoft did not stop infected machines from continuing to follow their previous commands, which involved operating an automated click fraud scheme.[57]

If Microsoft had targeted the malware directly, shutting it down or deleting it, the company could have skirted both of these problems. With the malware removed, there would be nothing for the botnet's creators to regain control of through the peer-to-peer system. Additionally, since the malware would not be sitting active on infected computers, the botnet would be unable to continue its automated fraud scheme. Targeting malware directly is a powerful technique because it turns even a partial, temporary sinkhole into a platform for taking an enormous and permanent bite out of a botnet.

C. Legal Constraints

American courts have so far authorized only two groups to use remote commands against botnets: Microsoft and the FBI. The Computer Fraud and Abuse Act prohibits unauthorized access to computer systems, which restricts some of the more aggressive uses of sinkholes.[58] In general, this is a good thing. Although remote commands are very effective at dismantling botnets, the fact that they intrude on private computers raises legal and ethical concerns.[59] Even the best-designed and most thoroughly tested software inevitably creates problems for some small percentage of consumers when it is installed en masse on thousands or hundreds of thousands of machines.[60] Given the sheer number of computers that make up many botnets, even a carefully planned cleanup operation could cause damage or disruption to some individual computers.[61]

If a private actor tries to clean malware off of a private computer without authorization from the computer's owners, and they inadvertently cause damage, they are criminally liable under the Computer

---

[57] *See id.* (explaining that the attack didn't affect prior commands to botnets).

[58] *See* 18 U.S.C. § 1030(a)(2)(C) (2012) (criminalizing obtaining information from a protected computer through unauthorized access); *id.* § (a)(5)(B)–(C) (criminalizing unauthorized transmission of commands to a protected computer when damage results).

[59] *See, e.g.*, Dittrich et al., *supra* note 20, at 6, 11–13 (describing various ethical concerns in botnet takedowns).

[60] *See* Fahmida Y. Rashid, *Microsoft, FBI Reprogram Botnet to Remove Coreflood Permanently*, EWEEK (Apr. 28, 2011), http://www.eweek.com/c/a/Security/Microsoft-FBI-Reprogram-Botnet-to-Remove-Coreflood-Permanently-488081/ (quoting the Electronic Frontier Foundation's concerns that remote botnet cleanup carries some risk of damaging or destroying a computer while trying to fix it).

[61] *See id.* (citing expert opinion that damage to private computers is a possible outcome of these actions).

Fraud and Abuse Act.[62] As a result, security researchers and other private sinkhole operators generally restrict themselves to keeping track of the numbers and IP addresses of bots as they report in and to notifying Internet service providers (ISPs) or other relevant actors about infected machines.[63]

Microsoft is a notable exception to this rule. The company's Digital Crimes Unit is very active in the fight against botnets, spearheading ten major takedown efforts to date.[64] In a series of ex parte proceedings, Microsoft has successfully convinced district courts to allow it to seize web domains used by botnet C&C servers.[65] During one of those takedowns, discussed above in Part I.B, Microsoft used remote commands to modify Citadel malware installed on private computers, making it easier for users to clean up their machines.[66] The Citadel injunction permitted Microsoft to alter the malware "consistent with the terms of Microsoft's licenses to its Windows operating system."[67] However, Microsoft did not make clear what part of its license actually permits this.[68]

The FBI is exempt from the CFAA because it is a law enforcement agency.[69] The Bureau has led takedown efforts against three botnets, all successfully: DNS Changer and Coreflood in 2011, and

---

[62] *See* 18 U.S.C. § 1030(a)(5)(B)–(C) (containing relevant provisions of the Computer Fraud and Abuse Act (CFAA)).

[63] *How Big Is Big?*, *supra* note 9 (describing sinkholing methods of private security researchers). Some security researchers have come under fire for selling data they acquire via sinkholes. *See* Gunter Ollmann, *Sinkholing for Profit*, DARK READING (Oct. 24, 2011), http://www.darkreading.com/risk/sinkholing-for-profit/d/d-id/1136541 (describing concerns that vendors will utilize information they receive from sinkholes for profit).

[64] Richard Domingues Boscovich, *Microsoft Takes on Global Cybercrime Epidemic in Tenth Malware Disruption*, MICROSOFT (June 30, 2014), blogs.microsoft.com/blog/2014/06/30/Microsoft-takes-on-global-cybercrime-epidemic-in-tenth-malware-disruption.

[65] *See, e.g.*, Microsoft Corp. v. John Does 1–82, No. 3:13-CV-00319 (W.D.N.C. Nov. 21, 2013) [hereinafter Citadel Order] (granting default judgment and permanent injunction, as well as forfeiting ownership of domains to Microsoft). Microsoft's legal theories in these cases have been quite novel, and it's unclear whether they would hold up in an adversarial proceeding.

[66] *See supra* notes 37–38 and accompanying text.

[67] Citadel Order, *supra* note 65, at 11.

[68] *See* Brief in Support of Microsoft's *Ex Parte* Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause for Preliminary Injunction, Microsoft Corp. v. John Does 1–82, No. 3:13-CV-00319 (W.D.N.C. July 29, 2014) (ignoring this issue).

[69] *See* 18 U.S.C. §§ 1030(d)(2), (f) (2012) (outlining the CFAA's exceptions for law enforcement activity).

Gameover ZeuS in 2014.[70] Of those three, the FBI employed remote commands only against Coreflood.[71]

The Coreflood takedown demonstrates how sinkholes combined with remote commands can be used effectively to neutralize malware en masse, but it also raises important constitutional questions. The FBI is not regulated by the CFAA, but as a law enforcement agency it must still obey the Fourth Amendment. When the government uses remote commands to disrupt or remove botnet malware on a private computer, is it performing a search or a seizure?

This question is particularly important because if a warrant were required to issue remote commands, it would be difficult or impossible to obtain one.[72] Rule 41 of the Federal Rules of Criminal Procedure

---

[70] *See Operation Ghost Click*, FBI (Nov. 9, 2011), http://www.fbi.gov/news/stories/2011/november/malware_110911 (publicizing action against DNS Changer); ZeuS Press Release, *supra* note 9 (detailing efforts to combat Gameover ZeuS); *supra* notes 1–5, 21–25, 39–40, and accompanying text (examining action against Coreflood). The FBI is a minor player in most botnet takedowns, where its role is to coordinate with other law enforcement agencies to attempt to catch the cybercriminals responsible for the botnet. *See, e.g.*, Mathew J. Schwartz, *Microsoft, FBI Trumpet Citadel Botnet Takedowns*, INFORMATION WEEK (June 6, 2013, 10:26 AM), www.darkreading.com/attacks-and-breaches/Microsoft-fbi-trumpet-citadel-botnet-takedowns/d/d-id/1110261? (describing the FBI's role in the Citadel botnet takedowns as providing "related information to its overseas law enforcement counterparts"). This paragraph discusses the minority of cases where the FBI also controls the technical aspects of taking over and dismantling the botnet itself.

