NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 18, ISSUE ON.: APRIL 2017

TRACKING CRIMINALS WITH INTERNET PROTOCOL ADDRESSES: IS LAW ENFORCEMENT CORRECTLY IDENTIFYING PERPETRATORS?

Erin Larson*

Technology's ever-changing pace has left law enforcement officials with the job of finding legal ways to investigate and search suspected criminal activity. The advent of the Internet has left these officials with a challenging landscape to navigate regarding what is considered a search and what constitutes probable cause to obtain a search warrant based on a suspect's online activity. As seen in various high-profile crimes, the technology-savvy individual can easily disguise and misdirect the IP addresses they use, notably when trying to hide illegal activity. This Recent Development argues that law enforcement must tread carefully when using Internet Protocol ("IP") addresses to obtain search warrants for suspected criminal activity because of the inherently unreliable information these addresses provide.

---

* J.D. Candidate, University of North Carolina School of Law, 2018. The author would like to thank the NC JOLT staff and editors for their feedback and encouragement, particularly Elizabeth Falconer, Shannon O'Neil, Sam Helton, and Caroline Poma.

I. INTRODUCTION

An IP address is analogous to a phone number in that both serve as a unique identifier for a particular device.[1] Similar to how a phone number is assigned to a telephone device, an IP address is assigned to a specific computer.[2] Furthermore, each router that a device uses to connect to the Internet also has an IP address assigned by the Internet Service Provider ("ISP"), comparable to how a phone number is assigned by the phone provider.[3] Just as a

---

[1] Cale Guthrie Weissman, *What Is an IP Address and What Can It Reveal About You?,* BUSINESS INSIDER: TECH INSIDER (May 18, 2015, 4:45 PM), http://www.businessinsider.com/ip-address-what-they-can-reveal-about-you-2015-5.

[2] Weissman, *supra* note 1; *see also What is Network Address Translation,* WHATISMYIPADDRESS.COM, http://whatismyipaddress.com/nat (last visited Jan. 17, 2017) (explaining that matters become complicated when users connect all of their devices, such as home computers, cell phones, and iPads, to a single IP address).

[3] Weissman, *supra* note 1. The IP address of a router is assigned by the Internet Service Provider (ISP) who manufactured the router (for example, Comcast or AT&T). It is difficult to identify the IP address for an individual's computer by looking at Internet usage; rather, the IP address an investigator would likely locate first is that of the router, which is assigned by an ISP. *Id.*

person would dial a given number to reach a specific individual, the assigned IP address allows various devices connected to the Internet to "talk" to each other so that data can be shared among them.[4] Each time a user visits a website, the website logs their IP address.[5] With this information, the website can keep a record of who visits the site via tracking the IP addresses that accessed the site, similar to how phone companies keep a log of their users' calls.[6]

An IP address can be obtained easily, and various websites offer free services to track down a desired address.[7] Finding a specific *user's* IP address, however, can be more difficult and is complicated by factors such as whether the IP address is static or dynamic[8] and whether the user was on an unsecured or secured network.[9] The ISP supplies their customers with a router and the

---

[4] Weissman, *supra* note 1.

[5] R. Kayne, *Do Websites Track and Record IP Addresses?,* WISEGEEK, http://www.wisegeek.org/do-websites-track-and-record-ip-addresses.htm (last modified Jan. 20, 2017). A website's server sends the computer's browser an IP address when it "accepts" the request from the user's computer. When the page loads, the website often records the IP address that loads the webpage. Websites often choose to keep a log of the IP addresses that access their site for analytical purposes. *Id.*

[6] Kayne, *supra* note 5.

[7] *See* Amandine Markham, *How to Trace an IP Address,* WIKIHOW: INTERNET SECURITY (March 2, 2015), http://www.wikihow.com/Trace-an-IP-Address ("[t]racing an IP address is fairly simple").

[8] There are two types of IP addresses: static and dynamic. Most ISPs have moved to assigning dynamic IP addresses to their networks, which assign the number only when users connect to the Internet, meaning the addresses change over time. Alternatively, static IP addresses never change, and these are less common among users. *See Static vs. Dynamic IP Addresses,* GOOGLE, https://support.google.com/fiber/answer/3547208?hl=en (last visited Jan. 13, 2017).

[9] There are secured and unsecured networks. Anyone can access an unsecured network because the network has no protections in place to limit access, for example a Wi-Fi connection that requires no password. Also, because more IP addresses are dynamic now, everyone who logs on the Internet at the local coffee shop could potentially have the same IP address. *See* United States v. Broadhurst, No. 3:11–cr–00121–MO–1, 2012 WL 5985615, at *1 (D. Or. Nov. 28, 2012) (noting that due to unsecured wireless networks, it was impossible to

associated IP address, meaning the public can only identify the *router's* IP address, which oftentimes does not provide personally identifying information because it does not identify the network within an individual's home.[10] Therefore, this IP address is analogous to locating the phone tower that a cell phone connected to, rather than the actual phone used. These factors play an important role in the reliability and specificity of information that the IP address reveals to law enforcement officials.[11]

Using IP addresses can be a valuable tool for law enforcement officials to begin their search to locate criminals through their Internet usage, because virtually everyone uses the Internet in some capacity. This means nearly every criminal inevitably leaves a trail each time he or she uses the Internet. However, officials' use of IP addresses to obtain search warrants creates Fourth Amendment privacy concerns, typically in the steps taken after an IP address is known.[12] In particular, Internet Service Providers,

---

conclude the source of child pornography file-sharing solely by using an IP address).

[10] Weissman, *supra* note 1. Courts have used this fact to conclude that a search warrant is not needed to obtain a user's IP address in the first place because it does not lead to personally identifying information. *See* United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *5 (C.D. Cal. Aug. 8, 2016) ("When a consumer purchases a computer, takes it home, opens it up, and turns it on, that computer does not have an IP address. Instead, it is assigned an IP address by an internet service provider (like Time Warner) when it connects to a particular network, and that IP address may change if the computer connects to a different network.").

[11] *See Dynamic IP vs Static IP,* WHATISMYIPADDRESS.COM, http://whatismyipaddress.com/dynamic-static (last visited Jan. 17, 2017). Additionally, dynamic IP addresses make it more difficult to accurately locate someone via their IP address because it changes. With a static IP address, geo-location services are more accurate and more expensive. *Id.*

[12] *See* U.S. CONST. amend. IV. The Fourth Amendment concerns typically arise in the additional steps that law enforcement officials take after obtaining an IP address to physically locate where the defendant is. *See, e.g.*, *Acevedo-Lemus*, 2016 WL 4208436, at *5 (explaining how Defendant's assertion that the government's use of malware to obtain his IP address was not a Fourth Amendment search "because an IP address is not a private physical feature of a computer, but a commonly disclosed digital one assigned by a third party[,]" leaving the Defendant with no subjective expectation of privacy). However, some have found the courts' reasoning to allow a foray into more intrusive ways

such as Comcast and AT&T, are subject to court subpoenas to provide personal information about their users.[13] Some privacy experts indicate that ISPs will become more reluctant to disclose this information readily, however, because of the burgeoning concerns about keeping customer information private.[14] This technique has become less reliable, though, as tech smart criminals have found ways to circumvent tracking via IP address searches.[15]

This Recent Development argues that IP addresses alone should not provide sufficient probable cause to obtain a search warrant and that more substantive information should be required

---

to obtain IP addresses and warn that "[w]hat matters is how the government obtain[s] the information," calling for caution in the techniques law enforcement uses to not only obtain IP address information, but also the steps taken after an IP address is known. *See* Orin Kerr, *Remotely Accessing an IP Address Inside a Target Computer is a Search*, WASH. POST (Oct. 7, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/07/remotely-accessing-an-ip-address-inside-a-target-computer-is-a-search/.

[13] ISPs are subject to court subpoenas and must provide the information requested in the subpoena. *See, e.g.*, *Privacy Policy: Information We Share*, GOOGLE, https://www.google.com/policies/privacy/#nosharing (last visited Feb. 16, 2017) (stating in their privacy policies that Google will "share personal information . . . [to] meet any . . . legal process or enforceable government request."). All ISPs are "provider[s] of electronic communication service" under the Stored Communications Act and are therefore subject to required disclosures upon proper governmental request. Stored Communications Act, 18 U.S.C. § 2703 (2012) (stating warrants must be issued in accordance with the Federal Rules of Criminal Procedure). ISPs are ordered to disclose the subscriber's name, address, length of service, and source of payment for the service. *See id.* § 2703(c)(2).

[14] There are growing privacy concerns of companies like Apple and Yahoo providing user information to government officials; concerns over the policies of ISPs are also expected to arise. *See generally Our Principles*, DIGITAL DUE PROCESS, https://digitaldueprocess.org/ (last visited Feb. 17, 2017) (stating a mission of "providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public").

[15] This can be done through use of public Wi-Fi, the Tor network, and Virtual Private Networks ("VPNs"). *See generally* Larry Greenemeier, *Back to Hackers*, SCIENTIFIC AMERICAN: TECH (June 11, 2011), https://www.scientificamerican.com/article/tracking-cyber-hackers/.

to issue a warrant. Part II provides background on the current law governing the use of IP addresses to obtain search warrants. Part III discusses how law enforcement officials obtain search warrants with IP address information and explores the reliability, or lack thereof, regarding this information. Part IV explores what additional information should be provided, in addition to an IP address, in order for a search warrant to be lawfully granted in a manner that does not infringe on constitutional rights. Part V discusses the privacy concerns with current and future methods law enforcement officials use to obtain identifying information.

II. BACKGROUND AND CURRENT LAW

Cyberspace crime challenges the breadth of law enforcement investigative techniques, creating a murky line between a user's Fourth Amendment right to privacy[16] and law enforcement's duty to apprehend criminals. Privacy surrounding Internet use has presented courts with challenging questions of exactly how much privacy users should reasonably expect when they enter cyberspace and the methods law enforcement officials can use when finding cyber criminals.[17] Generally, federal courts have reached an (almost) unanimous consensus that when users enter the cyber domain, privacy rights cease to exist.[18]

---

[16] U.S. CONST. amend. IV (granting citizens the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . and no Warrants shall issue, but upon probable cause").

[17] *Compare* United States v. Stanley, 753 F.3d 114, 120 (3d Cir. 2014) (holding Defendant did not have a reasonable expectation of privacy in the Internet signals he intentionally projected outside of his home, so the signal sensing device that detectives used to locate him did not require a warrant), *with* United States v. Croghan, No. 1:15-cr-48, 2016 WL 4992105, at *7 (S.D. Iowa Sept. 19, 2016) (finding the Defendant had a reasonable expectation of privacy in his IP address when the government obtained it by searching his computer, even though Defendant "lacked an objectively reasonable expectation of privacy in the information actually gathered").

