Note

Incognito Mode Is in the Constitution

*Travis Panneck**

"Visibility is a trap."[1]

INTRODUCTION

The Dread Pirate Roberts was apprehended not on the high seas but in the stacks of the San Francisco Public Library.[2] "Dread Pirate Roberts"[3] (DPR) was the name adopted by an internet user who had created and maintained the Silk Road, an online black market where users could buy and sell illicit drugs, medical supplies, and even Thai energy drinks.[4] After a lengthy investigation[5] involving fake identities, a staged torture, and a trip to Iceland,[6] the FBI believed that they had identified the man behind the moniker: Ross William Ulbricht.

* J.D. Candidate, 2020, University of Minnesota Law School. Thanks to Professor Kevin Reitz and the editors and staffers of the *Minnesota Law Review* for comments, suggestions, and diligent editorial work. All remaining mistakes are my own.

1. MICHEL FOUCAULT, DISCIPLINE & PUNISH: THE BIRTH OF THE PRISON 200 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977).

2. Natasha Bertrand, *The FBI Staged a Lovers' Fight To Catch the Kingpin of the Web's Biggest Illegal Drug Marketplace*, BUS. INSIDER (Jan. 22, 2015), https://www.businessinsider.com/the-arrest-of-silk-road-mastermind-ross-ulbricht-2015-1 [https://perma.cc/G6A6-CWC4].

3. The name derives from the fictional character from The Princess Bride who turns out to be not one man, but several who pass the identity to successors to maintain a fearsome reputation. *See* THE PRINCESS BRIDE (20th Century Fox 1987) ("I am not the Dread Pirate Roberts . . . . My name is Ryan; I inherited the ship from the previous Dread Pirate Roberts, just as you will inherit it from me. The man I inherited it from is not the real Dread Pirate Roberts either.").

4. *See 15 Things You Could Have Purchased on Silk Road*, COMPLEX (Oct. 3, 2013), https://www.complex.com/pop-culture/2013/10/silk-road/ [https://perma.cc/9DG9-DHTJ].

5. For a narrative account of this investigation and the capture of Ulbricht, see generally NICK BILTON, AMERICAN KINGPIN: THE EPIC HUNT FOR THE CRIMINAL MASTERMIND BEHIND THE SILK ROAD (2017).

6. Joshuah Bearman, *The Rise & Fall of Silk Road, Part 2: The Fall*,

Leading up to Ulbricht's arrest, the government tried to associate Ulbricht with the DPR moniker and the Silk Road by warrantlessly collecting information about his internet use.[7] Using "pen registers" and "trap and trace" devices to monitor Ulbricht's home router, the government obtained detailed information about Ulbricht's internet activity, including dates and times of use, duration of use, and other connection data.[8] Without ever having to show probable cause, the government peered into Ulbricht's daily internet use and built its case against him.[9] On the basis of this comprehensive and intrusive internet surveillance, the government obtained a warrant for Ulbricht's arrest.[10] Law enforcement seized Ulbricht and his laptop at the public library while he allegedly was working on the Silk Road.[11] Ulbricht was tried, convicted, and sentenced to two life sentences.[12] His conviction was affirmed on appeal.[13]

It is not merely masterminds of online marketplaces for drugs that should be worried about surveillance of internet use.[14] Online companies currently hold massive amounts of information about their users that is comprehensive and accurate;[15] rarely do people attempt to deceive their own computer

WIRED (June 2015), https://www.wired.com/2015/05/silk-road-2/ [https://perma.cc/945R-PEHX].

7. Petition for Writ of Certiorari at 5, Ulbricht v. United States, 138 S. Ct. 2708 (2018) (No. 17-950), 2017 WL 6812114, at *5.

8. *Id.* at 5–6, 2017 WL 6812114, at *5–6.

9. *Id.* at 5–6, 2017 WL 6812114, at *5–6.

10. *Id.* at 6–7, 2017 WL 6812114, at *6–7.

11. *See* Bertrand, *supra* note 2.

12. *See* Katherine Mangu-Ward, *Ross Ulbricht Is Serving a Double Life Sentence*, REASON (July 2018), https://reason.com/2018/05/31/ross-ulbricht-is-serving-a-dou [https://perma.cc/84F2-K8QZ]. The minimum sentence was ten years. *Id.*

13. United States v. Ulbricht, 858 F.3d 71, 90 (2d Cir. 2017), *cert. denied*, 138 S. Ct. 2708 (2018).

14. Consider, for example, six anonymous commenters that dared to express displeasure with Judge Katherine Forrest's decision in Ulbricht's case. The blog on which those comments appeared was served with a grand jury subpoena for "any and all identifying information" about those commenters. *See* Nick Gillespie & Matt Welch, *How Government Stifled Reason's Free Speech*, REASON (June 19, 2015, 5:08 PM), https://reason.com/2015/06/19/government-stifles-speech/ [https://perma.cc/4ZUF-NLCF].

15. *See, e.g.*, Dylan Curran, *Are You Ready? Here Is All the Data Facebook and Google Have on You*, GUARDIAN (Mar. 30, 2018), https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy [https://perma.cc/7Q28-A823].

about what they are looking for or communicating about online. As Bruce Schneier put it: "No one ever lies to a search engine."[16]

Though many are aware of the massive records held by companies like Facebook and Google, Professor Paul Ohm has argued that the information held by internet service providers alone could be used to "compile a detailed record of thoughts and behavior," getting lists of what you "read, watch, buy, and borrow."[17] The potential for harm arising from access to this information, Ohm says, is "limited only by the wickedness of one's imagination."[18] While current United States law requires a warrant when the government seeks the "contents" of internet communications,[19] this may not in practice limit the government from discovering the content via other forms of internet history that are less protected under the law.[20] The Supreme Court's revolutionary decision in *Carpenter v. United States*[21] presents a new way forward that safeguards legitimate privacy interests in internet activity while still allowing law enforcement to police the internet's worst members.

This Note will argue that *Carpenter* heralds a new approach to Fourth Amendment searches that courts can and should apply to law enforcement's collection of non-content internet history and basic subscriber information. Part I will explain the traditional approach to applying the Fourth Amendment to law enforcement acquisition of internet history. Then, Part I will lay out the decision in *Carpenter* and how the Court's approach to the Fourth Amendment appears to have shifted. Part II will show that lower courts do not presently appear to be responding

16. Liz Mineo, *On Internet Privacy, Be Very Afraid*, HARV. GAZETTE (Aug. 24, 2017), https://news.harvard.edu/gazette/story/2017/08/when-it-comes-to-internet-privacy-be-very-afraid-analyst-suggests/ [https://perma.cc/5HZX-C9A9].

17. Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1445 (2009).

18. *Id.* at 1444.

19. *See* 18 U.S.C. § 2703(b) (2012). For a discussion of how law enforcement collects various forms of internet history, see *infra* Part I.C.

20. *See* Saul Hansell, *One Subpoena Is All It Takes To Reveal Your Online Life*, N.Y. TIMES: BITS (July 7, 2008), https://bits.blogs.nytimes.com/2008/07/07/the-privacy-risk-from-the-courts/ [https://perma.cc/KBH9-Q5RZ] ("[W]ith a subpoena, the Internet provider can be forced to identify which of their customers was assigned a particular I.P. address at a particular time. That is how the recording industry has been identifying and suing people who use file sharing programs.").

21. 138 S. Ct. 2206 (2018).

to this shift, restricting the reasoning in *Carpenter* to the narrow set of facts before the Court in that case. Part II will also demonstrate that the current limitations on the collection of internet history are insufficient and illustrate how a failure to accord greater protections threatens privacy. Finally, Part III will posit that courts can and should extend *Carpenter*'s reasoning to cover non-content internet history and subscriber information. Part III will further suggest that courts should ultimately require that law enforcement seeking to collect these data obtain a warrant founded on probable cause.