[71] Although this Note examines the Fourth Amendment's role in regulating botnet takedowns, there are other constraints on the FBI that might prevent them from using remote commands. One is public opinion. Buried among the Snowden leaks was the revelation that the NSA hijacks botnets and uses them to install spyware on infected machines. Joseph Menn, *NSA 'Hijacked' Criminal Botnets to Install Spyware*, REUTERS (Mar. 12, 2014, 5:05 PM), www.reuters.com/article/2014/03/12/us-usa-security-nsa-botnets-idUSBREA2B21420140312. Given the current political climate surrounding government electronic surveillance, FBI interference with private computers might alienate the public and the press, regardless of its motivations. A second constraint is foreign law. Botnets are not restricted by physical borders, and infect computers all over the world. Although the FBI is exempt from the CFAA, meaning it can legally use remote targeting against malware on computers in the United States, this statutory exemption does not grant it permission to do the same on computers in other countries without their permission. This limitation reduces the effectiveness of such interventions. *See* Government's Supplemental Memorandum in Support of Preliminary Injunction at 10–11, United States v. John Doe 1–13, No. 3:11 CV 561 (D. Conn. June 21, 2011), *available at* www.justice.gov/sites/default/files/opa/legacy/2011/04/27/coreflood-govt-supp.pdf (noting that only computers inside the United States were issued commands to stop running Coreflood).

[72] This Note focuses on the question whether the Fourth Amendment regulates the use of remote commands in botnet takedowns at all, so the question whether exceptions to the warrant requirement apply is largely outside its scope. Going through a warrant exception provides no greater protection for privacy—in fact, it's worse than adopting the argument of this paper that the Fourth Amendment does not apply in the first place. The reason is that, to avoid triggering the Fourth Amendment, the FBI cannot collect any information from private computers. *See infra* Part III. However, if an exception to the warrant requirement is used, then there may well be no such limitation. In the Coreflood case, the

allows magistrate judges to issue warrants "to search for and seize a person or property located *within the district*"—a rule of little use against enormous botnets infecting millions of computers across America.[73] Even if prosecutors were to simultaneously seek warrants in every district in the country, the application might still fail for want of particularity.[74] The Fourth Amendment requires that warrant applications "particularly describ[e] the place to be searched, and the persons or things to be seized."[75] However, even prosecutors already armed with a sinkhole to collect bots' IP addresses will have only a

---

FBI invoked the community caretaking exception. Government's Memorandum of Law in Support of Motion for Temporary Restraining Order, Preliminary Injunction, and Other Ancillary Relief at 52–58, United States v. John Doe 1–13, No. 3:11 CV 561 (D. Conn. June 21, 2011), ECF No. 32 [hereinafter Coreflood Memo]. Under this doctrine, police do not need a warrant to carry out noninvestigative aspects of their traditional social role in the community. *See* Cady v. Dombrowski, 413 U.S. 433, 441 (1973) (establishing the doctrine); Michael R. Dimino, Sr., *Police Paternalism: Community Caretaking, Assistance Searches, and Fourth Amendment Reasonableness*, 66 WASH. & LEE L. REV. 1485, 1489–94 (2009) (discussing its development). The FBI analogized sending remote shutdown commands to computers infected with Coreflood as equivalent to closing a front door to a residence left open at night. Coreflood Memo, *supra*, at 53–54. However, this attempt to extend community caretaking to the Internet runs counter to the doctrine's underlying purpose. The doctrine represents judicial recognition of the historic role police officers perform in service to the community—it is justified, at least in part, by long-standing norms. *See* United States v. Markland, 635 F.2d. 174, 176 (2d Cir. 1980) (collecting cases and discussing a case where officers secured the personal effects of an accident victim). There are no equivalent norms about remotely altering or deleting files on private computers, and the doctrine cannot justify such a novel intervention. Furthermore, preexisting norms about the role of police serve to delineate the boundaries of community caretaking. Since no similar context exists for police behavior online, blindly expanding the exception could pose a serious threat to privacy. A more plausible warrant exception is the doctrine of special needs, in which searches without reasonable suspicion are justified by a government interest outside of normal law enforcement. *See, e.g.*, 79 C.J.S. SEARCHES § 60 (2015) (describing the doctrine). In this case, the special need would be dismantling the botnet as a matter of public safety unrelated to any investigation of the owners of individual infected computers. The search would likely be reasonable because it is minimally intrusive, and because the government has a strong public safety interest in eliminating botnets. *Cf.* United States v. Heckenkamp, 482 F.3d 1142, 1147–48 (9th Cir. 2007) (securing university mail center was special need justifying minimally intrusive remote search of a student's computer to determine if it was the machine used to hack the mail center); MacWade v. Kelly, 460 F.3d 260, 271–73 (2d Cir. 2006) (justifying minimally invasive suspicionless searches of bags in New York subway with appeal to special need of preventing terrorist bombing).

[73] FED. R. CRIM. P. 41(b) (emphasis added). Although there are numerous exceptions, none are relevant. *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 757–58 (S.D. Tex. 2013) [hereinafter Premises Unknown] (memorandum and order) (refusing to authorize remote electronic surveillance of an out-of-district computer).

[74] *See* Premises Unknown, 958 F. Supp. 2d at 758–59 (requiring application to show how computers will be found).

[75] U.S. CONST. amend. IV.

very general idea of the location and number of infected machines.[76] At any given time, only some fraction of the infected machines is connecting to the C&C server.[77] Furthermore, many computers on a single network can share the same IP address, while a single laptop can have different IP addresses as it moves between locations (home, work, school, a café, etc.).[78]

In its Coreflood filings, the FBI briefed the Fourth Amendment issue, but it did so ex parte, and the eventual court order granted their request without meaningful analysis.[79] In the sections that follow, this Note will analyze how the Fourth Amendment regulates the botnet takedown tactics described in Part I.B above, first through the lens of seizure and then through the lens of search.

Before continuing further, it is important to acknowledge that the question whether and how the Fourth Amendment regulates remote commands is not the same question as whether botnet takedowns require court supervision. When the government sets up a sinkhole, it requires a civil forfeiture warrant under 18 U.S.C. § 981(b) to enable it to take over domains being used by the C&C server, and a trap-and-trace order under 18 U.S.C. § 3123 allowing collection of the IP addresses of infected computers making contact.[80] The arguments in this Note do not affect these requirements.

II
Botnet Takedowns as Seizures

A. Legal Principles

If the government uses a sinkhole to remotely disable or clean up a botnet, the result could be a seizure under the Fourth Amendment. Depending on which of the tactics discussed in Part I.B are employed, the operators of the sinkhole may be running code and modifying or deleting files on a private computer without the owner's consent. Even if the government attempts to do something harmless, the mere

---

[76] *See supra* note 33 and accompanying text (describing use of sinkholes to measure botnets).

[77] *See* Sancho & Link, *supra* note 29, at 3 (showing variation in captured botnet requests over time).

[78] *See* Daniel Plohmann et al., Botnets: Detection, Measurement, Disinfection & Defence 55 (2011), *available at* https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/botnets-measurement-detection-disinfection-and-defence (noting inaccuracies in using IP addresses to measure botnet size).

[79] *See* United States v. John Doe 1–13, No. 3:11-CV-561, at 4–5 (D. Conn. Apr. 25, 2011) (granting temporary restraining order); Coreflood Memo, *supra* note 72, at 45–58 (briefing the Fourth Amendment issue).