[18] *See, e.g.*, United States v. Broadhurst, No. 3:11–cr–00121–MO–1, 2012 WL 5985615, at *4 (D. Or. Nov. 28, 2012) ("A defendant who connects to the Internet by hijacking his neighbor's wireless network does not have a privacy interest in the signals coming from his house that society is prepared to recognize as reasonable."). *But see Croghan*, 2016 WL 4992105, at *7

The Supreme Court has determined that one's expectation of privacy is a two-fold inquiry: first, a user must have a subjective expectation of privacy; and second, society must view this expectation as reasonable.[19] When engaging in conduct on the Internet, courts have found that "Internet users do not have reasonable expectations of privacy in their own IP addresses or the IP addresses of the websites they visit"[20] because this information is available to others,[21] not just to law enforcement officials during investigation.[22] Due to the advent of free online services, anyone can trace an IP address.[23] Additionally, when law enforcement officials obtain IP address information from third parties, specifically from ISPs, courts have concluded that because users voluntarily disclosed this information to third parties,[24] there is no reasonable expectation of privacy in that information.[25] The

---

(explaining the FBI's search of Defendant's computer through the use of malware to locate his IP address was an unconstitutional search because there was a reasonable expectation of privacy in the contents of his computer, despite the fact he used the Internet for illegal activity).

[19] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). This two-step requirement is used routinely today by courts when evaluating expectation of privacy matters. *Id. See also* United States v. Bautista, 362 F.3d 584, 589 (9th Cir. 2004).

[20] United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *4 (C.D. Cal. Aug. 8, 2016).

[21] *See* Smith v. Maryland, 442 U.S. 735 (1979) (ruling people do not have an expectation of privacy in information they voluntarily disclose to others).

[22] *See Acevedo-Lemus*, 2016 WL 4208436, at *4 (citing United States v. Martinez, 588 F. App'x 741 (Mem.) (9th Cir. 2014) (unpublished).

[23] *See* Markham*, supra* note 7.

[24] United States v. Christie, 624 F.3d 558, 573 (3d Cir. 2010) ("Federal courts have uniformly held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."). The information disclosed often includes name, address, phone number, and other information that ISPs may require when registering a router for Internet service. Comcast Legal Response Center, *Law Enforcement Handbook,* COMCAST 1, 14 (Rev. May 1, 2015), http://www.comcast.com/~/Media/403EEED5AE6F46118DDBC5F8BC436030.ashx.

[25] *Acevedo-Lemus*, 2016 WL 4208436, at *4. For example, Google explicitly states in their privacy policy terms they collect information that is used, and often required, to create a Google Account and will share this information when

consensus among the courts is that Internet activity, including IP address information, is not a "private" activity that society considers protectable under the Fourth Amendment.[26] Targeted advertisements,[27] Find My iPhone,[28] and other valuable location services that people utilize every day are available *because* Internet activity is not private. This has all contributed to the notion that users should not assume a reasonable expectation of privacy in online conduct, specifically with respect to IP addresses.[29]

---

the government properly requests it. *See Privacy Policy: Information We Share*, *supra* note 13.

[26] *Acevedo-Lemus*, 2016 WL 4208436, at *4 ("Internet users have no expectation of privacy in the . . . IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing information.") (quoting United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007)). One court even went so far as to recognize that "society's view of the Internet . . . has undergone a drastic shift[,]" changing the "corresponding expectation of privacy" in that information. United States v. Matish, 193 F. Supp. 3d 585, 618 (E.D. Va. 2016). On the contrary, defendants often argue that Internet activity conducted *inside* of their home is a private activity because they are protected by the walls of their home. See for example United States v. Stanley, 753 F.3d 114, 120–21 (3d Cir. 2014), where Defendant attempted to use the successful defense from *Kyllo*, that the home acts as a shield to keep activities conducted within the walls from public observation, but the court declined to follow this reasoning with respect to Internet activity. Kyllo v. United States, 533 U.S. 27, 31–32 (2001).

[27] Targeted advertisements are directed at individuals and are generated through tracking technology that companies use on web sites. *See* Darla Cameron, *How Targeted Advertising Works*, WASH. POST (Aug. 22, 2013), https://www.washingtonpost.com/apps/g/page/business/how-targeted-advertising-works/412/.

[28] Find My iPhone allows users to locate their phone when it is lost. When the device is online, the phone's location can be found using GPS technology. *See Find My iPhone*, ITUNES, https://itunes.apple.com/us/app/find-my-iphone/id376101648?mt=8 (last visited Jan. 27, 2017).

[29] United States v. Johnson, No. 15-00340-01-CR-W-GAF, 2016 WL 6136586, at *8 (W.D. Mo. Oct. 20, 2016) (finding "[Defendant] did not have a reasonable expectation of privacy in his IP address because [Defendant's] subjective expectation of privacy simply is one that society is not prepared to recognize as reasonable"). Interestingly, courts have begun to rely on society's understanding and expectation that Internet activity is no longer considered by many to be private. *See generally id.* ("The concept of an interest in privacy that

Concerns arise when law enforcement makes use of this "public" information in a way that seems to be more invasive.[30] Once police have obtained an IP address, additional steps are usually taken to pinpoint the location of the suspected criminal.[31] These additional steps are what defendants usually allege as invasions of privacy.[32] Defendants typically argue that they have a "reasonable expectation of privacy in the contents of [their] computer,"[33] and when law enforcement uses techniques that allow them to view that content without a warrant, their Fourth Amendment rights are violated.[34] However, these additional "invasive" steps are typically necessary for law enforcement to obtain search warrants, because although an IP address alone will narrow down the suspect list, it rarely leads directly to the suspect.[35] To illustrate, suppose a criminal goes to Starbucks and

---

society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation . . . that certain facts will not come to the attention of the authorities.") (quoting United States v. Jacobson, 466 U.S. 109, 122, 104 S. Ct. 1652, 1661 (1984)).

[30] *See, e.g.*, *Stanley*, 735 F.3d at 116–17 (considering Fourth Amendment implications of detective's warrantless use of a "MoocherHunter" to locate the suspect based on the wireless signals transmitted from his home).

[31] *See id.*; United States v. Broadhurst, No. 3:11-cr-00121-MO-1, 2012 WL 5985615, at *1 (D. Or. Nov. 28, 2012).

[32] *See, e.g.*, *Broadhurst*, 2012 WL 5985615, at *1 (using "the Shadow") (discussed *infra* Section III.B); *Stanley*, 735 F.3d at 114 (using a "MoocherHunter") (discussed *infra* Section III.B).

[33] United States v. Allain, No. 15-cr-10251, 2016 WL 5660452, at *13 n.5 (D. Mass. Sept. 29, 2016) (holding that there is a reasonable expectation of privacy in contents on a computer).

[34] *See* Kerr, *supra* note 12 ("Government access to information stored inside a suspect's computer without permission is a search regardless of whether the information has been voluntarily revealed in some other way to someone else."). This argument was made in the Playpen cases, where the FBI sent malware to registered computers of a child pornography website to learn their IP address, which was obtained by looking at the contents on the user's computer. *See, e.g.*, United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *4 (C.D. Cal. Aug. 8, 2016).

[35] *See generally* Hoschar v. Layne, 647 F.App'x 632, 634 (6th Cir. 2016) (where suspect connected to a stranger's network and the network owner was accused and arrested for the illegal activity); United States v. Stanley, 753 F.3d

connects to an unsecured (non-password-protected) Wi-Fi network to conduct illegal cyber activity. When this connection to an unsecured network is made, courts have held that the defendant no longer has a "reasonable expectation of privacy in signals he intentionally emitted to connect to unauthorized networks."[36]

Matters are further complicated when criminals use dark web browsers[37] to remain private. Dark web browsers attempt to safeguard user's information by allowing "users to access the Internet in an anonymous fashion," helping users to remain private on the seemingly non-private web.[38] The advantage of using a dark web browser, particularly for criminal activity, is that the IP address location is hidden, and therefore not easily ascertainable.[39] However, even on a dark web browser, an IP address is still provided when the user is on the network.[40] The difference is that these browsers will anonymize the originating user, similar to making a private phone call where "No Caller ID" or "Blocked

---

114, 115–16 (3d Cir. 2014) (where IP address was traced to neighbor's home because suspect connected to her network).

[36] *Broadhurst*, 2012 WL 5985615, at *5; *see also Stanley*, 735 F.3d at 119–20 (finding that Defendant's conduct of sharing child pornography with other Internet users on a stranger's Internet connection "deliberately projected *outside* of his home, as it required interactions with persons and objects beyond the threshold of his residence.").

[37] An example is the Tor network, which is an anonymous web browser that allows users to connect through "virtual tunnels rather than making a direct connection," allowing users greater privacy. *Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en (last visited Jan. 10, 2017).

[38] United States v. Matish, 193 F. Supp. 3d 585, 593 (E.D. Va. 2016).

[39] "Although a website's operator usually can identify visitors to his or her site through the visitors' Internet Protocol ('IP') addresses, Tor attempts to keep a user's IP address hidden." *Id*. at 593–94 (explaining how the Tor network, a popular dark web browser, operates). *See also Tor: Overview*, *supra* note 37 ("[i]ndividuals use Tor to keep websites from tracking them and their family members" and to protect against Internet surveillance). A high-profile example of a site hosted on the Tor network is The Silk Road, where users were trafficking drugs and weapons, among other illegal activities. *See* Donna Leinwand Leger, *How FBI Brought Down Cyber-Underworld Site Silk Road*, USA TODAY, http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/ (last updated May 15, 2014).

[40] *See also Tor: Overview*, *supra* note 37.

Number" appears on the receiver's phone.[41] Courts have not been persuaded by this attempt at anonymity and have found that the IP addresses were still part of the public domain because the IP address still needs to be disclosed to the network initially, meaning that an individual cannot use these browsers without first revealing his or her IP address.[42] A user must still initially "disclos[e] his identifying information to complete strangers" in order to use the browsers, thereby "taking a significant gamble on any real expectation of privacy under these circumstances."[43] This could be loosely likened to a person using a Post Office ("P.O.") Box, where the user only reveals his personal address to the Postal Service and provides everyone else with the P.O. Box address. The user is actively taking steps to conceal his personal address, but in order to do so he had to provide that address to a third party helping him remain private.