I. THE FOURTH AMENDMENT AND THE LAW SURROUNDING COLLECTION OF INTERNET HISTORY

The use of the internet produces massive amounts of information,[22] much of which may be of interest to law enforcement seeking to root out crime. Law enforcement must, however, abide by the Fourth Amendment, which protects against "unreasonable searches and seizures."[23] "Searches" is a term of limitation, meaning that the Fourth Amendment does not reach conduct that is not a "search."[24] Where a Fourth Amendment "search" does not occur, there is no constitutional requirement that police conduct be reasonable. While Congress is free to set up additional protections for citizens against actions of law enforcement,[25] the Constitution does not hamstring law enforcement conduct that is not a search.

This Part will describe how the government can currently collect information about a criminal suspect's internet history and a recent development in Fourth Amendment jurisprudence that may require changes in these established methods. First, Section A will describe the different types of history a user generates when they use the internet. Next, Section B will provide the constitutional backdrop for government collection of internet history, including a description of the law of searches and an important exception, the third-party doctrine. Section C will then describe how this law is applied in practice, showing the application of the third-party doctrine to internet history and subscriber information. Finally, Section D will describe *Carpenter v.*

22. *See* Josh James, *Data Never Sleeps 6.0*, DOMO (June 5, 2018), https://www.domo.com/blog/data-never-sleeps-6/ [https://perma.cc/C9M2-DMTR].

23. U.S. CONST. amend. IV.

24. *See, e.g.*, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 356 (1974).

25. Limited of course by their constitutional ambit.

United States, a recent Supreme Court decision that may upend how the government collects a criminal suspect's internet history.

A. THE CREATION AND STORAGE OF INTERNET HISTORY

When someone uses the internet, a great deal of history about their session is created and stored. The internet is a set of protocols that allows computers to communicate with each other.[26] For example, if DPR wants to access a webpage on the internet, DPR's computer needs to know where the webpage is and what the webpage contains.

To identify where a webpage lives on the internet, computers must be able to find each other. To accomplish this, each computer connected to the internet is given an Internet Protocol (IP) address. IP addresses "are the unique numbers assigned to every computer or device that is connected to the Internet."[27] Users typically obtain IP addresses through internet service providers (ISPs).[28] Buying an internet connection generally entails communicating basic subscriber information to an ISP, which may include the user's real name, address, email addresses, and credit card or bank numbers. ISPs obtain allocations of IP addresses from registries, which they then assign to users that buy connections to the internet from them.[29] Usually, these IP addresses are dynamic—the home user's IP address can change

26. *See generally* Aaron Titus, *How the Internet Works in 5 Minutes*, YOUTUBE (Feb. 18, 2009), https://www.youtube.com/watch?v=7_LPdttKXPc (explaining the basic structure of the internet).

27. ICANN, BEGINNER'S GUIDE TO INTERNET PROTOCOL (IP) ADDRESSES 2 (2011), https://www.icann.org/en/system/files/files/ip-addresses-beginners-guide-04mar11-en.pdf [https://perma.cc/C9UQ-LDRM]. The use of "unique" here may not be entirely accurate. As noted later in this paragraph, IP addresses can change upon connection to the internet. Because there are a limited number of IP addresses, this can lead to situations where an internet service provider (ISP) may allocate an IP address to a user that has already been assigned before or is currently in use by another user. This Note is concerned with the situation where an IP address has provided reliable information about a user. But it is important to realize that the use of IP addresses as an investigative tool at all is itself fraught. *See* AARON MACKEY ET AL., ELECTRONIC FRONTIER FOUND., UNRELIABLE INFORMANTS: IP ADDRESSES, DIGITAL TIPS AND POLICE RAIDS (2016), https://www.eff.org/files/2016/09/22/2016.09.20_final_formatted_ip_address_white_paper.pdf [https://perma.cc/57TM-ABWH].

28. *See Number Resources*, INTERNET ASSIGNED NUMBERS AUTHORITY, https://www.iana.org/numbers [https://perma.cc/NV99-VUWC].

29. *See id.*

each time they connect to the internet.[30] Registries keep track of which IPs they issue to which ISPs, such that if a person knows an IP address, they can determine which ISP issued that address.[31] Information about which ISP issued which IP address is publicly available.[32]

IP addresses are 32-bit numbers expressed as a "dotted decimal number," like so: 162.241.16.20.[33] Perhaps because people have trouble remembering long strings of numbers,[34] computers (most often servers providing websites) can be given "domain names."[35] Domain name servers (DNS) may then be used to associate a domain name with an IP address.[36] For example, querying a DNS would tell a user that minnesotalawreview.org is, as of this writing,[37] located at 162.241.16.20.

But an IP address and domain name can only tell a user on which website a webpage lives, not what is on the webpage. A more specific address, called a uniform resource locator (URL), is used to direct a computer to a specific piece of content on the internet, such as a particular webpage.[38] URLs are displayed in

30. *See* Jeff Tyson, *How Internet Infrastructure Works*, HOWSTUFFWORKS (Apr. 3, 2001), https://computer.howstuffworks.com/internet/basics/internet-infrastructure9.htm [https://perma.cc/KR7P-S8BX]. Some users that seek to run servers will obtain a "static" IP address that does not change. *Id.*

31. *See* AM. REGISTRY FOR INTERNET NUMBERS, https://www.arin.net [https://perma.cc/EX89-Z7SH].

32. *See id.*

33. ICANN, *supra* note 27, at 5. Note that not *all* IP addresses take this form. *See id.* IPv4 addresses look like this, but ISPs and other network operators are switching to IPv6 because IPv4 can only support just over four billion devices. *Id.* IPv6 addresses are 128-bit numbers that take the form 2001:0db8:0000:0000:0000:0000:0000:0053. *Id.* IPv6 supports more devices, having a capacity of 340 undecillion addresses. *Id.*

34. *See, e.g.*, Lauren Schenkman, *In the Brain, Seven Is a Magic Number*, ABCNEWS (Dec. 6, 2009), https://abcnews.go.com/Technology/brain-memory-magic-number/story?id=9189664 [https://perma.cc/H8J8-PHRL] ("[O]n average, the longest sequence a normal person can recall on the fly contains about seven items.").

35. *See Web Terms 101: The Difference Between a URL, Domain, Website, and More.*, GOOGLE DOMAINS, https://domains.google/learning-center/web-terms-101/ [https://perma.cc/EP5T-8WR4].

36. *See DNS and WHOIS – How It Works*, ICANN WHOIS, https://whois.icann.org/en/dns-and-whois-how-it-works [https://perma.cc/3QV8-ZNXT] (last updated July 2017).

37. Website accessed on October 14, 2019.

38. *See* Tim Berners-Lee, *Universal Resource Identifiers in WWW*, WORLD WIDE WEB CONSORTIUM, https://www.w3.org/Addressing/URL/uri-spec.html [https://perma.cc/9XSD-V9YP].

the "address bar" of most web browsers and may look like this: https://www.minnesotalawreview.org/2017/11/21/carpenter-iphone-fourth-amendment/. URLs will usually include the domain name (minnesotalawreview.org) and additional text directing the computer to serve a specific piece of content (/2017/11/21/carpenter-iphone-fourth-amendment/). Once a computer requests content from a URL, that content is divided into packets, which are then reassembled to deliver the content on the destination computer.[39]

This internet traffic is directed through ports.[40] A port "is a type of electronic, software- or programming-related docking point through which information flows from a program on your computer or to your computer from the Internet or another computer in a network."[41] Some types of internet traffic, like email and hypertext (what most webpages use), receive specific port numbers to identify and direct the internet traffic, such that the information is only available through that port.[42] These reserved ports might be thought of as filters that only allow one type of content through. To continue the example from above, web browsers accessing the *Minnesota Law Review* webpage will "ask" to receive information through port 80, the port number reserved for hypertext transfer (represented as 162.241.16.20:80). If a request is made on port 80 to see the *Law Review*'s webpage, it will succeed. Trying to access the page through a port reserved for some other type of content, like port 17 (represented as 162.241.16.20:17), which is reserved for servers providing quotes of the day, would fail: the computer hosting the webpage would reject the request.