[80] *See, e.g.*, Coreflood Memo, *supra* note 72, at 3 (describing orders requested from the district court to enable a botnet takedown).

act of pushing commands to hundreds of thousands of machines risks damaging or disrupting at least a few of them.[81] This Part will show that as long as the government targets malware directly during a botnet takedown, seizure doctrine does little to constrain it. However, if the government attempts to patch security holes in the user's software or otherwise modify the user's files, it runs a much greater risk of violating the Fourth Amendment.

The Supreme Court defined seizures in *United States v. Jacobsen*.[82] The *Jacobsen* Court held that the government seizes property within the meaning of the Fourth Amendment when it "meaningful[ly] interferes" with the owner's "possessory interest[ ] in [his or her] property."[83] Importantly, to be a seizure, the law enforcement conduct in question must be willful or intentional.[84] The Fourth Amendment does not protect against "the accidental effects of otherwise lawful government conduct."[85]

Applying seizure doctrine to botnet takedowns presents questions of first impression in the court system. Law enforcement rarely acts remotely on private computers without the owner's consent, and the few cases in which it has done so have not been litigated—in fact, the Coreflood case discussed above appears to be the only instance in which such an effort reached a court.[86] The developing law of computer searches and seizures yields few insights for the botnet problem, since it focuses on the physical seizure of machines, on whether copying data can be a search or seizure, and on the scope of search warrants and the plain view doctrine.[87] As a result, the analysis that follows will extrapolate from the core principles of Fourth Amendment doctrine set forth by the Supreme Court and make analogies to more common situations that arise in the everyday world of policing.

---

[81] *See* Rashid, *supra* note 60 (citing the Electronic Frontier Foundation's concerns that remote botnet cleanup carries some risk of damaging or destroying a computer while trying to fix it).

[82] 466 U.S. 109, 113 (1984).

[83] *Id.*

[84] Brower v. Inyo Cnty., 489 U.S. 593, 596–97 (1989).

[85] *Id.* at 596.

[86] *See* Susan W. Brenner, *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force*, 81 Miss. L.J. 1229, 1231 (2012) (analyzing remote searches and seizures via Trojan horse software as "as yet unexploited" by law enforcement).

[87] Relevant papers in this area include: Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005) (analyzing how the Fourth Amendment applies when the government retrieves evidence from an individual's computer); Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 Miss. L.J. 193 (2005) (surveying Fourth Amendment issues in the electronic context); and Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, 2008 Stan. Tech. L. Rev. 2 (2008) (applying seizure doctrine to personal data).

B. The Possessory Interest

As the FBI argued in its Coreflood filing, a computer owner or user has no possessory interest in the malware infecting her machine.[88] The botnet software was installed illegally without her knowledge, used without her knowledge (most likely to rob her), and can be removed without her knowledge as well. Simply put, the malware is not the computer user's property.[89] It would be as if a criminal defendant, upon learning that the police bugged his office, were to claim a possessory interest in the bug and complain of warrantless seizure of his property when it was removed.

Moreover, malware is an instrumentality of crime. Private citizens cannot have a possessory interest in instrumentalities of crime such as contraband and stolen goods.[90] Although the law of seizures is no longer premised on the state asserting a superior property interest as it was at common law,[91] the seizure of this category of object is presumptively reasonable and does not require a warrant.[92]

---

[88] Coreflood Memo, *supra* note 72, at 48–51.

[89] In the Coreflood case, the FBI compared the owner of an infected computer to the plaintiff in *Shaul v. Cherry Valley-Springfield Cent. Sch. Dist.*, 363 F.3d 177 (2d Cir. 2004). A teacher, Shaul sued over the seizure of his teaching materials. The Second Circuit held that the materials were property of the school district under the work-for-hire doctrine. Despite the fact that Shaul had created the materials and used them regularly, they were not his, and he controlled them only at his employer's sufferance. Because Shaul did not own the materials, he had no possessory interest (outside of that granted by the employer) and no remedy against the seizure. *Id.* at 185–86.

[90] Warden v. Hayden, 387 U.S. 294, 305–06 (1967) (describing suppression of instrumentalities of crime as dependent on a privacy right in the area searched, because there can be no possessory interest in such objects).

[91] *Id.* at 306 n.11.

[92] *See* Payton v. New York, 445 U.S. 573, 586–87 (1980) (noting that it is "well settled that objects such as weapons or contraband found in a public place may be seized by the police without a warrant"). This principle (sometimes known as the open view doctrine) does not permit law enforcement to violate a reasonable expectation of privacy in a constitutionally protected area in order to reach the seizable item, even if the item is clearly visible from outside. *See* Washington v. Chrisman, 455 U.S. 1, 9 (1982) (holding that despite open view of marijuana, seizure was justified only because officer had a separate right to enter dormitory room); Howard E. Wallin, *Plain View Revisited*, 22 PACE L. REV. 307, 326 (2002) ("Since the [open view] doctrine only supplements a prior justified invasion, it does not in and of itself legitimize an intrusion."). In other words, the doctrine excuses lack of a warrant only for the seizure, not for a corresponding search. The question whether efforts to remotely modify or delete malware invade a reasonable expectation of privacy and thus constitute a search is taken up in Part II.B, *infra*. Note that this principle is *not* the same as the plain view doctrine, which allows law enforcement to seize evidence of crimes on probable cause alone, without a warrant. The plain view doctrine applies only when police are lawfully intruding on a reasonable expectation of privacy, typically pursuant to a warrant, and allows seizure of any kind of evidence on probable cause, regardless of whether the owner has a legitimate possessory interest. Wallin, *supra*, at 326.

Computer owners certainly have a possessory interest in both their software and their hardware. However, interventions that modify software (for instance, by patching vulnerabilities) or use hardware resources constitute seizures only if they "meaningfully interfere" with a possessory interest.[93] Meaningful interference involves government conversion of private property, not "mere technical trespass."[94] In *Jacobsen*, meaningful interference was accomplished when DEA agents took "dominion and control" over a package and performed a field drug test that destroyed some of its contents.[95] Similarly, in *Soldal v. Cook County*, the Court held that a seizure had occurred when the government towed away a mobile home.[96] However, when the government doesn't physically take someone's property, the standard for seizure is rarely met unless the owner is deprived of the benefit of her property.[97] For instance, the placement of an electronic tracking device in a can of chemicals was determined not to be a seizure;[98] as was the handling of checked luggage that did not delay the owner or the baggage,[99] and the handling of a package that did not delay its delivery.[100]

A pair of cases helps to illustrate the outer limits of the meaningful interference doctrine: *Porter v. Jewell*[101] and *United States v. Ryan*.[102] In *Porter*, a police officer banged loudly on Porter's door, cracking the doorframe and damaging the deadbolt.[103] The Eleventh Circuit held that because this damage was easily repaired, it was "at most" a de minimis temporary interference with Porter's possessory interest in her door.[104] There was no meaningful interference and therefore no seizure. In *Ryan*, the defendant was a rental car operator who scammed renters out of large sums of money to "replace" wind-

---

93 *E.g.*, United States v. Jacobsen, 466 U.S. 109, 113 (1984) ("A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interest in that property.").