III. USING IP ADDRESSES TO OBTAIN SEARCH WARRANTS

Law enforcement officials use IP addresses to obtain search warrants because IP addresses are viewed as public knowledge.[44] To obtain a search warrant, law enforcement officials must present

---

[41] *Id.*

[42] United States v. Michaud, No. CR15-5351RJB 2016, WL 337263 at *7 (W.D. Wash. Jan. 28, 2016) ("Although the IP addresses of users utilizing the Tor network may not be known to websites, . . . using the Tor network does not strip users of all anonymity, because users accessing [website at issue] must still send and receive information, including IP addresses, through another computer, such as an Internet Service Provider, at a specific physical location. Even though difficult for the Government to secure that information tying the IP address to Mr. Michaud, the IP address was public information, like an unlisted telephone number, and eventually could have been discovered."); *see also* United States v. Johnson, No. 15-00340-01-CR-W-GAF, 2016 WL 6136586, at *3 (W.D. Mo. Oct. 20, 2016) ("Defendant had no expectation in the privacy of his IP address, even when using the Tor network.").

[43] United States v. Farrell, No. CR15-029RAJ, 2016 WL 705197, at *2 (W.D. Wa. Feb. 23, 2016).

[44] *See generally* Hoschar v. Layne, 647 F. App'x 632, 633 (6th Cir. 2016) (where police detectives searched and arrested an innocent man based on an IP address); United States v. Stanley, 753 F.3d 114, 116–17 (3d Cir. 2014) (where detective observed Internet signal strengths after investigating several suspect IP addresses).

evidence, through affidavits, as to the nature of the probable cause for the search.[45] At first, search warrants were granted after officials presented only an IP address and information from the ISP as probable cause, which in turn did not directly lead investigators to the suspect.[46] The identifying information provided by the ISP typically only includes the router owner's name, home address, and payment information, but the router owner is often not the person conducting the illegal activity.[47] For example, when a UNC student illegally downloads content while connected to the University's network, the download is traced back to the University generally, not to the specific student. Therefore, the University then must do additional work to identify the student or students responsible for the activity.[48] The same is true for router owners. Consequently, router owners have had their personal computers searched when they had no connection to the crime other than the fact that the suspect connected to their network router.[49] This section will explore illustrative examples of how

---

[45] The Fourth Amendment does not define "probable cause" but the Supreme Court has reasoned that probable cause exists if the magistrate has a substantial basis to believe there is a "fair probability that contraband or evidence of a crime will be found in a particular place." *See* Illinois v. Gates, 462 U.S. 213, 238 (1983).

[46] *Hoschar*, 647 F. App'x at 633 (where a search warrant was granted with only IP address information).

[47] For example, some of the customer information that Comcast collects is a customer's name, service address, billing address, e-mail address, telephone number, driver's license number, social security number, bank account number, and credit card number (although "typically not all" of this information is collected for each customer). *See Comcast Customer Privacy Notice: Disclosure,* XFINITY (Aug. 1, 2015), https://www.xfinity.com/Corporate/Customers/Policies/CustomerPrivacy.html#. In *Stanley*, detectives subpoenaed Comcast for a subscriber's name and home address associated with an IP address. *Stanley*, 753 F.3d at 115-16.

[48] Morgan Baskin, *Think Twice Before Illegally DownloadingIntellectual Property Companies are Watching You*, USA TODAY COLLEGE (March 5, 2015), http://college.usatoday.com/2015/03/05/think-twice-before-illegally-downloading-intellectual-property-companies-are-watching-you/.

[49] *See, e.g.*, *Stanley*, 753 F.3d at 116 (observing that the "search revealed that none of the Neighbor's computers contained [] child pornography").

police have used IP addresses and other techniques to garner more information after knowing an IP address.

A. Illustrative Cases of Evidence Provided for Search Warrants

Law enforcement officials have frequently linked online criminal activity with an IP address and obtained a search warrant with this information. In *United States v. Coca*,[50] officials searched the defendant's home after the investigating officer provided an affidavit outlining the number of e-mails exchanged, the IP address of a computer, and the name and street address associated with the IP address from a subpoena to the ISP, Comcast.[51] The defendant challenged the issuance of the search warrant, alleging the small amount of information offered to obtain the warrant did not provide "a sufficient nexus that evidence of criminal activity would be found at" his address.[52] Based on his home's location near a college campus, he argued that the e-mail account that sent over sixty e-mails containing child pornography was a random, temporary user who accessed his account from a device not located within his home.[53] The court ultimately ruled that the high volume of e-mails sent from the account, and the short period of time the account was "inactive" before the warrant was served, gave the magistrate information that was "more than sufficient to demonstrate probable cause that evidence of criminal activity . . . would be found."[54] *Coca* provides an example where the police had substantive evidence in addition to the IP address to justify issuing a search warrant. However, *Coca* is somewhat of an outlier when it comes to an IP address leading to the criminal's location.

In a rather extreme example, the property of Joyce Taylor in Potwin, Kansas became the default IP address location for over a decade for MaxMind, an IP address geo-location company that maintains a database of IP address locations used by approximately

---

[50] U.S. v. Coca, No. 14-262, 2016 WL 7013037 (W.D. Pa. Dec. 1, 2016).
[51] *Id*. at 2-3.
[52] *Id*. at 6.
[53] *Id*.
[54] *Id.* at 6-7.

5,000 companies.[55] When their database cannot identify a location, Taylor's home becomes the default.[56] Her home has been associated with over 600 million IP addresses, and linked to runaway children, identity thieves, suicidal veterans, and scammers.[57] The residents alleged they have been subject to "repeated visits and calls by law enforcement officers, at all hours of the day and night . . . [and] private individuals have attempted to enter their property . . . [and] access their Internet."[58] An IP address alone has caused this Kansas home to become a "criminal hotspot."[59]

Similarly, in cases where a criminal has connected to an unsecured network, law enforcement officials have obtained warrants to search the home of these network owners. Oftentimes, the network owners are not the ones who committed the crime. A pastor in Pittsburg, Tennessee, David Hoschar, endured eighteen months of investigations and court proceedings, including an arrest and forced resignation from his church, because a search warrant was granted with only IP address information.[60] An investigator discovered that images of child pornography were being downloaded from an IP address that was traced to the pastor's

---

[55] *See* Kashmir Hill, *How an Internet Mapping Glitch Turned a Random Kansas Farm into a Digital Hell*, FUSION (Apr. 10, 2016, 10:00AM), http://fusion.net/story/287592/internet-mapping-glitch-kansas-farm/ (explaining companies would use MaxMind's database when, for example, they want to identify a user who has been illegally downloading music). Some examples of companies who use MaxMind are Facebook and Google. *Id.*

[56] Arnold v. MaxMind, Inc., No. 16-1309-JTM, 2016 WL 6124985, at *2 (D. Kan. Oct. 20, 2016).

[57] *See id.*; *see also* Hill, *supra* note 55.

[58] *Arnold*, 2016 WL 6124985, at *1.

[59] Hill, *supra* note 55.

[60] Hoschar v. Layne, 647 F. App'x 632, 632 (6th Cir. 2016) (this case was brought by the accused pastor against the principal investigating officers for giving false or misleading testimony to a grand jury in order to secure an indictment). *See also* Pam Sohn, *Sohn: Where is Justice When Justice is Done?*, TIMES FREE PRESS (May 14, 2016), http://www.timesfreepress.com/news/opinion/times/story/2016/may/14/sohn-where-justice-when-justice-done/365536/.

home and identified as belonging to his wife.[61] There was no password on their router, and thus the network was unsecure.[62] The investigator was granted a search warrant based on the IP address information and seized a computer and laptop from the home, of which neither had any trace of child pornography.[63] When testifying before the grand jury, the police investigators did not explain that the Hoschar's router was not password protected, a key fact given anyone in the vicinity of their home could have downloaded the images by connecting to their network.[64] These mix-ups are not uncommon when only IP address information, even when coupled with personal data from ISPs, is used to obtain a search warrant.[65] When technology easily provides for anonymity, law enforcement must demand more information in order to locate a suspect. In addition to an IP address, officials have used devices to identify the location of suspects once an IP address is known.

B. Police Techniques Used in Conjunction with IP Addresses

IP addresses unquestionably provide officials with a solid starting point to trace criminal activity. However, the addresses alone typically do not lead officials to the suspect.[66] Therefore, law

---

[61] *Hoschar*, 647 F. App'x at 633. This information was obtained after the ISP was subpoenaed, specifically pointing to his wife.

[62] *Id.*

[63] *Id.* at 633–34. After the Tennessee Bureau of Investigation conducted an analysis, there was no sign of any downloaded images nor evidence that it was "scrubbed" of child pornography.

[64] *Id*. at 634–35. The Hoschars additionally challenged that the investigators did not present that their home was located next to a motel, which would have led to an even larger suspect pool in addition to the unsecured router.

[65] *See* Ansel Herz, *Police Go on Fishing Expedition, Search the Home of Seattle Privacy Activists Who Maintain Tor Network*, THE STRANGER (Mar. 30, 2016, 12:56 PM), http://www.thestranger.com/slog/2016/03/30/23885710/police-go-on-fishing-expedition-search-the-home-of-seattle-privacy-activists-who-maintain-tor-network (commenting further that even Tor users are not immune from search warrants based on IP addresses).

[66] *See Hoschar*, 647 F. App'x at 633; U.S. v. Coca, 2016 WL 7013037 (W.D. Pa. Dec. 1, 2016); Arnold v. MaxMind, Inc., 2016 WL 6124985 (D. Kan. Oct. 20, 2016).

enforcement has developed more advanced techniques that use IP addresses as a starting point to launch more invasive searches.[67]

In *United States v. Broadhurst*,[68] detectives traced an IP address using a signal-locating device known as the Shadow.[69] A detective discovered that child pornography photographs were being shared on a peer-to-peer network[70] and traced the source to a particular neighborhood after identifying ten IP addresses that were sharing the photographs.[71] After subpoenaing the ISPs for the ten IP addresses, the search was narrowed down to six addresses in the neighborhood; but, once again, the addresses were accessed through an unsecured wireless network.[72] Knowing that unsecured networks lead to a much larger suspect range, the detective employed the Shadow device to narrow down the suspect pool.[73] The Shadow works by scanning the area for radio signals emitted by station devices (e.g., computers) and access points (e.g., wireless routers) that allow the devices to connect to each other, facilitating an Internet connection.[74] By observing the signal strength, the operator can know if the station device or access point

---

[67] United States v. Acevedo-Lemus, 2016 WL 4208436, at *4 (C.D. Cal. Sept. 29, 2016).

[68] United States v. Broadhurst, 2012 WL 5985615 (D. Or. Nov. 28, 2012).

[69] The Shadow is a device that allows the user to observe and locate wireless access points (mechanisms, like routers, that allow wireless devices to connect to that network) and station devices (computers, tablets, smart phones) by receiving radio signals within the immediate area of the device. *Id.* at *2–3.