ISPs can see (and therefore collect) most of this information.[43] Despite efforts to encrypt connections to reduce visibility of this information, ISPs can see domain names and may also

39. *See What Is a Packet?*, HOWSTUFFWORKS (Dec. 1, 2000), https://computer.howstuffworks.com/question525.htm [https://perma.cc/398L-VQNM].

40. *See What Is a Port?*, WHATISMYIPADDRESS.COM, https://whatismyipaddress.com/port [https://perma.cc/G7KD-WCJF].

41. *Id.*

42. *See id.*

43. *See* Aaron Rieke et al., *What ISPs Can See*, UPTURN (Mar. 2016), https://www.upturn.org/reports/2016/what-isps-can-see/ [https://perma.cc/3BYE-WHUY]. Servers of individual websites can also track information like which IP addresses visit which aspects of their website at what times of day. *See, e.g.*, *Log Files*, APACHE HTTP SERVER PROJECT, https://httpd.apache.org/docs/1.3/logs.html [https://perma.cc/XU25-TJ9Y]. However, owners of servers

be able to see URLs and content that users visit.[44] URLs and content can reveal sensitive information about a user, including health problems, debts, and consumer product preferences.[45] Domain names and IP addresses may be less revealing, but collectively may give substantial insight into a person's personal predilections.

While a history of the IP addresses that a user visits can be revealing, the user's *own* IP address may also provide information about them. An IP address may provide a rough sense of location, and ISPs certainly know which user they have given which IP address.[46] Though the accuracy will vary user to user, IP addresses could be used as a location-tracking tool.[47]

All this information is potentially reachable and useful to law enforcement. If law enforcement comes across an IP address accessing contraband, they might ask an ISP to provide information about who they issued that IP address to.[48] Law enforcement suspecting someone of accessing certain websites containing contraband might install a device to track which websites a person accesses.[49] In some cases, law enforcement may want to request all of a person's communications over Facebook or Twitter to find evidence of a crime.[50] To determine whether any or all of this conduct triggers Fourth Amendment protections, one

are less likely to have access to the real name, address, and other identifying information associated with a user's IP address. *See id.*

44. *See* Rieke et al., *supra* note 43.

45. *Id.*

46. *See How Your IP Address Could Lead Anyone to Your Front Door*, WHATISMYIPADDRESS.COM, https://whatismyipaddress.com/find-me [https://perma.cc/XRW8-3EE3].

47. *See, e.g.*, Brief for Defendant-Appellant at 118–20, United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2017) (No. 15-1815), *cert. denied*, 138 S. Ct. 2708 (2018), 2016 WL 158389, at *118–20.

48. *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1199 (10th Cir. 2008) ("Pennsylvania authorities obtained another disclosure order requiring Cox to provide the subscriber information for that IP address.").

49. *See, e.g.*, *Ulbricht*, 858 F.3d at 95 ("[T]he government used five pen registers and trap and trace devices to monitor IP addresses associated with Internet traffic to and from Ulbricht's wireless home router and devices that regularly connected to that router.").

50. *See, e.g.*, United States v. Brewer, No. 4:18-CR-215-CDP-NAB, 2018 WL 7114606, at *1 (E.D. Mo. Dec. 12, 2018) ("Detective Burton learned that the arrangements for the sale of the heroin or fentanyl had been made through Facebook Messenger. The detective then applied for a search warrant . . . ."), *report and recommendation adopted*, No. 4:18CR00215 SNLJ, 2019 WL 319402 (E.D. Mo. Jan. 24, 2019).

must gaze into the Fourth Amendment law surrounding searches and seizures, an area of law that "has not—to put it mildly—run smooth."[51]

B. THE FOURTH AMENDMENT AND THE THIRD-PARTY DOCTRINE

The modern test for when government conduct amounts to a Fourth Amendment search was first formulated in *Katz v. United States*.[52] In *Katz*, the Court held that law enforcement had conducted a Fourth Amendment search when they bugged a public payphone.[53] Recognizing that the Fourth Amendment protected "people, not places,"[54] the Court rejected an earlier approach to the Fourth Amendment under cases like *Olmstead v. United States*, which required an invasion of a property interest for a Fourth Amendment search to occur.[55] Justice Harlan's concurrence, later adopted by the Court in full,[56] set out a two-prong test for when government collection of information constituted a search: (1) the person must exhibit a subjective expectation of privacy in the information; and (2) the expectation of privacy must be one that "society is prepared to recognize as 'reasonable.'"[57]

The Supreme Court has recognized a notable exception to the *Katz* test in the third-party doctrine.[58] The doctrine provides

51. Chapman v. United States, 365 U.S. 610, 618 (1961) (Frankfurter, J., concurring).

52. 389 U.S. 347 (1967).

53. *Id.* at 353.

54. *Id.* at 351.

55. *Id.* at 352; *see also* Olmstead v. United States, 277 U.S. 438 (1928), *overruled by Katz*, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967). The Court has recently revived this approach to the Fourth Amendment, with the late Justice Scalia being the most fervent advocate of the claim that *Katz* did not overrule this line of cases, but merely added additional protections. *See, e.g.*, Florida v. Jardines, 569 U.S. 1, 5 (2013) ("[T]hough *Katz* may add to the baseline, it does not subtract anything . . . ."); United States v. Jones, 565 U.S. 400, 408 (2012) ("*Katz* did not narrow the Fourth Amendment's scope."). Justice Gorsuch has also expressed sympathy for this approach. *See* Carpenter v. United States, 138 S. Ct. 2206, 2267–68 (2018) (Gorsuch, J., dissenting) ("[T]he traditional approach asked if a house, paper or effect was *yours* under law. . . . Though now often lost in *Katz*'s shadow, this traditional understanding persists.").

56. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 740 (1979) (using Justice Harlan's two-step formulation to frame the Fourth Amendment analysis).

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

58. For a more complete overview of the third-party doctrine background

that "if information is possessed or known by third parties, then, for purposes of the Fourth Amendment, an individual lacks a reasonable expectation of privacy in the information."[59]

The first cases to recognize this limitation to Fourth Amendment protections were cases that concerned the use of undercover informants, wires, and eavesdropping. Prior to *Katz*, the Court held in *On Lee v. United States* that there was not a Fourth Amendment problem with being informed upon by a friend wearing a wire.[60] In *On Lee*, Lee was selling opium from his laundry in Hoboken.[61] Lee had a conversation about the opium with his friend, who turned out to be wearing a wire and acting as an undercover informant for the Bureau of Narcotics.[62] The Court found that because the "friend" had entered with the consent of Lee, there was no Fourth Amendment violation.[63] Three cases following *On Lee* confirmed that there was no Fourth Amendment search when a suspect voluntarily disclosed information to an undercover informant.[64]

Following *Katz*, the Court reassessed the question of whether undercover informants violated the Fourth Amendment. After all, wiretapping and electronic eavesdropping did not violate the Fourth Amendment under the *Olmstead* regime because there had been no "official search" nor a "physical invasion."[65] Yet, in *United States v. White*, the Court found that, despite the change to the "reasonable expectation of privacy" test,

prior to *Carpenter*, see Monu Bedi, *The Fourth Amendment Disclosure Doctrines*, 26 WM. & MARY BILL RTS. J. 461 (2017); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV 561, 567–70 (2009).

59. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528 (2006).

60. On Lee v. United States, 343 U.S. 747 (1952).

61. *Id.* at 748–49.

62. *Id.* at 749.

63. *Id.* at 753–54.