94 United States v. Va Lerie, 424 F.3d 694, 702 (8th Cir. 2005).

95 *Jacobsen*, 466 U.S. at 120.

96 506 U.S. 56, 61 (1992).

97 Examples of this sort of seizure are rare, but they are occasionally litigated. For instance, the Fifth Circuit found a seizure in *Auster Oil & Gas, Inc. v. Stream*, 764 F.2d 381, 389–90 (5th Cir. 1985), when state troopers blocked an oil pipeline, "delaying Auster's transportation and sale of the oil." *Id.* at 385.

98 United States v. Karo, 468 U.S. 705, 712–13 (1984).

99 *Va Lerie*, 424 F.3d at 696; United States v. Gant, 112 F.3d 239, 242 (6th Cir. 1997); United States v. Harvey, 961 F.2d 1361, 1363–64 (8th Cir. 1992); United States v. Lovell, 849 F.2d 910, 916 (5th Cir. 1988).

100 United States v. Quoc Viet Hoang, 486 F.3d 1156, 1162 (9th Cir. 2007).

101 453 F. App'x 934, 937 (11th Cir. 2012).

102 283 F. App'x 479, 481 (9th Cir. 2008).

103 453 F. App'x at 936.

104 *Id.* at 937.

shields with tiny chips in them.[105] Undercover agents rented cars from the defendant, intentionally chipped the windshields, and then paid Ryan's fee to help build the case against him.[106] The Ninth Circuit held that chipping the windshield was only a de minimis interference.[107]

If the events in *Porter* and *Ryan* do not constitute meaningful interference, it is hard to see how patching computer software could meet the standard. Those cases concerned physical *damage* to private property. Patching, by contrast, is a repair that makes software function better—the only thing the user loses is a security vulnerability. However, meaningful interference may still occur if the patch (presumably created by the software's original designer) does more than just remove a vulnerability. If the patch is part of a larger update to the software that changes its features, interface, or compatibility with other programs, then the fix has the potential to directly interfere with the user's enjoyment of her computer.[108] Under those circumstances, patching security vulnerabilities without user consent could be a seizure within the meaning of the Fourth Amendment.

Given the limits of seizure case law, tort law provides a helpful point of comparison in considering how "meaningful interference" should apply online. In civil cases, courts have had several decades to engage with the problem of when electronic communications interfere with property rights enough to give rise to liability. The tort of trespass to chattels contains a variant of the "meaningful interference" standard of seizure law: To bring a claim, the plaintiff must show damages, dispossession, or deprivation of use for a substantial time.[109]

---

[105] 283 F. App'x at 480.

[106] *Id.* at 481.

[107] *Ryan* is complicated by the fact that the Ninth Circuit took notice of the payment Ryan received from the agents. The language in the case is ambiguous and can be read to support the proposition that there was no meaningful interference with Ryan's property only because he had already been compensated for the damage. *See id.* ("[T]he interference, considering that the damage was paid for many times over, was minimal."). However, even under this reading, remotely uninstalling malware or patching software would not be a seizure, because these actions do not inflict damage on property (hardware, software, or data).

[108] *See, e.g.*, Brad Chacos, *Patch Tuesday Disaster Breaks Office 2013 for Thousands; Here's How to Fix It*, PCWORLD (June 16, 2014, 8:47 AM), http://www.pcworld.com/article/2363784/patch-tuesday-disaster-breaks-office-2013-for-thousands-heres-how-to-fix-it.html (describing a Microsoft Office patch that prevented approximately 44,000 users from running Office programs); Renai LeMay, *Disastrous Patch Cripples CommBank*, DELIMITER (July 30, 2012, 1:00 PM), http://delimiter.com.au/2012/07/30/disastrous-patch-cripples-commbank/ (telling story of a Microsoft Windows patch that rendered more than 9000 computers temporarily unusable at the Commonwealth Bank of Australia).

[109] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 218 (1965) (describing the prerequisites to liability for trespass to chattels).

Although some early cases involving "cybertrespass" seemed to recognize a broad right to exclude unwanted electronic communications, the doctrine today requires plaintiffs to show damage or impairment to the affected computer.[110] The most analogous cases are those in which plaintiffs sued defendants for running code on their electronic devices without their consent. In *Sotelo v. DirectRevenue, LLC*, defendants installed spyware that slowed down plaintiffs' computers, ate up their bandwidth, and covered their screens in pop-ups—enough impairment to sustain an action for trespass to chattels.[111] At the other end of the spectrum, iPhone owners sued Apple for trespass to chattels over iPhone apps that secretly collected users' geolocation data.[112] The plaintiffs alleged that transmitting and storing geolocation data used up memory, bandwidth, and battery life on their phones.[113] The Northern District of California dismissed the case, holding that while the "allegations conceivably constitute a harm, they do not plausibly establish a significant reduction in service constituting an interference with the intended functioning of the system, which is

---

[110] *See* 1 DATA SECURITY & PRIVACY LAW § 8:11 (2014) ("[I]n cases where no or only negligible harm or damage is shown to the chattel (as opposed to infringement of the plaintiff's exclusive right to use that chattel), the court may find that the necessary elements for a claim of trespass to chattels have not been met."). *Compare* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1017, 1022 (S.D. Ohio 1997) (holding that spam emails trespassed on defendant's computers despite lack of evidence of physical damage, loss of functionality, or system downtime), *with* Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1347 (2003) (holding that unwanted emails were not trespass to chattels because Intel presented no evidence of damage or disruption to its computer systems). Some courts remain willing to find a trespass to chattels where damage has not actually occurred, but *could* occur if enough people replicated the trespass at the same time. *See* Kevin Emerson Collins, *Cybertrespass and Trespass to Documents*, 54 CLEV. ST. L. REV. 41, 55–61 (2006) (discussing potential versus actual harm to computer systems and examining cases). In *Register.com, Inc. v. Verio, Inc.*, the defendant used automated queries to find newly registered websites so it could send the website owners marketing materials. 356 F.3d 393, 396 (2d. Cir. 2004). The district court found (and the Second Circuit agreed) that trespass to chattels had occurred—not because Verio's queries caused any damage, but because if Verio won the case, more companies would begin sending similar queries. *Id.* at 404–05. The aggregate of queries from an unknown number of companies could eventually overtax and crash Register.com's servers. *Id.* However, these cases are easily distinguished from the botnet situation for three reasons. First, there is no reason for large numbers of people to try to remotely end a single botnet infection at once. Second, it would be technically infeasible—remotely uninstalling the botnet requires first seizing control of it, an arduous process that often entails a court order. *See supra* Part I.B. Third, the CFAA makes it illegal for private actors to use these tactics, suggesting that overuse to the point of damage is unlikely. *See supra* Part I.C.

[111] Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219, 1230–31 (N.D. Ill. 2005).

[112] *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1069 (N.D. Cal. 2012); *see also In re* Google Android Consumer Privacy Litig., No. 11-MD-02264, 2013 WL 1283236, at *13 (N.D. Cal. Mar. 26, 2013) (rejecting a similar suit against Google on the same grounds).