[70] A Peer-to-Peer ("P2P") network allows users to share files among themselves by connecting directly to another computer, providing an anonymized route of the traffic. *See, e.g.*, Margaret Rouse, *Peer-to-Peer (P2P)*, TECHTARGET: SEARCHNETWORKING, http://searchnetworking.techtarget.com/definition/peer-to-peer (last updated Aug. 2014). When users are on a P2P network, a "peer" can search for files being shared on the network and download ones of interest. *Broadhurst*, 2012 WL 5985615, at *12 n.1. Popular examples of P2P networks are Napster and BitTorrent.

[71] *Broadhurst*, 2012 WL 5985615, at *1.

[72] *Id.* (explaining that because users were accessing the photographs on an unsecured network, anyone could theoretically access the network as long as they were in the wireless range).

[73] *Id.* at *2-3.

[74] *Id.*

is close.[75] In *Broadhurst*, as in other cases, it was determined that the router owner was not involved after their home was searched. However, when detectives used the Shadow while walking in the vicinity of the other suspected addresses, one address had a high signal spike that indicated the suspect was there.[76] A search warrant was then obtained based on the information gathered using the Shadow.[77]

The defendant argued that, before the Shadow could be used, law enforcement needed to first obtain a warrant because monitoring the signals emitted from his device constituted a Fourth Amendment search.[78] He argued he had a constitutional right to privacy in the signals that the device analyzed.[79] The federal court rejected this argument because the defendant, through his use of another's network, voluntarily disclosed his IP address information to third parties.[80] The *Broadhurst* court, agreeing with the Sixth Circuit, reasoned that "[w]hen criminals use modern technological devices to carry out criminal acts and to reduce the possibility of detection, they can hardly complain when the police take advantage of the inherent characteristics of those very devices to catch them."[81]

---

[75] *Id*. Because the Shadow requires the user to select access points or station devices to observe, the user must have an idea of whom they wish to observe. In this case, the detective walked around the addresses in question with the device and observed the signal strength at each address to gather information. *Id.*

[76] *Id*. at *3.

[77] *Broadhurst*, 2012 WL 5985615, at *4.

[78] *Id.* Defendant alleged it "intruded upon a constitutionally protected privacy interest" in the signals. *Id.*

[79] *Id.*

[80] *Id.* The court recognized a nuance when defendants use a third party's unsecured network to avoid detection. "On the one hand, [the] defendant would serendipitously receive Fourth Amendment protection because he hijacked another person's Internet connection to share child pornography files. On the other hand, another individual who uses his own Internet connection to share the same files lacks such protection, merely because the IP addresses would track back to his house . . . . [T]he court should not recognize an expectation of privacy in one case simply because one individual uses a hijacked wireless signal." *Id.* at *5.

[81] *Id.* at *5 (quoting *United States v. Skinner,* 690 F.3d 772, 774 (6th Cir. 2012)).

With an almost identical fact pattern to *Broadhurst*, the Pennsylvania Police Department in *United States v. Stanley*[82] used a "MoocherHunter" to locate the person suspected of downloading child pornography.[83] The detective discovered the user on a P2P network,[84] found the IP address and subpoenaed the ISP for identifying information.[85] Detectives then searched the router owner's home, ultimately finding no evidence of child pornography but discovering that the router was not password-protected.[86] The detective left a police computer in the neighbor's home connected to the router and was able to observe the suspect downloading the illegal images and obtain the suspect's IP and MAC address.[87] Without a search warrant,[88] the detective was able to see when Stanley was sharing images and was able to identify Stanley's IP address because the neighbor allowed the detective to observe who was connecting to his router.[89] Once the detective knew the IP address, he used the "MoocherHunter" and determined Stanley's apartment was the suspected place of the illegal

---

[82] United States v. Stanley, 753 F.3d 114 (3d Cir. 2014).

[83] *Id.* at 115. The "MoocherHunter" is mobile tracking software, much like the Shadow device, that measures the signal strength of the radio waves emitted from the mooching device. The signal strength increases when the device is pointed towards where the mooching device is located. *Id.* at 116. The device is called the "MoocherHunter" because it is used to find those who are "mooching" off another person's wireless router. *Id.* at 115.

[84] *See supra* explanation in note 70.

[85] *Id.* at 115–16.

[86] *Id.* at 116.

[87] *Id.* This information would have been available to anyone who was connected to the wireless router at that time. *Id*. A MAC (Media Access Control) address is assigned to network hardware adapters assigned by the provider. *See What Is a MAC Address*, WHATISMYIPADDRESS.COM, http://whatismyipaddress.com/mac-address (last visited March 3, 2017).

[88] Notably, the detective contacted the United States Attorney before proceeding with their investigation to inquire whether a search warrant was needed. They "discussed the practical impossibility of obtaining a search warrant without knowing which one of the many nearby residences the signal was being transmitted from," and concluded that a warrant was not needed. *Stanley*, 753 F.3d at 117.

[89] *Id.* at 116.

activity.[90] With this information, the detective obtained a search warrant for Stanley's home, finding 144 images and videos classified as child pornography.[91] As seen in *Hoschar,* where strangers were connecting to the pastor's unsecured network, the same was true in *Stanley.*[92] Stanley was able to connect to his neighbor's unsecured network in an attempt to avoid detection.[93] The detective in *Stanley*, however, was able to provide more substantive evidence to obtain a search warrant after using the MoocherHunter.[94] This additional information was needed to accurately determine that Stanley was the suspect.[95] Consequently, this type of information should be required in search warrants where the IP address associated with the router does not belong to the criminal.

IV. WHAT SHOULD BE INCLUDED IN SEARCH WARRANTS

As seen in the illustrative cases in Section III.B, searches conducted with information only obtained from a user's IP address narrow the suspect list down to virtually anyone, anywhere, with access to a given network at a given time. The ability to narrow down the suspect list, often to a specific neighborhood or street, is undoubtedly helpful information. Therefore, this information—when coupled with other techniques—can be lawfully utilized to gather substantive evidence before seeking a search warrant. It is evident that courts do not consider the wireless devices that law enforcement officials have used to be an illegal search under the Fourth Amendment. However, as technology and the techniques used to locate criminals become more advanced , an intrusion

---

[90] *Id.* at 117.
[91] *Id.*
[92] *Id.*
[93] *Stanley*, 753 F.3d at 117.
[94] *See id.* The detective knew the MAC address of the suspect because of the computer left at the neighbor's house to observe who was connecting to the network, and the MoocherHunter then confirmed that the wireless signals connecting to the network were emitted from Stanley's apartment. This additional investigation was needed after the IP address of the router was known to lead to the suspect. *Id.*
[95] *Id.*

further and further into people's privacy is on the horizon. One such current technique includes sending malware to computers, which is viewed as more intrusive than using a device that reads wireless signals.[96] This section will discuss factors that law enforcement officials should consider to ensure probable cause is established before seeking a search warrant. The privacy concerns implicated by vague search warrants, oftentimes including only IP address information, will also be explored. This includes how ISPs respond to subpoenas and the potential for greater resistance from ISPs moving forward.

A. Further Investigation Should be Conducted to Meet the Probable Cause Standard

Given the unreliable nature of an IP address when used to pinpoint the exact suspect in a crime, law enforcement officials should conduct a more thorough investigation before seeking a search warrant. The Fourth Amendment does not define what is required to establish probable cause before a search warrant is issued, but the Supreme Court has reasoned probable cause is found when "there is a fair probability that . . . evidence of a crime will be found in a particular place."[97] An IP address simply does not meet this probable cause standard because, as seen in Section III, the IP address often leads to an innocent home where a criminal has been connecting to a network.[98]

i. Unsecured Networks

In addition to receiving information from the user's ISP, one of the most important facts officers should determine is whether the network is secured or not.[99] Unsecured networks should be a red

---

[96] *See, e.g.*, United States v. Michaud, 2016 WL 337263, at *2 (W.D. Wash. Jan. 28, 2016) (describing the FBI's use of a Network Investigative Technique ("NIT") that sent malware to users that, when downloaded, sent identifying information back to the FBI, including the user's IP address).

[97] Illinois v. Gates, 462 U.S. 213, 238 (1983).

[98] *See, e.g.*, Hoschar v. Layne, 647 F. App'x 632, 633 (6th Cir. 2016).

[99] For instance, in *Hoschar*, a claim of malicious prosecution was brought against the detectives because they neglected to testify before the grand jury that the wrongfully accused had an unsecured Wi-Fi network, meaning that anyone

flag to investigators because they leave open a large pool of suspects. Anyone within the wireless range can connect, meaning suspects can look for unsecured networks to use as a shield for their physical location,[100] as seen in Section III. Therefore, a search of the router owner's home should not be conducted without more corroborating information pointing to them as a suspect.[101]

Even on a secured network, it can be relatively simple for some users to hack into password-protected Wi-Fi, leading to a larger suspect pool even when secured networks are identified.[102] Router

---

within range could connect to the network. The detectives were ultimately protected by immunity. *Id.* at 635–37.

[100] Interestingly, the Third Circuit hinted in *United States v. Stanley* that simply connecting to an open Wi-Fi network may itself be a criminal act. *Stanley*, 753 F.3d at 120 ("The presence of Stanley's unauthorized signal was itself 'wrongful.'"). The court reasoned that Stanley "essentially hijacked his [n]eighbor's router, forcing it to relay data to Comcast's modem and back to his computer, all without either the [n]eighbor's or Comcast's knowledge or consent," acting as a "virtual trespasser." *Id.* The judge even went so far as to cite several state statutes that have "criminalized unauthorized access to a computer network." *Id.* at n.10. While this issue was not the focus of the opinion, it has raised privacy concerns because the neighbor intentionally left their Wi-Fi open (or at least neglected to set a password) so it is difficult to see this act as a theft or trespass. *See* TechDirt, *Appeals Court Says Using Open WiFi May Be a Crime*, ABOVE THE LAW (June 13, 2014, 10:08AM), http://abovethelaw.com/2014/06/appeals-court-says-using-open-wifi-may-be-a-crime/ (stating it is "quite troubling" to have this language in an appeals court ruling).

[101] *See Stanley,* 753 F.3d at 116, for an example of good evidence of corroborating information. The officer used the MoocherHunter after knowing Defendant's name, home address, and the MAC address of the suspected computer, and had evidence that the defendant was connected to the suspected network. This information was obtained because the router owner allowed the officer to set up a police computer in their home that was connected to the network Stanley was accessing. This allowed the officer to observe who connected to the network and link the activity to Stanley. If the router owner had refused, detectives would have presumably had greater difficulty in locating Stanley. *See also* U.S. v. Coca, 2016 WL 7013037 (W.D. Pa. Dec. 1, 2016).