64. *See* Hoffa v. United States, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."); Lewis v. United States, 385 U.S. 206, 209 (1966) ("[I]n the detection of many types of crime, the Government is entitled to use decoys and to conceal the identity of its agents."); Lopez v. United States, 373 U.S. 427, 439 (1963) ("We think the risk that petitioner took in offering a bribe to Davis fairly included the risk that the offer would be accurately reproduced in court, whether by faultless memory or mechanical recording.").

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

there was still no Fourth Amendment violation when law enforcement listened in on conversations conducted by someone voluntarily wearing a wire.[66] In *White*, James A. White was tried and convicted on narcotics charges.[67] Law enforcement had surreptitiously listened in on White's conversations with one of their informants using a wire and radio equipment.[68] The court of appeals reversed the conviction, holding that *Katz* had overruled *On Lee*.[69]

The Supreme Court reversed the court of appeals.[70] The Court carried forward the precedent that a person carrying on conversation with another about illegal activities cannot reasonably expect privacy; they *assume the risk* of being informed upon.[71] The Court noted that the Fourth Amendment could not protect against friends later reporting their conversations to the police.[72] Given this precedent, the Court reasoned that lines could not be so finely drawn between the informant that merely reported what was said to the police and the informant that wore a wire.[73] The logic thus survived *Katz*.

Following *White*, cases in the 1970s found that information communicated in business records to businesses was the same as information communicated to undercover informants. In *United States v. Miller*, the government issued subpoenas to Mitch Miller's bank to obtain "all records of [his] accounts."[74] Without advising Miller, the bank turned over his incriminating records to the government.[75] Holding that Miller had no reasonable expectation of privacy in the bank records, the Court explained that Miller had "voluntarily conveyed" the records to the bank and that the information was "exposed to their employees in the ordinary course of business."[76] The Court thus extended the third-party doctrine beyond conversations to encompass

66. *Id.* at 750.
67. *Id.* at 746–47.
68. *Id.* at 747.
69. *Id.*
70. *Id.*
71. *Id.* at 752 ("Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police. . . . But if he has no doubts, or allays them, or risks what doubt he has, the risk is his.").
72. *Id.* at 751.
73. *Id.* at 751–52.
74. 425 U.S. 435, 437 (1976).
75. *Id.* at 438.
76. *Id.* at 442.

business records.

The third-party doctrine was expanded again in *Smith v. Maryland*.[77] In *Smith*, Michael Lee Smith allegedly robbed Patricia McDonough and afterwards placed several obscene and threatening phone calls to her residence.[78] Based on a description of Smith's car, police identified Smith and requested the local phone company to track the numbers dialed from Smith's phone using a device called a "pen register."[79] Police made this request without a warrant.[80] Upon review of the calls placed from Smith's phone, police found that Smith had dialed McDonough's number and, on that basis, obtained a search warrant for his home.[81] This search revealed incriminating evidence.[82] The trial court denied Smith's motion to suppress the pen register evidence on Fourth Amendment grounds and the appeals court affirmed.[83]

The Supreme Court affirmed the appeals court ruling.[84] Recognizing the reasonable expectation of privacy test discussed above,[85] the Court rejected that Smith had either a subjective expectation of privacy, or an expectation of privacy that society was prepared to recognize as reasonable.[86] In determining that Smith had no subjective expectation of privacy, the Court narrowed in on the specific activity that Smith would have sought to preserve as private.[87] Here, the Court distinguished between the "contents" of Smith's communications and the numbers dialed. The Court reasoned that while Smith may have desired to conceal the content of his communication with McDonough by using the phone inside his private residence, he could not make the same claim about concealing the numbers he dialed.[88] The Court concluded that even if Smith had a subjective expectation

77. 442 U.S. 735 (1979).
78. *Id.* at 737.
79. *Id.*
80. *Id.*
81. *Id.*
82. *Id.*
83. *Id.* at 737–38.
84. *Id.* at 746.
85. *Id.* at 740.
86. *Id.* at 743–44.
87. *Id.* at 743 ("Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.").
88. *Id.*

of privacy, it was not one society was prepared to recognize as reasonable.[89] The Court favorably quoted *Miller* and *White*, noting that Smith had assumed the risk that the number he dialed would be turned over to the police by sending it to the phone company.[90]

The Court then rejected two of Smith's arguments notable for the electronic context. First, the Court concluded that automation made no difference.[91] Despite the fact that Smith did not directly communicate the phone numbers to a human, he had still exposed his information by revealing it to the phone company's equipment.[92] Second, it did not matter whether the phone company regularly recorded phone numbers. Declining to make a "crazy quilt" out of the Fourth Amendment, the Court found the only significant fact was that Smith had exposed his phone number to a company with the capacity to record the information.[93] That alone meant the information could not be protected.

C. COLLECTION OF INTERNET HISTORY BY THE GOVERNMENT

Based on the Court's holdings in *Smith* and *Miller*, one might expect that the third-party doctrine would render all information that ISPs collect on internet users available to law enforcement. Though this is broadly true, Congress has passed legislation that adds some additional protections to internet history and subscriber information not covered by the Fourth Amendment. This Section will explain how courts have applied the third-party doctrine to the internet and the two statutory mechanisms under the 1986 Electronic Communications Privacy Act of 1986 (ECPA)[94] that define when law enforcement may compel an ISP to turn over an internet user's records.

1. Applying the Third-Party Doctrine to the Internet

The Court decided *Miller* and *Smith* in the very early stages of the internet,[95] likely without a concept of what the internet

89. *Id.*
90. *Id.* at 744.
91. *Id.* at 744–45.
92. *Id.*
93. *Id.* at 744.
94. Pub. L. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2701–2712 (2012)).
95. *See generally* BARRY M. LEINER ET AL., INTERNET SOC'Y, BRIEF HISTORY OF THE INTERNET (1997), https://www.internetsociety.org/wp-content/uploads/

was to become (if the Justices were even aware of the internet). Though the Supreme Court has yet to rule conclusively on the application of the Fourth Amendment to the internet,[96] lower court decisions have suggested that the third-party doctrine applies to much of the non-content internet history discussed above.[97] Courts confronting the issue have uniformly concluded that basic subscriber information, IP addresses, and email addresses in the to/from lines are "addressing information" equivalent to the phone numbers dialed in *Smith*.[98]

In *United States v. Forrester*, the Ninth Circuit held that these pieces of information were "constitutionally indistinguishable" from the information in *Smith*.[99] The *Forrester* court first reasoned that, like the phone numbers in *Smith*, users know or should know that this information is necessary to route the content information.[100] Thus, any information turned over was turned over "voluntarily."[101] Second, the court held that this information was not itself content information because it could only reveal as much content as a phone number could.[102] Be-

2017/09/ISOC-History-of-the-Internet_1997.pdf [https://perma.cc/3LVU-HLGZ] (providing a brief overview of the history of the internet); LO AND BEHOLD, REVERIES OF THE CONNECTED WORLD (Magnolia Pictures 2016) (reflecting on the history of and future possibilities for the internet).

96. *Cf.* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . This approach is ill suited to the digital age . . . .").

97. *See supra* Part I.A.

98. *See, e.g.*, United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010) ("[N]o reasonable expectation of privacy exists in an IP address . . . ."); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (concluding that computer surveillance to obtain "to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account" did not require warrant protections).

99. *Forrester*, 512 F.3d at 510.

100. *Id.* ("Internet users have no expectation of privacy in the to/from addresses of their messages or 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 of information.").

101. *Id.*

102. *See id.* ("[W]hen an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the

cause the *Smith* Court had already concluded that phone numbers were not content, this kind of internet history could not be content either.[103] The court analogized this information to the information on the outside of an envelope—people have a reasonable expectation of privacy in information inside in the envelope (the content), but not the non-content addressing information on the outside of the envelope.[104]

The *Forrester* court and other courts have, however, afforded protections to content information on the internet. The *Forrester* court exempted URLs from its analysis, noting that a "URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's internet activity."[105] The content of an email is also protected by the Fourth Amendment and requires a warrant based on probable cause.[106]

Despite non-content and subscriber information not being protected under the Fourth Amendment, Congress has stepped in to afford some limited protections to disclosure of this information by the companies that hold it.