[113] *In re* iPhone Application Litig., 844 F. Supp. 2d at 1069.

necessary to establish a cause of action for trespass."[114] These cases make clear that unless a botnet cleanup interferes with the normal functions of a private computer in a nontrivial way, it will not be considered a trespass to chattels. In fact, after malware is shut down or uninstalled, the host computer may well run *better* than it did before.[115]

Government use of remote commands to clean up a botnet is unlikely to trigger the Fourth Amendment's restrictions on seizures. If the government's commands modify malware behavior, disrupt it, shut it off, or even delete it, there will not be an unconstitutional seizure because the computer's owner has no possessory interest in the malware.[116] This suggests that in theory, the government could even patch security vulnerabilities in legitimate software as part of botnet cleanup, on the grounds that a patch does not meaningfully interfere with the owner's possessory interest in the software. However, the government is not free to propagate patches that change the user experience or create compatibility problems with other programs or files, since those could potentially produce meaningful interference and thus constitute a seizure.

C. Probabilistic Harms and Unintentional Seizures

The problem of incompatibility that remote patching creates is a small piece of a larger problem. Even the best-designed and best-tested software inevitably creates problems for some consumers when it is installed en masse on thousands or hundreds of thousands of machines.[117] This is especially problematic in the botnet cleanup con-

---

114 *Id.*

115 *See, e.g.*, *Bots and Botnets—A Growing Threat*, NORTON, http://us.norton.com/botnet/promo (last visited Feb. 9, 2015) (noting that botnet malware can cause computers to "slow down, display mysterious messages, or even crash").

116 This principle may be generalizable to other kinds of digital contraband like child pornography. In theory, the FBI could use a sinkhole to remotely delete such files (assuming they could be distinguished from legitimate materials, which largely rules out pirated media or software), without implicating the Fourth Amendment's regulation of seizures. There are two caveats, however. First, if the FBI attempted to delete the contraband and accidentally disrupted or damaged legitimate files or software, they would be committing a seizure. Unlike malware, contraband belongs to the computer user, which would prevent the government from deploying the unintentional seizure argument developed in Part II.C, *infra*. Second, unlike malware, most other contraband on private hard drives doesn't make its presence known on the Internet unless the owner is actively sharing it. If the FBI wanted to obtain evidence that such contraband existed on a particular computer (a prerequisite for any prosecution), it would be conducting a search. *See infra* Part III.B (noting that botnet cleanups do not qualify as searches if no information is sent back from the computer to the authorities).

117 *See* Rashid, *supra* note 60 (discussing the extent of the FBI's Coreflood effort and mentioning the risks to target machines).

text. Although the commands the government would run as part of a botnet cleanup are far simpler than a typical piece of consumer software, it would likely receive much less testing than a typical commercial program and would have to work through the unreliable intermediary of botnet malware. Given the sheer number of computers that make up many botnets, even a carefully planned cleanup operation could well cause damage or disruption to a few individual computers.[118]

The risk of damage alone, however, is not enough. The government does not seize any computers within the meaning of the Fourth Amendment if it pushes commands to all of the computers in a botnet, as long as those commands are not *intended* to meaningfully interfere with the possessory interests of computer owners or users. This is true even if the government knows that some small percentage of those computers will likely be damaged as a side effect of running the commands.

In *Brower v. County of Inyo*, the Supreme Court established that a seizure entails intentional acquisition of control by the government, not merely the unintended consequences of government actions.[119] In other words, "the detention or taking itself must be willful."[120] This is not to say that a chain of events must unfold precisely as the government envisioned in order for courts to find a seizure. In *Brower*, police set out a roadblock to stop a suspect, who was driving a stolen car.[121] The suspect crashed into the roadblock and died.[122] The police protested that they merely intended to force the suspect to stop, not to make him crash—but the Court explained that it was "enough for a seizure that a person be stopped by the very instrumentality set in motion or put in place in order to achieve that result."[123] Similarly, in *Nelson v. City of Davis*, a seizure occurred when police shot a student in the eye with a pellet filled with pepper spray, even though they had intended the pellet to burst over the heads of Nelson and his friends.[124] The court reasoned that because the use of force was intentional and aimed at a group of people including Nelson, whatever harm resulted to Nelson was intentional, too. In *Fisher v. City of Memphis*, a police officer fired at a car driving towards him, hitting

118 *Id.*

119 489 U.S. 593, 596–97 (1989).

120 *Id.* at 596.

121 *Id.* at 594.

122 *Id.*

123 *Id.* at 599.

124 685 F.3d 867, 872 (9th Cir. 2012).

and injuring a passenger.[125] The Sixth Circuit held the use of force intentional, since the officer had intended to stop the car by shooting at the driver, "effectively seizing everyone inside, including the [passenger]."[126] Thus, groups of people or objects can sometimes be aggregated for purposes of evaluating whether police intentionally used force against them.

One could argue that courts should treat an infected computer, malware and all, as a single unit just like the car and passenger in *Fisher*. If the FBI targets a part of the whole, the Bureau should be responsible for whatever results. However, computers and malware cannot be aggregated in this way because the computer is innocent, while the malware is being used for criminal activity. Consider *Childress v. City of Arapaho*.[127] On the surface, the facts of *Childress* are identical to *Fisher*: Cops fired on a moving vehicle to stop it, accidentally striking a passenger.[128] But, unlike in *Fisher*, the passenger shot in *Childress* was a hostage.[129] The *Childress* court recognized that although police intended to seize the criminals controlling the car, they intended to free the hostage, and the resulting injuries were therefore not intentional.[130] Nor is *Childress* an outlier. In addition to the Tenth Circuit, the First, Second, Fourth, Sixth, and Seventh Circuits have all confronted cases where police use of force directed at criminals has accidentally injured hostages or bystanders, and all have concluded that no seizure occurred because the force was not deliberately aimed at the victim.[131]

---

[125] 234 F.3d 312, 315 (6th Cir. 2000).

[126] *Id.* at 318–19.

[127] 210 F.3d 1154 (10th Cir. 2000).

[128] *Id.* at 1155–56.

[129] *Id.*

[130] *Id.* at 1157.

[131] *See* Milstead v. Kibler, 243 F.3d 157, 163–64 (4th Cir. 2001), *abrogated on other grounds by* Pearson v. Callahan, 555 U.S. 223, 235 (2009) ("Under the first form of mistake, where the seizure is directed appropriately at the suspect but inadvertently injures an innocent person, the innocent victim's injury or death is not a seizure that implicates the Fourth Amendment because the means of the seizure were not deliberately applied to the victim."); Claybrook v. Birchwell, 199 F.3d 350, 354, 359 (6th Cir. 2000) (no seizure when stray bullet shot bystander during a police gunfight); Schaefer v. Goch, 153 F.3d 793, 796–97 (7th Cir. 1998) (no seizure when police officer shot at suspect and hit hostage); Medeiros v. O'Connell, 150 F.3d 164, 169 (2d Cir. 1998) (same); Rucker v. Harford Cnty. 946 F.2d 278, 281 (4th Cir. 1991) (no seizure when police officer fired gun at fleeing suspect and hit innocent bystander); Landol-Rivera v. Cruz Cosme, 906 F.2d 791, 795 (1st Cir. 1990) (no seizure when police officer shot at suspect and hit hostage). This rule does not apply to situations where the police shoot a victim under the mistaken belief that they are the perpetrator. *See, e.g.*, *Medeiros*, 150 F.3d at 169. However, that caveat is irrelevant to the arguments in this Note.