[102] "For example, hacking is much more prevalent now than it was even nine years ago, and the rise of computer hacking via the Internet has changed the public's reasonable expectations of privacy . . . . Now, it seems unreasonable to think that a computer connected to the Web is immune from invasion. Indeed, the opposite holds true: in today's digital world, it appears to be a virtual

passwords that are assigned by the ISP are found on the back of the device, and unless a user changes that password, anyone with access to that device can obtain the password.[103] The ease with which a criminal can access a stranger's Wi-Fi network in an attempt to avoid detection leads to the conclusion that further investigation is needed for search warrants.[104] Devices such as the Shadow and the MoocherHunter can be employed to gather further information and, in conjunction with the router's location, pinpoint a suspect.[105]

ii. Additional Devices

Courts have allowed law enforcement to use devices like the Shadow and MoocherHunter without a search warrant, and until a court declares them unlawful to use without a search warrant,[106] these mobile geo-location tools will be helpful. These devices measure signal strength, which in turn helps locate where the signal is originating from, and, as it stands today, there is no reasonable expectation of privacy in these transmissions.[107] Defendants argue that using these devices is like looking inside their home to view their activity.[108] The government, on the other

---

certainty that computers accessing the Internet can—and eventually will—be hacked." United States v. Matish, 193 F. Supp. 3d 585, 619 (E.D. Va. 2016). *See also* Aseem Kishore, *Prevent Someone Else from Using Your Wireless Internet Connection*, ONLINE TECH TIPS (Sept. 21, 2015), http://www.online-tech-tips.com/computer-tips/secure-wireless-connection/ ("Many people assume that setting a strong WiFi password is all they need, but this is not [the] case.").

[103] *See* Kishore, *supra* note 102. The author warns against keeping the long passwords that are assigned from the ISPs, often found on the device itself, because anyone "can still gain access by simply copying the password printed on your wireless router, since most people don't change the default password set by their ISP." *Id.*

[104] Aaron Mackey, Seth Schoen & Cindy Cohn, ELEC. FRONTIER FOUND., *Unreliable Informants: IP Addresses, Digital Tips and Police Raids* 11 (Sept. 2016), https://www.eff.org/files/2016/09/22/2016.09.20_final_formatted_ip_address_white_paper_0.pdf.

[105] *See supra* Section III.B.

[106] *See infra* Section V.A.

[107] United States v. Stanley, 753 F.3d 114, 114 (3d Cir. 2014).

[108] *Id.* at 117–18.

hand, explains that these signals are being sent outside the home and therefore are no longer private information.[109] Likewise, no content on their devices is being searched or intercepted with these devices; solely their Internet signal is identified.[110] Additionally, the police must have identified a radius of where the suspected user is before employing the device, meaning some preliminary search has been conducted prior to locating signals.[111]

The National Institute of Justice also lists several tools for police to use, such as the Cantenna (a Wi-Fi detector) and the Air Magnet.[112] Other experts urge police to search chat rooms, such as Reddit,[113] in specific subgroups where the suspects may be likely to post about their crimes or provide tips for others on how to do

---

[109] *Id.* at 119 (explaining that Defendant projected his Internet signals outside of his home to connect to his neighbor's network, therefore creating no reasonable expectation of privacy).

[110] *Id.*

[111] *See* United States v. Broadhurst, 2012 WL 5985615, at *1–2 (D. Or. Nov. 28, 2012) The deputy identified ten suspect IP addresses in a neighborhood and the ISP subpoenas revealed that theses addresses were registered to six home residences in the neighborhood. With this information, the deputy used a signal reading device to observe when the IP addresses at these residences were accessing the website to share illegal content. *Id.*

[112] A cantenna is used to extend the range of a wireless network or detect/intercept other wireless networks in the region. A Wi-Fi detector is used to locate wireless network signals. An Air Magnet monitors networks by intercepting or detecting signals. *See* U.S. DEPT. OF JUSTICE, *Investigative Uses of Technology: Devices, Tools, and Techniques* 44 (Oct. 2007), https://www.ncjrs.gov/pdffiles1/nij/213030.pdf (Each device is designed to "locate or intercept wireless communications from . . . computer networks."). An explanatory scenario provided in the report explains how law enforcement identified an offender who was "illegally accessing the wireless hotspot of a local business in an effort to obtain anonymous Internet access" by turning down the signal strength of the network and observing a person who moved closer and closer to the building to remain connected, which led them to apprehend the offender. *Id.* at 46.

[113] Reddit is a website that allows users to post links and stories for others to see and comment. "Subreddits" are individual communities for specific topics. *See What is Reddit?*, REDDIT HELP https://reddit.zendesk.com/hc/en-us/articles/204511479-What-is-Reddit- (last visited Mar. 19, 2017).

the same.[114] For a less invasive way to track criminals using the dark web, officials can check IP addresses with a list of Tor exit relays[115] on ExoneraTor.[116] If the IP address is also used as a Tor exit relay, then the IP owner is likely not a suspect.[117] If a warrant application is still sought, this information should be included and explained so the court can determine if there is probable cause. Unfortunately, the dark web is a tricky place and new techniques will need to be used for proper searches.

The use of these devices will likely remain controversial as cyber savvy criminals create new techniques to avoid detection. Concerns will continue to arise over whether the devices are an unconstitutional invasion of privacy and if new devices intrude further into private lives, thus constituting a Fourth Amendment violation.

B. ISP Subpoenas

As seen above, investigators must subpoena the ISP after identifying an IP address to locate the owner of the router.[118] Because the IP address obtained is that of the Internet router, not the actual device,[119] this information can only marginally narrow their broad list of suspects. With non-password protected Wi-Fi, free Internet connections, and savvy Internet users able to hack

---

[114] *See* Alan Woodward, *Viewpoint: How Hackers are Caught Out by Law Enforcers*, BBC NEWS (Mar. 12, 2012), http://www.bbc.com/news/technology-17302656 (recounting how one hacker was discovered by law enforcement).

[115] Mackey, Schoen & Cohn, *supra* note 104, at 18. "An exit relay is the final relay that Tor traffic passes through before it reaches its destination." *What Is a Tor Relay?*, ELEC. FRONTIER FOUND., https://www.eff.org/torchallenge/what-is-tor.html (last visited Apr. 6, 2017).

[116] ExoneraTor is a database of all Tor exit relays. Mackey, Schoen & Cohn, *supra* note 104, at 18.

[117] *Id.* (explaining that Tor exit relays are hosted by volunteers, therefore preserving anonymity).

[118] *See supra* Section III.

[119] Routers can be located anywhere and can be accessible to the public if the connection is through an unsecured network or the router is in a public place, such as a coffee shop or airport. *See What Is a Router?*, WHATISMYIPADDRESS.COM, http://whatismyipaddress.com/router (last visited Mar. 26, 2017).

into private Internet connections, more information is needed to justify a lawful search. As seen, police have searched incorrect homes and disrupted families, accusing loved ones of downloading child pornography, all because an unforeseeable criminal connected to their internet network.[120] This is problematic because connecting to available wireless networks is common and devices often locate these available networks automatically.[121] When the neighborhood gossip catches wind of the reasons police visited a home, rumors will spread and potentially tarnish their reputation. In the case of the pastor in Tennessee, rumors ruined eighteen months of his life with a false arrest on child pornography charges and forced his resignation from the church.[122] The potential disruption, coupled with growing privacy concerns and distrust of law enforcement nationwide, could lead to a movement for a change in ISP policies that calls for greater protection of user data.[123]

---

[120] *See* Hoschar v. Layne, 647 F. App'x 632 (6th Cir. 2016); United States v. Stanley, 753 F.3d 114 (3d Cir. 2014); United States v. Broadhurst, 2012 WL 5985615 (D. Or. Nov. 28, 2012).

[121] *See* U.S. DEPT. OF JUSTICE, *supra* note 112 (explaining that Windows operating systems can be configured to automatically scan for wireless networks).

[122] *Hoschar*, 647 F. App'x at 634.

[123] *See* Whitney Gibson, VORYS, SATER, SEYMOUR, & PEASE LLP, *Subpoena Guide for Identifying Anonymous Internet Poster* 6, n.1 (2014), http://internetdefamationblog.wp.lexblogs.com/wp-content/uploads/sites/297/2014/07/Supoena-Guide-for-Identifying-Anonymous-Internet-Posters.pdf; *see, e.g.*, 47 U.S.C. § 551 (2012) (explaining that ISPs that also provide cable services (Comcast, AT&T, TWC) are subject to the Cable Privacy Act, which prohibits these entities from releasing any personally identifying customer information without a court order), *but see* H.R. 1981, 112th Cong. (2011). This proposed bill passed a House vote in 2011 but was never enacted into law. The Bill's stated purpose was to aid in enforcing child exploitation laws by requiring ISPs to retain twelve months of logs of customers' names, credit card information, and other identifying information. *Id.* This was thought by some privacy activists to allow law enforcement officials to identify a user's personal habits, along with a fairly detailed picture of where they were each day. *Id.*

i. Privacy Concerns with ISP Subpoenas

A move towards greater privacy protection took place when the Federal Communications Commission ("FCC") passed "Protecting the Privacy of Customers of Broadband Data and Other Telecommunications Services in 2016," aimed at protecting users' personal data.[124] This rule restricts what user information can be sold, shared, or traded with third parties, for example, advertisers.[125] However, subpoenas carry more weight than third parties buying the information for advertising purposes, and the FCC rule does not address law enforcement issues.[126] ISPs must respond to a subpoena, and there is little a user can do when his or her information is being hunted.[127] More likely than not, a subscriber will not know their ISP received a subpoena for their information until after the information has been surrendered because consent is not needed to provide this to law enforcement.[128] This is of great concern to users whose information is being subpoenaed without their knowledge because they often do not know they are being investigated until police come knocking at their door with a search warrant.[129] If

---

[124] This rule was enacted on November 2, 2016 to "adopt a framework that provides heightened protections for sensitive customer information" because of the wide range of information broadband providers are able to obtain now. FCC Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 47 C.F.R. § 64.2 (2016). The rule requires carriers to "obtain customers' opt-in approval for use and sharing of sensitive customer [personal information] . . . [and] opt-out approval for the use and sharing of non-sensitive customer [personal information.]" *Id.* at 5. For an example of the opt-in opt-out policies, *see AT&T Privacy Policy: Your Rights & Choices*, AT&T, http://about.att.com/sites/privacy_policy/rights_choices (last visited Feb. 19, 2017).

[125] Kate Cox, *FCC Adopts New Privacy Rule Limiting What ISPs Can Do With Your Personal Data*, CONSUMERIST (Oct. 27. 2016, 10:42 AM), https://consumerist.com/2016/10/27/fcc-adopts-new-privacy-rule-limiting-what-isps-can-do-with-your-personal-data/.

[126] 47 C.F.R. § 64 (2016).

[127] *Frequently Asked Questions for Subpoena Targets*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/frequently-asked-questions-subpoena-targets#prevent_disclosure (last visited Jan. 10, 2017).