2. Statutory Mechanisms: The Stored Communications Act and the Pen/Trap Statute

The Electronic Communications Privacy Act of 1986[107] provides procedures by which the government can obtain information about a user's internet activity. One of the ways that the government can obtain internet traffic information is by requesting it through "electronic communications services," typically

phone number may even show that the caller had access to specific content information.").

103. *Id.*

104. *Id.* at 511 ("E-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of communication are identical. The contents may deserve Fourth Amendment protection, but the address and size of the package do not.").

105. *Id.* at 510 n.6.

106. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause."); *see also* United States v. Ackerman, 831 F.3d 1292, 1306–07 (10th Cir. 2016).

107. Pub. L. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2701–2712 (2012)).

ISPs.[108] The Stored Communications Act (SCA),[109] Title II of the Electronic Communications Privacy Act of 1986, governs how the government may compel providers to disclose stored electronic communications.[110]

The government may obtain internet traffic information from an ISP through a court order under 18 U.S.C. § 2703(d) (a D order).[111] A D order allows law enforcement to obtain most records of user information held by ISPs, including subscriber information and records of IP addresses visited by a particular user.[112] Under § 2703, "[a] court order . . . shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records . . . are relevant and material to an ongoing criminal investigation."[113] Legislative history and subsequent court interpretations of this Section have suggested that this is a standard lower than probable cause, similar to the reasonable suspicion standard articulated in *Terry v. Ohio*.[114]

If the government only wants to find out the identity of a person associated with a known IP address, the standard is even lower. Basic subscriber information, including a person's name, address, records of lengths of connection, and sources of payment, is available upon subpoena.[115] The standard for issuing a subpoena is even more lenient than the specific and articulable facts standard required for a D order.[116]

108. For a discussion of what constitutes an "electronic service provider" under the Stored Communications Act, see H. MARSHALL JARRETT ET AL., OFFICE OF LEGAL EDUC., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 117–19 (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf [https://perma.cc/8QEU-PA64].

109. Pub. L. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2701–2712 (2012)). The phrase "Stored Communications Act" appears nowhere in the statute, but that is how it is popularly referred to. *See* JARRETT ET AL., *supra* note 108, at 115 n.1.

110. 18 U.S.C. § 2703.

111. JARRETT et al., *supra* note 108, at 130.

112. *See id.* at 130–32.

113. *Id.*

114. *Id.* at 131; *see* Terry v. Ohio, 392 U.S. 1, 20–27 (1968) (describing the standard).

115. 18 U.S.C. § 2703(c)(2).

116. JARRETT ET AL., *supra* note 108, at 128 ("The legal threshold for issuing a subpoena is low. . . . Investigators may obtain disclosure pursuant to § 2703(c)(2) using any federal or state grand jury or trial subpoena or an administrative subpoena authorized by a federal or state statute.").

If the government, however, wishes to obtain information about internet activity in real-time, they may seek to compel installation of a pen register and/or a trap and trace device.[117] Whereas monitoring an internet user's content in real-time would be governed by the federal Wiretap Act,[118] the government can monitor "addressing information" under a lower standard using the Pen Registers and Trap and Trace Devices (Pen/Trap Statute or PTS) chapter of Title 18.[119]

In the telephony context, pen registers and trap and trace devices are distinct. Pen registers monitor outgoing numbers and trap and trace devices monitor incoming numbers.[120] In the internet context, both incoming and outgoing information is contained in the same entity, called a header.[121] So, the devices used to capture internet headers in real-time are called "pen/trap" devices.[122] Used in the internet context, these devices may capture "almost all non-content information in a communication."[123] In other words, these devices can capture the IP addresses of computers receiving and sending messages, port numbers, and email to/from addresses. The standard to meet for ordering installation of a pen/trap device is lower than the specific and articulable facts standard of a D order; the government may order the installation if "the information likely to be obtained is relevant to an ongoing criminal investigation."[124]

D. *CARPENTER* AND A NEW FOURTH AMENDMENT ANALYSIS

In 2011, after a series of robberies of cell phone and electronics stores in Michigan and Ohio, police arrested a suspect that told them about several accomplices to the robberies.[125] One of these accomplices was Timothy Carpenter.[126] Under 18 U.S.C. § 2703(d), law enforcement obtained court orders requesting that MetroPCS and Sprint produce over 150 days of records

117. *See id.* at 151.
118. 18 U.S.C. §§ 2510–2522.
119. 18 U.S.C. §§ 3121–3127.
120. *See* JARRETT ET AL., *supra* note 108, at 153–54.
121. *Id.* at 154.
122. *Id.*
123. *Id.*
124. 18 U.S.C. § 3122(b)(2).
125. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).
126. *Id.*

showing the location of Carpenter's cell phone during these robberies.[127] These requests produced over 12,000 data points on Carpenter's location.[128] Law enforcement arrested Carpenter and charged him with several counts of robbery and carrying a firearm during a crime of violence.[129] The District Court denied Carpenter's motion to suppress the cell-site records.[130] At trial, an FBI agent testified about the cell phone location data and showed maps that illustrated that Carpenter's phone had been near the sites of four of the robberies.[131] Carpenter was convicted, and the Sixth Circuit affirmed, holding in part that Carpenter lacked a reasonable expectation of privacy in the historical cell-site location data.[132]

The Supreme Court granted certiorari and reversed. The Court held that law enforcement collection of seven days of historical cell-site location information (CSLI) was a Fourth Amendment search, which required a warrant.[133] The Court held first that the information collected invaded Carpenter's reasonable expectation of privacy, and second, that the third-party doctrine did not govern this case.[134] For the purposes of this Note, there are a number of salient takeaways from the Court's opinion.

First, in finding that law enforcement's access to historical CSLI invaded Carpenter's reasonable expectation of privacy, the Court recognized that it was not merely concerned with movements, but the private personal information one might discover in knowing about someone's movements.[135] The Court adopted Justice Sotomayor's reasoning from her concurrence in *United States v. Jones*: "[T]he time-stamped data provides an intimate window into a person's life, revealing not only his particular

127. *Id.*

128. *Id.*

129. *Id.*

130. *Id.*

131. *Id.* at 2212–13.

132. United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016) ("In sum, we hold that the government's collection of business records containing cell-site data was not a search under the Fourth Amendment."), *rev'd and remanded*, 138 S. Ct. 2206 (2018).

133. *Carpenter*, 138 S. Ct. at 2217.

134. *Id.* at 2219–20.

135. *Id.*

movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[136] To wit, the Court appeared not only concerned by geolocation data but by data generally that can provide a comprehensive picture of a person's habits.[137]

Second, the Court outlined a broad set of attributes about the data collected and the manner of data collection that it finds important. Relevant factors include: (1) that the data are "deeply revealing"; (2) that the data are deep, broad, and comprehensive; and (3) that the data collection was "inescapable and automatic."[138] Furthermore, the Court expressed a concern about the cost efficiency of data collection, remarking that collection of historical CSLI is "easy, cheap, and efficient compared to traditional investigative tools."[139]

Third, the Court rejected the government's arguments for the application of the third-party doctrine in the context of historical CSLI. The Court noted that "seismic shifts in digital technology" undercut the argument in *Smith* that disclosure of information to a human and to technology were indistinguishable.[140] Instead, the Court seemed to say that information that has the attributes described above is a "distinct category of information" deserving of special treatment: "Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible."[141]

The Court reasoned that neither the limited intrusion nor the voluntary exposure justifications of the third-party doctrine applied to historical CSLI. The Court interpreted *Smith* and *Miller* to require an examination of the "nature of the particular documents" sought by law enforcement.[142] Because historical CSLI

136. *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

137. *But see id.* at 2219–20 (noting that the Court does have a "special solicitude" for location information).