A computer user whose machine is damaged or disrupted as a side effect of FBI botnet cleanup efforts is analogous to an innocent bystander or a hostage. If the intention of the cleanup is to help the computer owner, then the owner is akin to a hostage. If the intention is to help third parties by destroying the botnet, then the owner is like an innocent bystander. In both situations, however, the application of the intent rule is clear. Law enforcement use of force aimed at the perpetrator of a crime is not an intentional seizure when it accidentally harms innocent parties—even when the risks are clearly present, as they nearly always are in violent confrontations with the police. Remote cleanup efforts will therefore not be seizures unless they are risky to the point that the FBI could be said to willfully or intentionally disrupt victims' computers.[132]

It might seem that if the FBI is aware of a measurable risk and decides to take that risk many times (as it does when cleaning up a botnet on hundreds of thousands of computers), then the law of large numbers means that the FBI knowingly causes the harm to come to pass. However, the Fourth Amendment's protection is an individual right, not a collective one.[133] If an aggrieved citizen goes to court, she must say, "the government seized my computer." When the FBI responds that it did not act intentionally *towards her*, it is no answer to say that the agency knew it was highly probable that something would go wrong somewhere. The FBI simply created a risk for her. That risk might be enough to support a negligence claim in another context, but mere negligence is not sufficient for a seizure claim.[134] Return for a moment to the analogy of the hostage injured in a shootout. The police have policies and training on when the use of lethal force is appropriate. In developing these policies and allowing officers to open fire in hostage situations, the government must realize that if these policies are followed in enough situations, a hostage will eventually be shot. Nonetheless, despite this probabilistic certainty, we know from the cases that the shooting of a hostage is not an intentional seizure. The same holds true of decisions about acceptable risk level in remote botnet cleanup.

---

[132] Negligence is insufficient to support a seizure. *See* Ansley v. Heinrich, 925 F.2d 1339, 1344 (11th Cir. 1991) ("[N]egligent conduct alone . . . [cannot] form the basis of a section 1983 claim premised on the fourth amendment."). Whether something less than intentional law enforcement conduct (like grossly negligent or reckless disregard for a risk) could be "willful" as the term was used in *Brower* remains unclear. *See* Morrill v. Prince George's Cnty., 103 F.3d 119, 122 n.6 (4th Cir. 1996) (noting the uncertainty in lower courts' understanding of *Brower*'s intent standard).

[133] *See* Rakas v. Illinois, 439 U.S. 128, 133 (1978) ("Fourth Amendment rights are personal rights that may not be asserted vicariously . . . .").

[134] *See Ansley*, 925 F.2d at 1344.

Any effort to do mass botnet cleanup by pushing commands to infected machines through a sinkhole carries at least a small risk of damage to some computers. This holds true whether the FBI is merely trying to alert users and request consent for further activities or actively deleting malware from users' hard drives. However, unless this risk is so great that the FBI can be said to be intentionally or willfully interfering with a computer, there can be no seizure.

The danger of a seizure is much greater if the FBI is attempting to remotely patch security flaws on infected computers en masse. This is because the government would be intentionally modifying files and programs in which the computer's users have legitimate possessory interests. Since the government is intentionally targeting legitimate software with its virtual use of force, if something went wrong—if, for instance, the patch stopped the program from working properly or made it incompatible with other programs on the computer—those unexpected consequences would still be considered intentional under *Nelson* and *Fisher*. Therefore, to avoid potential Fourth Amendment violations, the FBI should avoid remote patching unless it is certain the fix is completely harmless.

III
Botnet Takedowns as Searches

A. Legal Principles

One of the most powerful methods for cleaning up botnets is remotely deleting malware from infected computers. Unless the malware has some kind of uninstall functionality built in, however, the government would have to tell the computer exactly which files it is supposed to remove. To accomplish this, the government could use a sinkhole to send commands to infected computers through the malware. The commands would instruct the machines to search their hard drives for the botnet malware and delete it. This method can also be used to find and remove other malware on the hard drive, such as a dropper that could reinfect the computer.[135] In colloquial terms, using such techniques would mean that the hard drive has been searched. But has the government performed a search within the meaning of the Constitution? This Part will argue that sending and executing remote commands on private computers in the course of botnet cleanup is not a Fourth Amendment search as long as no information is returned to the government.

[135] *See supra* notes 41–42 and accompanying text (describing the cleanup of malware).

The government performs a search when it invades an individual's reasonable expectation of privacy,[136] or when it gathers information—private or not—by physically intruding on an individual's property.[137] In the physical world, these two theories (often overlapping) regulate government intrusions into private spaces. Entering a home or opening a package are archetypal examples of physical searches that generally cannot be performed without a warrant.[138] Such intrusions violate reasonable expectations of privacy both because the object of the search is private, and because the act of searching exposes a private space to the public eye.[139] The law deems some spaces to be more private than others. With respect to the home, the Supreme Court has said that "all details are intimate details"—a search occurs even if an officer goes only a few inches beyond the threshold.[140] Once an officer is lawfully present in a private place, however, the law accepts that they will gather information with their senses. The plain view doctrine permits a police officer in such circumstances to seize incriminating evidence and report anything they see in court.[141]

Searches of computers create difficulties for this physical-world paradigm.[142] Computer searches are typically litigated in the context of digital forensics. Instead of opening and entering a private space or container, as it does in the physical world, the government seizes a computer, creates a perfect copy of the hard drive, and then scans the copy for evidence.[143] To be sure, people can have a reasonable expectation of privacy in the contents of their hard drives.[144] If the govern-

---

136 *See* Katz v. United States, 389 U.S. 347 (1967) (establishing the tie between Fourth Amendment protections and citizen expectations).

137 *See* United States v. Jones, 132 S. Ct. 945, 952 (2012) (noting that the *Katz* reasonable expectation of privacy test did not supplant the physical trespass test); *see also* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) (use of a drug-sniffing dog, which is not a search under *Katz*, was a search when the dog trespassed in the curtilage of a home).

138 *See* Kerr, *supra* note 87, at 549 (summarizing Supreme Court doctrine defining searches).

139 *See* United States v. Place, 462 U.S. 696, 708–09 (1983) (explaining the privacy-invading elements of ordinary searches that are not present during dog sniffs).

140 Kyllo v. United States, 533 U.S. 27, 37 (2001).

141 *See, e.g.*, Minnesota v. Dickerson, 508 U.S. 366, 374–75 (1993) (describing the plain view doctrine).

142 *See* Kerr, *supra* note 87, at 538 (discussing how digital searches differ from physical searches because of the environment they take place in, the copying process, the storage mechanism, and the retrieval mechanism).

143 *Id.* at 540–41.