[128] *See, e.g.*, *Privacy Policy: Information We Share*, *supra* note 13.

[129] *See Frequently Asked Questions for Subpoena Targets*, *supra* note 127.

notification is received, the subscriber can file a motion to quash the subpoena, however, aside from this request, nothing else can be done.[130] This creates privacy concerns for users and ISPs who want their subscribers to feel secure in sharing their information. Notably, the new FCC chairman under President Trump's administration has already begun moves to undo key aspects of the recently enacted FCC rule, creating uncertainty for privacy regulations moving forward because of the amount of customer information that could be shared between ISPs, web browsers, and companies seeking to buy customer data.[131] The more people who have access to this information, the easier it may become to misidentify suspected criminals using only IP address information. The FCC's rule, though, as enacted in 2016, serves as a strong indicator that the federal government is beginning to respond to users' demands for greater privacy protection of their data.[132]

There are also time limits on how long ISPs keep data that law enforcement officials will find valuable, such as what websites a user visits, along with the time and date of the visit.[133] Given the sheer volume of data, most providers keep these records for only six to nine months.[134] Consequently, law enforcement officials must act relatively quickly when they identify a potential suspect, possibly leading to a hurried investigation to obtain a search

---

[130] *Id.*

[131] Jeff Dunn, *Republicans Are Moving To Kill Rules That'd Make Internet Providers Get Your Consent Before Selling Your Web Browsing Data*, BUSINESS INSIDER (Mar. 9, 2017), http://www.businessinsider.com/r-congress-may-overturn-obama-internet-privacy-rules-2017-3.

[132] Jon Brodkin, *FCC Imposes ISP Privacy Rules and Takes Aim at Mandatory Arbitration*, ARS TECHNICA (Oct. 27, 2016 12:17 PM), https://arstechnica.com/information-technology/2016/10/isps-will-soon-have-to-ask-you-before-sharing-private-data-with-advertisers/. But, ISPs are not happy about this and law enforcement officials would likely not be either if it makes their investigations more difficult.

[133] Alex Wawro, *FAQ: Will Your ISP Protect Your Privacy?*, PCWORLD (Oct. 11, 2016, 6:00 PM), http://www.pcworld.com/article/241591/faq_will_your_isp_protect_your_privacy_.html.

[134] *See* Gibson, *supra* note 123, at n.1.

warrant prior to the information being deleted.[135] Police need to reconcile the desire to move quickly and the necessity to ensure rights are not violated. Search warrants should not be granted when only an IP address and information from the ISP is known, because this does not provide specific enough identifying information. It is therefore important for law enforcement officials to have other techniques in place to corroborate information beyond an IP address, which is public information.

ii. ISPs Begin to Push Back

ISPs have begun to implement data protection policies to ensure subscribers that their information is not being sold or accessed without their permission.[136] As it stands, ISPs are under no obligation to retain user's data, such as Internet browsing history, for any period of time.[137] This creates problems for law enforcement officials when they seek information about an IP address that was used beyond what the ISP has in storage.[138] For example, Comcast stores IP address information for 180 days and states in their Retention Policy that if they are asked for identifying information "used more than 180 days prior to receipt of the request, Comcast will not have information to provide."[139] There are two potential explanations for this: (1) ISPs do not have the

---

[135] *See, e.g.*, United States v. Christie, 624 F.3d 558, 563 (3d Cir. 2010) ("By the time government agents got the IP addresses [of the suspects], there was not enough time to subpoena customer identities from the ISPs before the ISPs had purged their records reflecting which IP addresses had been assigned to which customers."). It was not until the FBI gained administrator-level access to the child pornography website that they were able to obtain the IP addresses of those posting and viewing illegal content.

[136] FCC Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 47 C.F.R. § 64.4 (2016) (explaining the new FCC rule requires broadband providers to have opt-in approval from customers to share personal information and "material retroactive changes" must be made to privacy policies to reflect the this).

[137] Ernesto Van der Sar, *How Long Does Your ISP Store IP-Address Logs?*, TORRENTFREAK (June 29, 2012), https://torrentfreak.com/how-long-does-your-isp-store-ip-address-logs-120629/.

[138] Comcast Legal Response Center, *Law Enforcement Handbook: Retention Policies, supra* note 24.

[139] *Id.*

storage capacity to retain all this customer data for extended periods of time, so they must purge it frequently,[140] or (2) ISPs are beginning to make small moves towards greater protection of customer's data. These greater protections include frequently deleting this information, similar to an individual clearing his or her browsing history.[141] Both of these are probable explanations. Given the amount of data that ISPs receive daily, it is not feasible to maintain storage for long periods.[142] Moreover, after notable cases such as the FBI's feud with Apple[143] and Yahoo,[144] ISPs have come under scrutiny from customers that companies are not adequately protecting their data.[145]

It is a bit worrisome to leave power in the hands of ISPs to re-write data privacy rules because law enforcement has a vested interest in being able to access identifying information of suspected criminals. Users can "spoof" their IP address to re-route to another address,[146] and ISPs similarly allow users to obtain new

---

[140] *See* Gibson, *supra* note 123, at n.1.

[141] *See* 47 C.F.R. § 64 (evidencing that ISPs will be required by law to ensure some customer data remains private through opt-in and opt-out rules).

[142] While there are no data retention laws in the United States, ISPs generally do not retain customer data for long periods. Some worry this would create a large source of private data that would be enticing to hackers and accidental disclosures. *See* ELEC. FRONTIER FOUND., *Mandatory Data Retention*, https://www.eff.org/issues/mandatory-data-retention (last visited Mar. 2, 2017).

[143] Arash Khamooshi, *Breaking Down Apple's iPhone Fight with the U.S. Government*, N.Y. TIMES (Mar. 21, 2016), https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html.

[144] Andy Greenberg*, How Did The Feds Get Past Yahoo's Encryption? Yahoo!*, WIRED (Oct. 4, 2016, 5:56 pm), https://www.wired.com/2016/10/yahoo-spy-scandal-shows-encryption-fails-without-backbone/.

[145] FCC Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 47 C.F.R. § 64.3 (2016) (explaining this regulation was enacted in response to users' requests for increased protection of their data, specifically in regards to selling customer data).

[146] "Spoofing" is used to disguise IP addresses by re-routing through those trying to determine where the router is to another computer or by providing a false IP address. *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 759 (S.D. Tex. 2013).

IP addresses when they desire.[147] This is similar to clearing your browsing history to remove any Internet searches that may point towards evidence of illegal activity. These methods of concealing identities harm both the ISPs and the government because ISPs use customers' history logs to improve browsing capabilities, provide relevant advertisements, and make other improvements.[148] This also harms government officials because it severely complicates their ability to track criminals online.[149] A workable solution must include compromises on both sides.

But, what other options could ISPs provide to their customers to help them feel secure that their privacy is being protected? It will go beyond fighting the government's desire to have a backdoor into ISP's records.[150] An FCC rule enacted in 2016 allows users to opt-in and opt-out of sharing certain data, showing the possibility that ISPs may request more information from the government when they receive subpoenas for customer information.[151] While the rule did not affect law enforcement

---

[147] *How to Change Your IP Address*, WHATISMYIPADDRESS.COM, http://whatismyipaddress.com/change-ip (last visited Mar. 4, 2017).

[148] *See Privacy Policy: How We Use Information We Collect*, GOOGLE, https://www.google.com/policies/privacy/#infouse (last visited Feb. 16, 2017).

[149] *See, e.g.*, United States v. Christie, 624 F.3d 558, 563 (3d Cir. 2010) (where the government was unable to receive information from an ISP because the ISP had already purged the data).

[150] The geopolitical climate and national security concerns will prevent ISPs from allowing United States law enforcement officials to have a backdoor mechanism into their software, precisely so that they will not have to allow other foreign governments to do the same. *See* Khamooshi, *supra* note 143 (contending that if Apple allowed the United States government to overcome the encryption then they would be hard pressed to deny other countries, such as China, the same access).

[151] But see FCC, Dissenting Statement of Commissioner Ajit Pai on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, (Nov. 2, 2016) https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1.pdf, where, interestingly, the new head of the FCC strongly dissented in the adoption of this Rule. Pai's strongest criticism of the Rule is that ISPs are now subject to stricter regulations than edge providers, such as Google and Yahoo, who are regulated by the Federal Trade Commission. *Id.* at 209. He disagrees with the FCC's justification that ISPs need greater regulation because they have access to a

issues, if search warrants continue to be granted based on IP address information only, it is likely that ISPs will begin to question the probable cause associated with the subpoenas more often.[152] If tension occurs between law enforcement and ISPs, ISPs could begin to request more information from officials or alert customers before they disclose the information sought. This inevitably lengthens the process of receiving information from the ISPs and government officials then run the risk of the data being automatically purged during the discourse. Without that data, the government will presumably lose a large portion of its evidence against the suspect.[153]

"vast sea" of customer data, while edge providers only see a "slice" of this data. *Id.* at 210. This could be a sign that ISPs, moving forward, will not be subject to further regulations that allow customers greater control over how their data is being used. This certainly guarantees a fight between privacy activists and the FCC over how to treat this data, leading to belief that a regulatory alternative may not be politically feasible. Notably, a few months after its enactment, the Senate voted to overturn the Rule. *See* Chris Mills, *ISPs Can Now Sell Your Browsing History Without Permission, Thanks to the Senate*, BGR (Mar. 23, 2017, 1:42PM), http://bgr.com/2017/03/23/fcc-privacy-rules-senate-overturned-ajit-pai/.

[152] *See infra* Section V.B.

[153] *See* United States v. Christie, 624 F.3d 558, 563 (3d Cir. 2010) (where the FBI was unable to subpoena the ISP for customer information because the ISPs no longer had that data saved). A similar situation arose in the Tenth Circuit, notably in a decision authored by Supreme Court nominee Neil Gorsuch, that found the National Center for Missing and Exploited Children's ("NCMEC") action of opening e-mails forwarded to them by AOL was an unconstitutional search under the Fourth Amendment. United States v. Ackerman, 831 F.3d 1292, 1304–07 (10th Cir. 2016). Judge Gorsuch's decision rested on the fact that this was a "warrantless opening and examination of (presumptively) private correspondence" that the Fourth Amendment protects. *Id.* at 1307. The NCMEC is a government entity that receives and investigates tips about possible child trafficking instances, and AOL forwarded a user's e-mail that they suspected contained illegal content. (AOL noticed certain hashes in the e-mail that had been previously associated with child pornography photographs.) The NCMEC opened the attachment to determine if the e-mail had illegal images, which it did. The Tenth Circuit found that NCMEC needed to obtain a warrant before they could open the attachments, which seems to put NCMEC's ability to investigate at a disadvantage and could hinder the efficiency and effectiveness of their work. Interview by Steven Baker, *Steptoe Cyberlaw Podcast: Interview with Jason Healey*, STEPTOE & JOHNSON LLP (Feb. 6, 2017)

V. INVASION OF PRIVACY CONCERNS

Some of the current investigative tools law enforcement officials use raise privacy concerns. Some courts espouse the viewpoint that "[l]aw enforcement cannot afford to be hamstrung by technologically creative criminals,"[154] conceivably suggesting that greater deference will be given to investigative techniques regardless of privacy intrusions. This section presents the privacy concerns created by signal monitoring devices, as seen in Section III, and analyzes a new malware technique used by the FBI to obtain IP addresses that edges closer towards an unconstitutional search under the Fourth Amendment.