138. *Id.* at 2223. Though this Note will refer to these attributes as the *Carpenter* "factors," it is important to note that these factors do not constitute a rigid multi-part test and only represent attributes of CSLI that the court considered important. For a more comprehensive look into each of these factors, see Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357 (2019).

139. *Carpenter*, 138 S. Ct. at 2218.

140. *Id.* at 2219.

141. *Id.*

142. *Id.*

gave law enforcement easy access to comprehensive chronicle of a person's movements, it was not the same as the checks in *Miller* or the telephone logs in *Smith*.[143] Access to historical CSLI could not therefore be a limited intrusion.

Further, the voluntary exposure rationale was suspect. The Court recognized that the use of a cell phone had become "indispensable to participation in modern society" and that "[v]irtually any activity" on a phone generated CSLI.[144] Because a phone automatically generated CSLI, often with no "affirmative act" on the part of the user, users were not voluntarily exposing their physical location in any "meaningful sense."[145]

Finally, the Court concluded that because access to historical CSLI constituted a Fourth Amendment search, law enforcement must obtain a warrant founded upon probable cause before accessing historical CSLI.[146] Though the Court recognized that there may be situations where law enforcement may not be required to obtain a warrant, like responding to an emergency, the Court concluded that a warrant was required in the "mine-run criminal investigation."[147]

II. PRIVACY OF INTERNET HISTORY IS CURRENTLY INADEQUATELY PROTECTED

This Part will show that lower courts are shying away from a broad application of the reasoning of *Carpenter*, leaving internet history under-protected. First, this Part will show that decisions in the wake of *Carpenter* have focused on physical location and the specific factual circumstances of *Carpenter* itself instead of applying the reasoning of the decision. Next, this Part will suggest that this lack of extension is not only a missed opportunity but leaves internet history insufficiently protected from government intrusion. Finally, this Part will attempt to illustrate the value of internet privacy and explain why it might deserve greater protections in a democratic society.

143. *Id.*
144. *Id.* at 2220.
145. *Id.*
146. *Id.* at 2221.
147. *Id.* at 2223.

A. COURTS ARE RELUCTANT TO BROADLY EXTEND *CARPENTER* TO THE INTERNET

Though many initial cases following *Carpenter* did not have to consider its applicability to new facts owing to the good faith exception,[148] cases have increasingly had to confront *Carpenter*'s applicability to new sets of facts. But courts have hesitated to extend *Carpenter* to facts not dealt with in the opinion, including government collection of pole camera footage,[149] real-time GPS location information,[150] and utility records.[151] A few cases bear directly on the question considered in this Note: whether *Carpenter* can be read to apply to internet history information, including information that associates an individual with an IP address.

In *United States v. Contreras*, the Fifth Circuit considered whether *Carpenter* applied when an ISP provided an IP address that identified where a person resides.[152] In *Contreras*, law enforcement discovered that a computer associated with an IP address had uploaded "sexually graphic images" of children to Kik, an internet messaging service.[153] Law enforcement discovered that Frontier Communications, an ISP, had provided the IP address to one of their users, and the Northern District of Florida issued a grand jury subpoena to Frontier for the subscriber information associated with the IP address.[154] Frontier gave law enforcement the information, including the home address of the subscriber.[155] Based on this information, a court granted a search warrant for the residence.[156] Law enforcement executed

148. Nathaniel Sobel, *Four Months Later, How Are Courts Interpreting* Carpenter*?*, LAWFARE (Oct. 18, 2018, 8:57 AM), https://www.lawfareblog.com/four-months-later-how-are-courts-interpreting-carpenter [https://perma.cc/8SS2-5HPN].

149. United States v. Kubasiak, No. 18-CR-120-PP, 2018 WL 4846761, at *6 (E.D. Wis. Oct. 5, 2018); United States v. Tirado, No. 16-CR-168, 2018 WL 3995901, at *1–2 (E.D. Wis. Aug. 21, 2018).

150. State v. Sylvestre, 254 So. 3d 986, 989–90 (Fla. Dist. Ct. App. 2018).

151. United States v. Lightfoot, No. CR 17-0274, 2018 WL 4376509, at *6 (W.D. La. Aug. 30, 2018), *report and recommendation adopted*, No. CR 17-0274, 2018 WL 4374196 (W.D. La. Sept. 13, 2018).

152. 905 F.3d 853, 857 (5th Cir. 2018).

153. *Id.* at 855.

154. *Id.* at 855–56.

155. *Id.* at 856.

156. *Id.*

the warrant and discovered numerous videos depicting the sexual abuse of children.[157] The resident, Sebastian Contreras, was arrested, charged, and convicted of transportation and receipt of child pornography.[158]

Contreras argued on appeal that, considering *Carpenter*, law enforcement should have obtained a warrant to get the subscriber information from Frontier.[159] The Fifth Circuit quickly dismissed this attempt to extend *Carpenter*.[160] Judge Higginson wrote that this information fell "comfortably within the scope of the third-party doctrine."[161] Though the court acknowledged that *Carpenter* limited the power of the third-party doctrine, the court read *Carpenter* to require that the information collected bear on a person's "day-to-day movement."[162] The information provided to law enforcement only indicated Contreras's presence at his residence and nowhere else.[163] Thus, *Carpenter* did not apply.[164]

Numerous courts have reached similar results.[165] Courts have rejected applying *Carpenter* to IP addresses and subscriber

157. *Id.*
158. *Id.*
159. *Id.* at 856–57.
160. *Id.*
161. *Id.*
162. *Id.*
163. *Id.*
164. *Id.*
165. The First Circuit also concluded that third-party doctrine continued to apply to IP address information after *Carpenter*. United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) ("[A]n internet user generates the IP address data that the government acquired from Kik in this case only by making the affirmative decision to access a website or application. By contrast, as the Supreme Court noted in *Carpenter*, every time a cell phone receives a call, text message, or email, the cell phone pings CSLI to the nearest cell site tower without the cell phone user lifting a finger. . . . Thus, the government's warrantless acquisition from Kik of the IP address data at issue here in no way gives rise to the unusual concern that the Supreme Court identified in *Carpenter* . . . . Accordingly, we conclude that Hood did not have a reasonable expectation of privacy in the information that the government acquired from Kik without a warrant."). The Ninth and Fourth Circuits have also declined to extend *Carpenter* to IP address information, albeit in non-precedential opinions. United States v. VanDyck, 776 F. App'x 495, 496 (9th Cir. 2019) ("VanDyck argues that the evidence should be suppressed because the Fourth Amendment required a warrant to obtain the subscriber information associated with the IP address . . . . [W]e decline to extend *Carpenter* to encompass the argument advanced by VanDyck."); United States v. Wellbeloved-Stone, No. 18-4573, 2019 WL

information because the information is not detailed enough,[166] not a comprehensive account of day-to-day movement,[167] or because *Carpenter* itself remarked that it was a narrow decision.[168] Some courts have cited all three reasons.[169]

Though most courts have been skeptical about extending *Carpenter* to cover digital footprints, one decision in the District Court of Rhode Island seemed to recognize the possibility that

2474025, at *2 (4th Cir. June 13, 2019) (per curiam) ("Wellbeloved-Stone contends that he had a reasonable expectation of privacy in his IP address and subscriber information after *Carpenter* . . . . The Court explicitly emphasized the narrow scope of its holding, and Wellbeloved-Stone cites no post-*Carpenter* authority extending *Carpenter*'s rationale to IP addresses or subscriber information." (citation omitted)). Many federal district courts and some state courts have been similarly unpersuaded. *See, e.g.*, *infra* notes 166–70.