144 *See, e.g.*, United States v. Ziegler, 474 F.3d 1184, 1189–91 (9th Cir. 2007) (stating that the defendant had a reasonable expectation of privacy in computer located in his personal office); Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) (stating that searching personal computer required consent from someone with access and control); United States v. Barth, 26 F. Supp. 2d 929, 937 (W.D. Tex. 1998) (explaining that the warrantless search of

ment retrieves information from a private hard drive, it has performed a search. But when did the search take place? Professor Orin Kerr offers an exposure-based theory: A search occurs when data is exposed to human eyes.[145] Professor Jonathan Zittrain critiques this conception of search by turning from forensic analysis of individual computers to mass data collection like that performed by the NSA.[146] Zittrain argues that a search occurs the moment information is collected, triggering judicial regulation of searches at an earlier point in the process of government information gathering.[147] Zittrain argues that if the government is allowed to collect vast amounts of data unsupervised, it becomes difficult for neutral magistrates to effectively monitor how the government uses that data.[148]

B. The Information Gathering Requirement

To clean up a botnet, the government must use a sinkhole to send commands out to be run on infected computers, but the government need not receive any information back. The central question in a search analysis of botnet cleanup, then, is whether running commands on a computer can ever be a search if no information is collected. The best answer to this question is no. Although that response may sound like an endorsement of Professor Kerr's position, in fact both sides of the exposure debate assume that there is some collection of information. Zittrain would find a Fourth Amendment search when the FBI copies a hard drive or the NSA records online traffic, even if no human has yet looked at the data. But what if no data comes into the possession of law enforcement at all? Is a digital intrusion a search if no information is gathered? This question has not been litigated in the lower courts, which is unsurprising. Because intrusions in the physical world are carried out by people who gather information with their senses, a search that gathers no information can exist only in the digital context. Even in that context, botnet cleanups are unusual. The

defendant's hard drive violated the Fourth Amendment); Brenner, *supra* note 86, at 1239 (arguing that people have a reasonable expectation of privacy in hard drives because hard drives are closed containers).

145 Kerr, *supra* note 87, at 547–48; *see also* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 581 (2011) ("[I]ndividuals whose information is exposed only to automated systems incur no cognizable loss of privacy.").

146 Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83, 83–84 (2005).

147 *Id.* at 84 ("The acts of intruding upon a suspect's demesnes or compelling cooperation from a third party are natural triggers for judicial process or public objection.").

148 *See id.* (describing the Fourth Amendment's reliance on monitoring by "disinterested magistrates").

law of computer search and seizure developed in the context of forensic computer work that was clearly intended to gather evidence.[149] Given the lack of case law that fits the scenario we are analyzing, we therefore turn, as would a court of first impression, to principles articulated by the Supreme Court.

In *United States v. Place*, the Court held that no search occurred when a drug-detecting dog sniffed luggage at an airport.[150] The Court reached this conclusion for two reasons. First, the search did not intrude on the defendant's privacy through its method: The sniff did not require opening up the luggage and exposing its private contents to the world.[151] Second, the search did not intrude on the defendant's privacy through its results.[152] The sniff only identified the presence or absence of illegal drugs, and there can be no reasonable expectation of privacy in contraband.[153] The Court said the dog sniff was "sui generis" because it was the only investigative technique "so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure," and was therefore not a search.[154] In doing so, the Court implicitly argued that intrusion on a reasonable expectation of privacy necessarily involves revealing private information.

The Court made this reasoning more explicit in *United States v. Karo*.[155] In *Karo*, government agents planted a radio-tracking device without a warrant in a drum of chemicals that they then gave to the defendant.[156] The Tenth Circuit had held that transferring the can to Karo violated his reasonable expectation of privacy because it could be used to monitor him anywhere, even inside a private residence.[157] The Court disagreed. Instead, it ruled that giving Karo the can with the tracking device (as opposed to turning the device on) could not violate a privacy interest: "It conveyed no information that Karo wished to keep private, for it conveyed no information at all."[158] There may have been ways the government could have employed the tracking device to learn private information about Karo, but the Court

---

149 *See supra* note 87 and accompanying text (citing sources detailing the development of Fourth Amendment doctrine in the computer context).

150 462 U.S. 696, 707 (1983).

151 *Id.*

152 *Id.*

153 *Id.*

154 *Id.*

155 468 U.S. 705 (1984); *see also* Kerr, *supra* note 87, at 553 (arguing that *Karo* supports the exposure theory of search).

156 468 U.S. at 708–10.

157 *Id.* at 712.

158 *Id.*

explained that *potential* invasions of privacy did not constitute searches.[159]

The Court again defined searches in terms of gathering information in *Kyllo v. United States*.[160] *Kyllo* concerned warrantless use of a thermal camera to observe a home from a public street.[161] The Court rejected the argument that no search took place because the thermal camera merely picked up infrared radiation outside of the house.[162] Instead of focusing on physicality, it held that a search occurred when the government "obtain[ed] 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," at least when that technology was not in widespread public use.[163]

C. Electronic Trespass and United States v. Jones

Thus far I have argued that sending commands to infected computers without gathering information is less invasive than traditional computer forensics. However, there is one sense in which it is far more intrusive. Computer forensics, as discussed above, involves making a copy of a seized hard drive and then analyzing the copy.[164] The purpose of this procedure is to ensure that the original hard drive remains completely unchanged for evidentiary purposes.[165] By contrast, remote botnet cleanup involves actually running commands on a private computer, using its processing power, and scanning and modifying files on its hard drive. To locate hidden malware, the FBI might send code to index every file on a hard drive and produce a list of hash values corresponding to their contents.[166] The FBI could also send a table of hash values of known malware for comparison. Their program

---

159 *Id.*

160 533 U.S. 27, 34 (2001).

161 *Id.* at 29–31.

162 *Id.* at 34.

163 *Id.* at 40 (internal citation and quotation marks omitted).

164 *See* Kerr, *supra* note 87, at 540–42 (describing the process of seizing, copying, and analyzing a hard drive).

165 *See id.*

166 A hash function is an algorithm that takes in data (like a computer file) and, without processing the semantic meaning of that data, creates a string of alphanumeric characters called the hash value that corresponds to the file's pattern of zeroes and ones. The resulting hash value has two important properties. First, it is impossible to learn anything about the original file by looking at the hash. Second, it is virtually impossible for two inputs to produce the same hash value. Even tiny changes between original files will produce very different hashes. A hash value is therefore like a digital file's fingerprint—except many times more accurate than its biological analog. *See* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 38 (2005) (exploring the Fourth Amendment implications of hashing).

would compare the two sets of hash values; where it found a match (thus identifying a malicious file), it would delete the file.

This intuition—that the Fourth Amendment is implicated when the government runs a program on a private computer—is best analyzed under Justice Scalia's opinion in *United States v. Jones*.[167] In *Jones*, the Supreme Court held that a search took place when the government attached a GPS tracking device to the defendant's car.[168] A majority held that when the government trespasses on private property, it can perform a search even where there is no reasonable expectation of privacy.[169] Although it is unclear whether Justice Scalia thought the trespass rule of *Jones* could ever apply in the electronic context,[170] lower courts have at least left open the possibility that the case prohibits remote government intrusion on private computers.[171]

However, Justice Scalia articulated the rule of *Jones* as applying to physical intrusion or trespass on a constitutionally protected area *for the purpose of gathering information*.[172] If the government tres-

---

[167] 132 S. Ct. 932 (2012).

[168] *Id.* at 950.

[169] *Id.* at 949–53.