A. Concerns with Signal Monitoring Devices

First, defendants have alleged that use of signal devices like the Shadow and MoocherHunter is an invasion into a user's private home.[155] While the government tends to view suspects who use a stranger's Wi-Fi network without permission as "virtual trespassers," the defendants generally make the argument that the government is trespassing into their private home.[156] The oft-cited case to support the idea that signal monitoring is an invasion is *Kyllo v. United States*,[157] where officers parked across the street

---

(http://www.steptoecyberblog.com/2017/02/06/steptoe-cyberlaw-podcast-interview-with-jason-healey-2/). This important decision evidences at least one circuit's, and a potential Supreme Court Justice's, willingness "to be skeptical about government authority." *Id.*

[154] United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *6 (C.D. Cal. Aug. 8, 2016) (reasoning this especially applies "when what is at risk is the sexual exploitation and sadistic abuse of children"). This reasoning could also lead to prejudicial views by courts depending on what the crime is. In *Acevedo-Lemus*, the judge suggested that "the unspeakable harm caused by child pornography" was a large factor in the ultimate decision to deny suppression of the evidence obtained using the NIT, whereas other courts have allowed suppression of this evidence. *Id.*

[155] *See generally* United States v. Stanley, 753 F.3d 114, 118-19 (3d Cir. 2014) (explaining Stanley alleged an unconstitutional search occurred when the detective "used the MoocherHunter to trace Stanley's wireless signal back to the interior of his home").

[156] *Id.* at 120.

[157] 533 U.S. 27 (2001).

and used a thermal imager to determine the existence of a marijuana growing operation inside the residence.[158] The scanner showed that certain parts of the defendant's home were unusually warm, leading officers to conclude that high-powered lamps used to grow marijuana were inside.[159] The Supreme Court declared "obtaining [information] by sense-enhancing technology . . . [from the] interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area[] constitutes a search," and therefore the search inside Kyllo's home was unconstitutional.[160]

While this seemingly bright-line rule that use of "sense-enhancing technology" is unconstitutional without a search warrant, the rules have changed when it comes to Internet activity because these signals are projected *outside* the home. *Kyllo*'s reasoning has not been persuasive in court given the growing belief that IP addresses are not private information and the steps necessary to connect to the Internet are not private. This argument is also unlikely to be convincing in the future because courts have routinely used a nuance in Scalia's opinion regarding sensing technology to defend law enforcement's use of these devices — "without physical intrusion."[161]

Moreover, defendants often claim that their criminal activities were conducted within their home, purposefully shielded from the public eye, and should be protected from this type of "search."[162]

---

[158] *Id.* at 29–30.

[159] *Id.*

[160] *Id.* at 34 (internal citations omitted).

[161] *Compare Stanley*, 753 F.3d at 119 (where court upheld use of signal monitoring device to detect Internet signals) *with Kyllo*, 533 U.S. at 34 (where court found use of sense-enhancing technology to obtain information that would otherwise have only been obtainable through physical intrusion into the home was unconstitutional).

[162] *Stanley*, 753 F.3d at 119 ("In effect, Stanley opened his window and extended an invisible, virtual arm across the street to the Neighbor's router so that he could exploit his Internet connection. In so doing, Stanley deliberately ventured beyond the privacy protections of the home, and thus, beyond the safe harbor provided by *Kyllo*."). *But see* United States v. Ackerman, 831 F.3d 1292, 1307 (10th Cir. 2016) (holding that the NCMEC conducted an unconstitutional

Courts have found that intentionally sending out Internet signals in search of a network connection makes these signals public.[163] Additionally, many of the crimes that are conducted on the Internet involve file sharing, which requires projecting not only network signals outside of the home, but also interactions with third parties.[164] These interactions lessen the legitimacy of claims to privacy. It seems that using a computer inside of your home to conduct Internet activity is not enough to insulate a user from law enforcement officials and other monitoring of one's online conduct.

These conclusions seem in accordance with the Supreme Court's precedent in *Kyllo*, but it raises the question of where the line is drawn for law enforcement officials to gather information that otherwise could not be viewed "without physical intrusion." Courts are slow to adapt to the rapidly changing technological world, and lawyers likewise are not well equipped, nor do they have the time and resources, to fully account for the changing landscape of the Internet.[165] The precedent thus far gives law enforcement a broad use of power to "peer inside" a user's home by monitoring signals that, by their very nature, must be projected outside the confines of the private home to conduct activity on the Internet. As these investigations become more intrusive due to the prevailing view that Internet activity is not private, defendants and privacy advocates worry about the future of online privacy.

---

search when they opened previously unopened e-mails forwarded to them by AOL that contained child pornography photographs).

[163] United States v. Broadhurst, No. 3:11-CR-00121-MO-1, 2012 WL 5985615, at *5 (D. Or. Nov. 28, 2012) ("[D]efendant voluntarily sent out a signal to amplify access point signals and attach to third parties' networks with his computer.").

[164] *Stanley*, 753 F.3d at 119-20 ("Stanley made no effort to confine his conduct to the interior of his home. [H]is conduct—sharing child pornography with other Internet users via a stranger's Internet connection—was deliberately projected *outside* of his home, as it required interactions with persons and objects beyond the threshold of his residence.").

[165] Mackey, Schoen & Cohn, *supra* note 104.

B. Concerns with Future Techniques

Criminals have turned to the dark web to evade detection from law enforcement's signal monitoring.[166] Matters inevitably become more complicated when criminals use the dark web to intentionally remain anonymous, leading officials to use techniques that test the limits of Fourth Amendment privacy protections.[167] A sampling of the main privacy concerns that have arisen involve (i) government searches of computers through hacking techniques involving malware and (ii) magistrate judges issuing warrants that are executed nationwide, outside the district in which they were granted.

i. Government "Hacking"

An explanatory example of what the FBI recently did to circumvent this so-called anonymity on the dark web can be seen in the nationwide Playpen cases.[168] A child pornography site known as Playpen was hosted and used on the Tor network[169] where users were anonymous.[170] After receiving a tip from a

---

[166] *Tor: Overview*, *supra* note 37.

[167] These issues include government "hacking," whether a search was conducted on the suspect's computer to retrieve information, and debate about whether the search warrant particularly described the place to be searched. *See generally* Orin Kerr, *Government 'Hacking' and the Playpen Search Warrant*, WASH. POST: VOLOKH CONSPIRACY (Sept. 27, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/09/27/government-hacking-and-the-playpen-search-warrant/.

[168] *See generally* United States v. Matish, 193 F. Supp. 3d 585, 612 (E.D. Va. 2016).

[169] *See generally* Untied States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *1 (C.D. Cal. Aug. 8, 2016). The Tor network, and other dark web browsers, operate differently than ordinary websites that log the IP addresses of visitors after they visit the site. To access the Tor network, "a user must first download and install particular software, which subsequently shields the user's IP address by relaying it among 'nodes'—computers run by volunteers all over the world. When a user visits a website located on the Tor network . . . his actual IP address is not shown. Instead, [the site] can only see the IP address of the Tor 'exit node' – the final relay computer which sent the user's communication to [the site]." *Id.*

[170] *Id.* at *1-2.

foreign informant of the host's IP address, the FBI located the host and used his connection to infiltrate the computers of the other anonymous users.[171] The FBI used a "Network Investigative Technique" ("NIT") to send malware to users who accessed the website by running the site for a short period of time.[172] Once the user logged into the site and downloaded content, the malware was subsequently downloaded with the selected image.[173] This malware allowed the FBI to obtain IP addresses of users and later obtain home addresses after subpoenaing their ISP.[174] Federal courts across the nation have declared the use of the NIT was legal, despite vocal privacy advocates who have declared this was an illegal search and seizure.[175]

Defendants who were subject to the FBI's NIT allege that by sending them the malware to identify their IP addresses, the FBI conducted a Fourth Amendment search of their device because the malware was programmed to "search" their computer for this information.[176] This is an important assertion that most courts who heard these cases tended to brush aside.[177] It is well established that users do not have a reasonable expectation of privacy in their IP address because invariably they disclose it at least once to access the web.[178] The NIT created a different situation though. While the Tor users disclosed their IP address to the first node host, the FBI did not obtain the userss IP address from those hosts, or from the ISP as was done in the cases in Section III.[179] This is an important distinction because, rather than subpoenaing the third party for the IP address, the FBI obtained the IP address only after they installed a program on the suspect's computer that then

---

[171] *Id.* at *2-3.
[172] *Id.* at *2-4.
[173] *Id.* at *2.
[174] *Id.* at *5.
[175] *Acevedo-Lemus*, 2016 WL 4208436, at *4.
[176] *Id.* at *5.
[177] *See generally id*.
[178] *Tor: Overview*, *supra* note 37.
[179] United States v. Allain, 2016 WL 5660452, at *13 n.5 (D. Mass. Sept. 29, 2016).

searched through the computer for the address.[180] Therefore, the FBI searched the contents of the suspects' computers.[181] Some courts have said that the initial disclosure of the IP address to the first node renders the address non-private information.[182] Therefore, it does not matter how the FBI obtained this non-private information, even if it involved a warrantless search.[183] The initial disclosure is all that matters to render a warrant unnecessary.[184] Once law enforcement officials can "search" computers for specific information without a warrant, whether it is private information or not, there is no telling how far this broad grant of power could extend.[185]

---

[180] *Id*. ("The FBI's search not only implicated defendant's privacy interest in his IP address, but also in his computer.").

[181] *Id*.; *but see Acevedo-Lemus*, 2016 WL 4208436, at *6.

[182] United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *4 (C.D. Cal, Aug. 8, 2016).

[183] *Acevedo-Lemus*, 2016 WL 4208436, at *6 ("[A] necessary aspect of Tor is the initial transmission of a user's IP address to a third-party—the operator of the initial Tor node—and the fact that a user's IP address is subsequently bounced from node to node within the Tor network to mask his identity does not alter the analysis of whether he had an actual expectation of privacy in that IP address, which he had initially disclosed to a stranger.") (internal citations omitted); *but see* Kerr, *Government 'Hacking'*, *supra* note 165 (arguing that Tor users do not voluntarily share their IP addresses with the websites they visit, and so it does not matter that obtaining an IP address in other situations would not be a search, it was a search in these cases because it was the "absence of voluntarily sharing . . . [that] led the government to surreptitiously obtain the information using the NIT" in the first place).