166. United States v. McCutchin, No. CR-17-01517-001-TUC-JAS (BPV), 2019 WL 1075544, at *2 (D. Ariz. Mar. 7, 2019) ("The internet subscriber information differs drastically from the CSLI obtained in Carpenter. It provides business records that are not detailed or encyclopedic. Subscriber information does not reveal familial, political, professional, religious, sexual associations, or location."); United States v. Tolbert, 326 F. Supp. 3d 1211, 1225 (D.N.M. 2018) ("The privacy interest in this type of identifying data, which presumably any AOL or CenturyLink employee could access during the regular course of business, simply does not rise to the level of the evidence in *Carpenter* such that it would require law enforcement to obtain a search warrant.").

167. Brown v. Sprint Corp. Sec. Specialist, No. 17-CV-2561(JS)(ARL), 2019 WL 418100, at *4 (E.D.N.Y. Jan. 31, 2019) ("*Carpenter* focuses on the intrusion of tracking a person's physical movements, which Plaintiff does not allege is at issue here."); *see also* United States v. Germain, No. 2:18-cr-00026, 2019 WL 1970779, at *4 (D. Vt. May 3, 2019); United States v. Jenkins, No. 1:18-cr-00181, 2019 WL 1568154, at *4 (N.D. Ga. Apr. 11, 2019); United States v. Popa, 369 F. Supp. 3d 833, 838 (N.D. Ohio 2019); United States v. Streett, 363 F. Supp. 3d 1212, 1309 (D.N.M. 2018); United States v. Gregory, No. 8:18CR139, 2018 WL 6427871, at *2 (D. Neb. Dec. 7, 2018); People v. Sime, 88 N.Y.S.3d 823, 826 (N.Y. Crim. Ct. 2018).

168. Cryer v. Idaho Dep't of Labor, No. 1:16-cv-00526-BLW, 2018 WL 3636529, at *1 n.1 (D. Idaho July 30, 2018); United States v. Westley, No. 3:17-CR-171 (MPS), 2018 WL 3448161, at *14 n.9 (D. Conn. July 17, 2018).

169. United States v. Felton, 367 F. Supp. 3d 569, 575 (W.D. La. 2019) ("Felton's use of the IP address is not so closely related to his 'home' that the Court can say that there is a privacy interest as to his papers and personal effects. Second, the logs obtained from the USPS do not track Felton's every movement of every day; they only identify the fact that Felton was tracking the packages. The Court further recognizes the very narrow ruling in *Carpenter* and finds that it does not govern this case. Thus, the Court concludes that there was no reasonable expectation of privacy as to the information provided by Comcast (Felton's IP address) and the content of the communication between Felton's IP address and the USPS server."); *see also* United States v. Therrien, No. 2:18-cr-00085, 2019 WL 1147479, at *2 (D. Vt. Mar. 13, 2019).

Carpenter could apply to "exhaustive chronicle[s]" of digital activities and not just to physical activities.[170] In *United States v. Monroe*, law enforcement obtained a D order requesting that a website disclose the IP addresses of users that had downloaded video files depicting child pornography.[171] Law enforcement, using publicly available information on the internet, then learned which ISP issued these IP addresses and subpoenaed subscriber information to learn the identity of the users, including one Jordan Monroe.[172] Using this information, law enforcement obtained a search warrant for Monroe's residence and discovered a collection of child pornography.[173]

Monroe moved to exclude the evidence of his IP address obtained via the D order, arguing that the *Carpenter* reasoning should apply to IP addresses.[174] The court rejected this argument, observing that an IP address is more like the information in *Smith* and *Miller*.[175] "An IP address," the court argued, "is one link held by a third party in a chain of information that may lead to a particular person. It does not reveal the kind of minutely detailed, historical portrait of 'the whole of [a person's] physical movements' that concerned the Supreme Court in *Carpenter* . . . ."[176] But the court appears to have based its holding on its perception that law enforcement could glean little information from an IP address without further investigation.[177] The *Monroe* court seemingly recognized that if digital information, even information outside of CSLI, reached a certain level of intrusiveness, the *Carpenter* analysis could be appropriate.[178]

The *Monroe* court's willingness to even consider digital activities under the framework of *Carpenter* is a rarity. Most courts continue to dismiss the possibility that IP addresses and subscriber information are subject to *Carpenter*'s new Fourth Amendment analysis. Although commentators expressed that

170. United States v. Monroe, 350 F. Supp. 3d 43, 48 (D.R.I. 2018) (internal quotation marks omitted) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018)).

171. *Id.* at 44–45.

172. *Id.* at 44.

173. *Id.*

174. *Id.*

175. *Id.* at 49.

176. *Id.* (quoting Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018)).

177. *See id.* at 48.

178. *See id.*

Carpenter could have been a watershed moment for digital privacy, the current trend in the courts locks in the existing inadequate privacy schemes.

B. INTERNET HISTORY IS NOT SUFFICIENTLY PROTECTED BY CURRENT PRIVACY SCHEMES

Three concerns demonstrate that internet privacy may be in a precarious spot under current privacy schemes. First, the use of internet history information by law enforcement shows no signs of slowing and companies are not providing a meaningful check on information provided to law enforcement. Transparency reports by Google,[179] Twitter,[180] Facebook,[181] and large ISPs[182] all show that they continue to receive thousands of requests from law enforcement for information. In most cases, a company will provide at least some user information in response to a government request.[183] Though companies may often have incentives to protect user information and perhaps comply minimally with these requests,[184] companies are still providing the government with user information which threatens a user's privacy.

179. *Requests for User Information – Google Transparency Report*, GOOGLE, https://transparencyreport.google.com/user-data/overview?hl=en [https://perma.cc/9X7Y-AXF8].

180. *United States of America*, TWITTER, https://transparency.twitter.com/en/countries/us.html [https://perma.cc/T4XH-YPT4].

181. *Requests for User Data – United States*, FACEBOOK, https://transparency.facebook.com/government-data-requests/country/US (last visited Mar. 6, 2019).

182. COMCAST TRANSPARENCY REPORT: JANUARY 1, 2018 – JUNE 30, 2018 (2018), https://update.comcast.com/wp-content/uploads/sites/33/dlm_uploads/2018/12/Comcast-Tenth-Transparency-Report-FINAL-Dec-2018-1.pdf [https://perma.cc/6MD5-W3Q8]; *Transparency Report*, AT&T, https://about.att.com/csr/home/frequently-requested-info/governance/transparencyreport.html [https://perma.cc/9HT2-39RD]; *see also Transparency Reporting Index*, ACCESS NOW, https://www.accessnow.org/transparency-reporting-index/ [https://perma.cc/8LSG-8VPQ] (last updated 2016).

183. *See, e.g.*, *Requests for User Data – United States*, *supra* note 181 (showing that Facebook provided the government with some user information in response to 86% of requests).

184. *See generally* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99 (2018) (explaining that companies that serve as "surveillance intermediaries" between the government and a user often have financial and ideological incentives that do not align with government interests).

Second, while the SCA and the PTS would seem to provide some protections for internet users, the protections are very limited. All so-called non-content information can be obtained from a provider under a reasonable suspicion standard, and pen/trap devices may be installed on a showing of mere relevance.[185] Even though law enforcement may often possess more than probable cause in internet investigations when they seek to obtain additional information,[186] the increased use of the internet for all kinds of daily communication and transactions will increase incentives for law enforcement to argue for access to large portions of a suspect's internet history.[187]

Third, even if the SCA and PTS were protective, the statutes lack real bite in the event they are not followed. Suppression of evidence is not available for nonconstitutional violations of the SCA or PTS.[188] Because most conduct under these statutes would not constitute a search,[189] a suspect that demonstrated that the government had not made the proper showing, but received the court order anyways, could not then exclude the evidence. Thus, a person subject to internet surveillance lacks protection at the front and back end of the search.[190]

185. *See supra* Part I.C.2.