[170] The opinion distinguishes between physical intrusions, which trigger *Jones*, and "[s]ituations involving merely the transmission of electronic signals without trespass," which are analyzed solely under *Katz*. *Id.* at 953. That language presumably refers to situations where outgoing signals are intercepted, like a wiretap, and does not necessarily rule out remote intrusions on a private computer.

[171] The most relevant lower court cases are ones in which the government downloads child pornography from the defendant's computer that the defendant made publicly available via a peer-to-peer file sharing program. In *United States v. Brooks*, the district court held that the government did not "physically intrude on any of Brooks' [sic] constitutionally protected areas" for two reasons. No. 12-CR-166, 2012 WL 6562947, at *5 (E.D.N.Y. Dec. 17, 2012). First, "[t]he agent did not install any device or software on Brooks' computer[,] . . . did not physically enter Brooks' home, and did not physically access his computer." *Id.* Second, the agent did not "remotely access any of Brooks' computer files until after Brooks granted him access, and only then did the agent access those specific files which Brooks had designated for the agent to see." *Id.* In other words, the court contemplated that remote installation of software on Brooks's computer, or remote access without permission to files stored on the computer, could be an intrusion within the meaning of *Jones*. Similarly (though less articulately), the court in *Russell v. United States* found "no government trespass into Russell's home or effects" not because remote searches never implicate *Jones*, but because the defendant's file sharing program "broadcast the contents of his computer . . . and invited users to search those contents." 4:11 CV 1104, 2013 WL 5651358, at *8 (E.D. Mo. Oct. 16, 2013). The government made a similar argument in *United States v. Saville*, in which an agent used special software to find the physical location of a computer sharing child pornography on a public network. CR 12-02-BU-DLC, 2013 WL 3270411 (D. Mont. June 21, 2013). It argued that the court should reject the defendant's *Jones* claim because "the two surveillance devices only monitored information on the wireless network and did not actually intrude on his computer." *Id.* at *5.

[172] 132 S. Ct. at 949 ("The Government physically occupied private property for the purpose of obtaining information."); *id*. at 951 (stating the trespass principle as "when the

passes with no intent to obtain information, and no information is in fact gathered, there may be a Fourth Amendment seizure, but there is no search under *Jones*. In fact, if this were *not* the case, the law of searches would instantly consume the law of seizures. There would never be a question whether police "meaningfully interfered" with private property. If they so much as touched it—even if that touch were a bullet impact or a hammer chipping a windshield—there would be a search.[173] We should not interpret *Jones* to have overruled *Jacobsen* and its progeny without so much as a footnote about the implications.

The NSA's use of botnets provides a helpful point of comparison. Leaked documents show that the NSA "hijacks" criminal botnets and has used them to install spyware on more than 140,000 infected computers.[174] If *Karo* applies to this activity, no search would take place until the NSA actually activated the spyware to collect data. However, if *Jones* can apply to electronic communications, then the act of installing spyware on a private computer—like the act of installing a GPS device on a car—is a trespass for the purpose of gathering information, which triggers the Fourth Amendment.

If the government uses remote commands to clean malware from infected computers, it does not necessarily perform a search under the Fourth Amendment. This is true even if the commands it sends instruct the computer to search its hard drive for malware or software with security vulnerabilities. However, a search will take place if the remote commands gather any information from infected computers and relay it back to law enforcement—even something as simple as whether the remote commands have run successfully.[175] This does not mean, however, that the government can have no idea whether their efforts to clean up the botnet have been successful or not. As in the

---

Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment" (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring)).

[173] Note that while the "meaningful interference" standard of seizure law echoes the exclusion of mere "technical trespass" from trespass to chattels, *Jones* applies the lower trespass standard of real property even to chattels like cars. *See Jones*, 132 S. Ct. at 949 ("[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all . . . ." (quoting Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.) 817)).

[174] *See* Joseph Menn, *NSA 'Hijacked' Criminal Botnets to Install Spyware*, REUTERS (Mar. 12, 2014, 5:05 PM), www.reuters.com/article/2014/03/12/us-usa-security-nsa-botnets-idUSBREA2B21420140312 (describing the NSA program).

[175] This is particularly true under the *Jones* trespass rationale, where any gathering of information becomes a search when coupled with a physical intrusion, even if the information gathering would not normally be a search on its own. *See* Florida v. Jardines, 133 S. Ct. 1409, 1417–18 (2013) (holding that a drug dog sniff was a search where the dog trespassed on the curtilage of a home).

Coreflood case, the government can measure the number of botnets phoning in to their sinkhole before and after sending cleanup commands. Law enforcement remains free to monitor the overall size and health of the botnet in this manner. Retrieving information from individual infected machines, however, will constitute a search.

Conclusion

Once the government has successfully sinkholed a botnet, it can use the sinkhole to remotely control infected computers. This Note has shown that the government can exploit that control to dismantle the botnet without implicating the Fourth Amendment's regulation of searches and seizures. Sending commands that target malware without a warrant is not an unconstitutional seizure because computer owners have no possessory interest in malware. Nor will running those commands on an infected machine be a search, as long as they relay no information back to law enforcement. Although using remote commands on tens or hundreds of thousands of computers always carries some risk of collateral damage, this will not be a seizure either, because any disruption computer owners face will not be the intentional result of government action.

Despite this lacuna in Fourth Amendment protection, the Amendment still provides important limits on what the government can do in this arena. First, if law enforcement targets a user's files or software, the agency risks seizing them in the eyes of the Constitution. If the government patches or updates legitimate software in ways that impair their owner's enjoyment, they seize the software if the impairment rises to the level of "material interference." And once remote commands intentionally target legitimate files in which computer users have possessory interests, collateral damage to the files or to the computer will be an intentional seizure. As a result, the Constitution provides protection against the government tampering with or modifying private files and software. Furthermore, although law enforcement can delete malware remotely without conducting a Fourth Amendment search, it cannot gather information. Once information goes back to the government from an individual infected computer, the government has searched: It has invaded the owner's reasonable expectation of privacy in her hard drive, and perhaps even gathered information through an electronic trespass on private property. Either way, without a warrant or applicable exception, such behavior is presumptively unreasonable and violates the Constitution. Finally, whether the Fourth Amendment applies to use of remote commands or not, law enforcement will never be able to execute a botnet take-

down without supervision. The need for court orders to seize domain names and to record IP addresses ensures that courts will remain active participants in the takedown process.

This Note is not intended as an argument for expanded police power. Instead, it has endeavored to examine how the various pieces of Fourth Amendment doctrine fit together in an unusual context—albeit one that has important real-world consequences. There remains something uncomfortable about the idea that in some situations the government can delete files from our private hard drives without the Fourth Amendment having anything to say about it. That sense of intrusion as a privacy harm is reflected in *Jones*, of course, but *Jones* was designed for the physical world, and not for the problems of electronic systems connected through the Internet. And no court has fully grappled with intrusion as a privacy harm in an electronic context, where it can be separated from information gathering. Although the judiciary has begun the project of reshaping Fourth Amendment law to accommodate twenty-first-century technology, that effort is by no means finished. As more cases arise and work their way through the court system, the role of the Fourth Amendment (and thus the government) in botnet takedowns will be open to change.