[184] *Acevedo-Lemus*, 2016 WL 4208436, at *6.

[185] *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013). The court denied a warrant request to install software designed to extract certain stored electronic records and generate photographs and location information over a thirty-day period, which amounted to simply "a warrant to hack a computer suspected of criminal use." The government failed to assure the court that only information of the suspected criminals would be gathered and did not address various concerns such as whether the suspects used public computers, whether it belonged to family members who were not involved in the illegal scheme, whether a counterfeit address was being used, and whether the e-mail address was accessed on more than one computer. *Id.* at 759-60. Additionally, "[s]ome privacy advocates and analysts worry that in doing so, investigators may also wind up hacking and

On the one hand, this type of "hacking" may be necessary in the world of the dark web where criminals go to great lengths to remain undetected.[186] One court dealing with the Tor network stated, "the government should be able to use the most advanced technological means to overcome criminal activity that is conducted in secret."[187] However, the steps government officials have already taken seem to be pushing the limit. What if the FBI, in addition to searching for the IP address, was also able to access credit card information, social security numbers, and other personally identifying information from their "search" of the suspect's computer? As the NIT was used, personally identifying information was not searched for per se, and so the suspects' names and addresses were obtained from a subpoena to the ISP associated with the IP address found using the malware.[188] It is not difficult to imagine a situation where law enforcement could easily program the malware to search for even one piece of identifying information, such as to obtain access to passwords the suspect used for various sites. In one Playpen case, the FBI filed for voluntary dismissal of charges against the Defendant because they did not want to reveal the details of the malware they used to hack into the

---

identifying the computers of law-abiding people who are seeking to remain anonymous, people who can also include political dissidents and journalists." Ellen Nakashima, *This Is How the Government is Catching People Who Use Child Porn Sites*, WASH. POST: NATIONAL SECURITY (Jan. 21, 2016), https://www.washingtonpost.com/world/national-security/how-the-government-is-using-malware-to-ensnare-child-porn-users/2016/01/21/fb8ab5f8-bec0-11e5-83d4-42e3bceea902_story.html.

[186] Nakashima, *supra* note 185 ("Without using the hacking technique, officials said, it would be very difficult to locate pedophiles who go to great lengths to hide their tracks.").

[187] *Acevedo-Lemus*, 2016 WL 4208436, at *6 (quoting United States v. Matish, 193 F. Supp. 3d 585, 621 (E.D. Va. 2016)).

[188] *Id.* at *2. *But see* United States v. Croghan, 2016 WL 4992105, at *7 (S.D. Iowa Sept. 19, 2016) (explaining the judge found defendants had a reasonable expectation of privacy in the *location* where the IP address was stored; therefore, the government needed a valid search warrant to obtain this information directly from their home computers, despite the fact that defendants did not have a reasonable expectation of privacy in the information that was gathered).

Tor network during discovery.[189] This seems to create problems for both parties involved as the public would like to know what techniques law enforcement is using, but there is also an interest in keeping some aspects private so criminals cannot surpass detection techniques. The more access law enforcement has to private information without a warrant, the closer they move towards conducting an unconstitutional search.

On the other hand, if law enforcement officials are not able to obtain this information using malware (or another similar method), they may turn to third parties who are able get the information,[190] granting access to this information to more parties in addition to law enforcement. For example, the FBI enlisted the help of a third-party company when Apple refused to unlock the phone of the suspect in the San Bernardino attack.[191] Privacy experts have been vocal about preventing any "back door" mechanism for the government to bypass encryption and password protection methods, fearing that this will allow the government to have unfettered access to information.[192] In the changing cyber world, courts are struggling to address the interconnectivity of all users. Using malware is a direct way courts allow law enforcement to access criminals online, but a procedurally important aspect has risen to the surface as well: the territorial reach of warrants for searching Internet activity.

---

[189] Lily Hay Newman, *The Feds Would Rather Drop a Child Porn Case Than Give Up a Tor Exploit*, WIRED (Mar. 7, 2017), https://www.wired.com/2017/03/feds-rather-drop-child-porn-case-give-exploit/.

[190] Arjun Kharpal, *Apple vs FBI: All You Need to Know*, CNBC: CYBERSECURITY (Mar. 29, 2016 6:34AM), http://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html (reporting that the FBI found a third party who was able to unlock the phone for them).

[191] *Id.*

[192] Khamooshi, *supra* note 143.

ii. Legality of Warrants for All Users on a Website with Illegal Content

The other main issue in the Playpen cases dealt with the legality of the warrant issued to use the NIT.[193] A magistrate judge in the Eastern District of Virginia issued a warrant, but the malware was used—via downloading by users on the website—all across the country.[194] Under Federal Rule of Criminal Procedure 41, a magistrate judge "has authority to issue a warrant to search for and seize a person or property located within the district."[195] The FBI allowed the malware to be downloaded on thousands of computers outside the Eastern District of Virginia, outside the legally admissible jurisdiction.[196] Some courts found the warrant was valid, despite users being outside the Eastern District of Virginia, reasoning that the users made "a virtual trip via the Internet to Virginia" putting them within the reach of the warrant to be a legal search.[197] This is a broad construction of the warrant's jurisdiction and a view not all courts have been ready to follow.[198]

Other courts found the NIT being downloaded outside the Eastern District of Virginia was a Rule 41 violation.[199] As a result, these courts were compelled to suppress the evidence found using the NIT because it violated the Fourth Amendment.[200] Even though

---

[193] *Croghan*, 2016 WL 4992105, at *2 ("The Court notes that the NIT Warrant at issue in this case has resulted in a great deal of litigation across the country. The numerous district courts to consider motions similar to the present Motions to Suppress have reached varying conclusions on the legal issues at play.").

[194] *Id.* at 4.

[195] F.R. Crim. P. 41(b)(1).

[196] Nakashima, *supra* note 185; *see generally Croghan*, 2016 WL 4992105, at *5 (holding that the government's NIT warrant violated Federal Rule of Criminal Procedure 41 because it targeted information that was outside of the Eastern District of Virginia); United States v. Michaud, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016) (finding the NIT warrant "technically violates the letter [of Rule 41(b)], but not the spirit").

[197] United States v. Matish, 193 F. Supp. 3d 585, 612 (E.D. Va. 2016).

[198] *Croghan*, 2016 WL 4992105, at *7; United States v. Levin, 186 F.Supp.3d 26, 35 (D. Mass. 2016).

[199] *Id.* at 5. Rule 41 of the Federal Rules of Criminal Procedure governs search and seizure. FED. R. CRIM. P. 41.

[200] *Id.* at 8.

the government argued that "suppression [was] too extreme a remedy" and undoubtedly was a "victory" for the defendant who illegally downloaded child pornography, the court found the evidence obtained in the violation was simply too prejudicial to be admissible.[201] The IP addresses of defendants would not have been obtained but for the malware being sent outside of the magistrate's jurisdiction. The government often argues that this is a ministerial violation, but courts have found this to be a procedural violation that involved "substantial judicial authority."[202] In essence, "the magistrate judge lacked authority, and thus jurisdiction" to issue the warrant, rendering it invalid.[203]

The disagreement regarding jurisdictional limits of search warrants for information regarding technological devices poses a problem because defendants who were subject to the *same search warrant* from accessing the *same website* are being treated differently across the nation, raising judicial uncertainty for defendants. Recently, Rule 41 of the Federal Rules of Criminal Procedure was amended to address these concerns.[204] The amendments allow a magistrate judge "to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located *within or outside that district* if . . . the media . . . has been concealed through technological means [] or . . . [is] located in five or more districts."[205] These amendments establish the NIT warrant was valid because the rule allows warrants to reach beyond the jurisdiction where they are issued. However, even though courts prior to these amendments acknowledged that a "potent investigative technique" such as the NIT could someday be authorized under Rule 41, the privacy rights of individuals must still be respected with the "extremely intrusive nature of such a

---

[201] *See id.* at 6; *Levin*, 186 F. Supp. 3d at 35.

[202] *Levin*, 186 F. Supp. 3d at 36.

[203] *Id.*

[204] THE COMMITTEE ON THE JUDICIARY HOUSE OF REPRESENTATIVES, FEDERAL RULES OF CRIMINAL PROCEDURE, (Dec. 16, 2016), http://www.uscourts.gov/sites/default/files/rules-of-criminal-procedure.pdf (adopted December 16, 2016).

[205] *Id.* (emphasis added).

search."[206] As a clear standard of what law enforcement officials can do in online searches is being established, it is important that Fourth Amendment privacy concerns are protected.

VI. CONCLUSION

IP addresses are useful for locating criminals and provide a stepping-stone for launching subsequent investigations. Nevertheless, judges should persist to request more specific information before granting search warrants. With the advent of freely available information regarding users' online conduct, it is not unduly burdensome for officials to obtain additional information to support pending searches. With an IP address, for example, officials can first subpoena the ISP for customer information which can then be used to corroborate a suspect's online identity. From there, signal monitoring devices can be used to observe where the suspected online conduct originates. These additional steps are necessary to ensure proper judicial prudence when conducting new investigations.

As techniques become more intrusive, both officials and users must be wary about privacy concerns. Users must take extra steps to ensure their networks are secured and should actively check to see if any unauthorized users are accessing their network. Additionally, law enforcement officials carry a heavy burden themselves and must tread carefully so as not to cross into unconstitutional search territory. IP addresses do not always provide concrete details about a suspect's identity, so caution should be used when invasive techniques are used to obtain a suspect's IP address. As seen in cases where criminals use dark web browsers, IP addresses can easily be relayed among various different computers across the country or can be re-routed to another device. Officials should be hesitant to use invasive techniques to obtain this information, as it could prove fruitless to their search, particularly given some courts' decisions to suppress

---

[206] *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F.Supp.2d 753, 761 (S.D. Texas 2013).

evidence because legal procedures were not followed.[207] Similarly, if officials successfully bring charges against a suspect but are compelled to reveal specific details about their search techniques, they may choose to dismiss the criminal charges against the suspect, rather than have to reveal their method.[208] These concerns, among others, are shaping a new landscape for investigating criminal activity online. IP addresses alone should not provide sufficient probable cause to obtain a search warrant given their unreliable nature.

[207] *See, e.g.*, United States v. Croghan, No. 1:15-cr-48, 2016 WL 4992105, at *6 (S.D. Iowa Sept. 19, 2016); *Levin*, 186 F. Supp. 3d at 35.
[208] *See* Newman, *supra* note 189.