186. *Cf.* Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514 (2010). Professor Ohm argues that the justification standards (probable cause, reasonable suspicion, and the like) matter less in internet investigations where law enforcement is less likely to encounter a naked IP address in the wild. *Id.* Importantly, Ohm notes that fishing expeditions are one area where justification standards are likely to remain significant. *Id.* at 1550.

187. *See* Jennifer Stisa Granick, *If the Government Had Its Way, Everything Could Be Wiretapped*, ACLU (Feb. 19, 2019, 10:30 AM), https://www.aclu.org/blog/privacy-technology/internet-privacy/if-government-had-its-way-everything-could-be-wiretapped [https://perma.cc/99BL-38LV].

188. 18 U.S.C. § 2708 (2012) ("The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."); *see* United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008) (citing several cases for the proposition that violations of the Acts do not merit exclusion of evidence).

189. *See supra* Part I.C.1.

190. This Note argues that protection on the front end is important. For a compelling argument (one that this author agrees with) that the exclusionary rule should be added statutorily to protect the back end of the search, see Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805 (2003).

C. A LOSS OF INTERNET PRIVACY IS HARMFUL TO SOCIETY

The Fourth Amendment and its protections are at the heart of American democracy. In 18th-century America, colonists had become excellent smugglers and pirates, defying the Crown's attempts to mandate that the colonies only trade with Britain.[191] In response, the Crown authorized writs of assistance.[192] A writ of assistance allowed agents of the Crown to search broadly for smuggled goods without "a sworn declaration, notice, or probable cause."[193] In a five-hour oration before the Massachusetts State House, a young lawyer named James Otis, Jr. disputed the legality of the writs in defense of fifty-three Boston merchants.[194] Otis called the writs the "worst instrument of arbitrary power, the most destructive of English liberty . . . that was ever found in an English law-book."[195] Otis lost his case.[196] But John Adams, an audience member to Otis's oration would later write in a letter to William Tudor: "Then and there, the child independence was born."[197]

Otis's words in opposition to the writs of assistance loom large in Fourth Amendment jurisprudence.[198] There is clear doctrinal support for this conception of privacy. But merely because citizens have challenged government conduct in the past does not necessarily mean that the same issues pervade today. Indeed, numerous reports on the "death" of privacy suggest that people may not possess the concerns that Otis had with governmental overreach.[199] Because privacy is a notoriously slippery

191. Philip Foglia, *The Lawyer Who Lit the Fuse of the American Revolution*, N.Y. ST. B. ASS'N J., Mar./Apr. 2015, at 26, 26.

192. *Id.*

193. *Id.* at 27.

194. *Id.*

195. *Id.* at 28.

196. *Id.*

197. *Id.*

198. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018); Stanford v. Texas, 379 U.S. 476, 481 (1965); Boyd v. United States, 116 U.S. 616, 625 (1886).

199. *See, e.g.*, Geoff Duncan, *Zuckerberg: Online Privacy Is Not a "Social Norm,"* DIGITAL TRENDS (Jan. 11, 2010, 9:32 AM), https://www.digitaltrends.com/social-media/zuckerberg-online-privacy-is-not-a-social-norm/ [https://perma.cc/3HMW-GK9A]; John H. Fleming & Amy Adkins, *Data Security: Not a Big Concern for Millennials*, GALLUP (June 9, 2016), https://news.gallup.com/businessjournal/192401/data-security-not-big-concern-millennials.aspx [https://perma.cc/SZ65-CR7C] ("[M]illennials are the generation that is

concept[200] and because there may be some question of its value in a digital age,[201] mounting a defense of internet privacy may help elucidate why we might want to preserve it even if we are not diehard Otis-ites.

The right of privacy was famously described by Justice Louis Brandeis as "the right to be let alone."[202] Alan F. Westin expanded upon this definition in his influential treatise on privacy, describing privacy as the ability to control "when, how, and to what extent information about them is communicated to others."[203] For Westin, the individual's ability to control disclosure of information about them to certain parties and society writ large fostered four interrelated functions for individuals in a democracy: personal autonomy, emotional release, self-evaluation, and limited and protected communication.[204] The relevant aspects of these functions for internet privacy are considered below.

Personal autonomy is the ability to "avoid being manipulated or dominated wholly by others."[205] For Westin, democracies recognize that human dignity requires that humans be able to

most trusting of institutions to safeguard their personal data."); *Is Online Privacy Over?*, CTR. FOR DIGITAL FUTURE (Apr. 22, 2013), https://www.digitalcenter.org/online-privacy-and-millennials-0413/ [https://perma.cc/2RP2-RD7U]; Eric Limer, *CES 2018's Hot New Trend: The Total Death of Privacy*, POPULAR MECHANICS (Jan. 10, 2018), https://www.popularmechanics.com/technology/security/a15045965/2018s-hot-new-tech-trend-is-the-death-of-privacy/ [https://perma.cc/C3PN-B97Q]; Alex Preston, *The Death of Privacy*, GUARDIAN (Aug. 3, 2014), https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston [https://perma.cc/MW8N-4YJ7]. Privacy's death has likely been greatly exaggerated. *See* DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 14 (2017) ("Everyone values privacy. Different people just draw different boundaries. That is true even of millennials.").

200. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1–8 (2008) (arguing privacy rights arguments often fail due to a failure to fully conceptualize privacy); *see also* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013) ("[O]ur society lacks an understanding of why (and when) government surveillance is harmful.").

201. *See supra* note 199.

202. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

203. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

204. *Id.* at 32.

205. *Id.* at 33.

preserve and protect a "core" of individuality.[206] Further, development of independent and diverse thought requires that humans be able to experiment in private.[207] A lack of privacy could have a levelling effect, leaving people afraid to express thoughts too far outside the mainstream.[208]

Societies must also allow individuals the opportunity for emotional release. People play different social roles in different situations, each coming with their own sets of expectations and permitted behaviors.[209] Westin argues that not only do people need time off from playing their different social roles, it is necessary to have enough privacy to complain about others.[210] People should have enough privacy, Westin argues, such that they can express commentary that is not First Amendment-protected speech, commentary that is "wholly unfair, frivolous, nasty, and libelous."[211] This serves as a "safety-valve" in a democracy, allowing people to complain about authority in private while developing measured speech for public presentation.[212] Moreover, privacy in this domain allows society to accommodate minor infractions of the law.[213] Whereas society may be forced to take action if it knew of all lawbreaking behavior, a hardy right to privacy allows the state to place minor infractions or mere suspicions of lawbreaking beyond its cognition.[214]

Further, privacy is necessary for self-evaluation to occur. The ability to "integrate" one's experiences in private not only facilitates creative thought but allows people to measure their

206. *Id.*

207. *Id.* at 34.

208. *Cf.* FOUCAULT, *supra* note 1, at 202–03 ("He who is subjected to a field of visibility, and who know it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection."). For an argument that the revelation of online pornography preferences could have this type of levelling effect, further disciplining the difference of already marginalized groups, see Elena Maris et al., Tracking Sex: The Implications of Widespread Sexual Data Leakage and Tracking on Porn Websites 5–7 (July 15, 2019) (unpublished manuscript), https://arxiv.org/pdf/1907.06520.pdf [https://perma.cc/4NCG-T7ZD].

209. *See* WESTIN, *supra* note 203, at 35.

210. *See id.* at 35–36.

211. *Id.* at 36.

212. *Id.* at 35–36.

213. *Id.* at 35.

214. *Id.*

performance against their personal ideals.[215] For Westin, the ability to take "moral inventory" of one's actions in private brings the "conscience into play," allowing people to improve themselves.[216]

Finally, privacy allows for limited and protected communication. The ability to choose the subject, extent, and recipient of one's disclosures permits individuals to maintain relationships and guard their associations with "doctors, lawyers, ministers, psychiatrists, psychologists, and others."[217] Anonymity in communication and action can allow better testing of ideas and prevent unwanted government intrusion.[218]

These functions are active on the internet. People express themselves on the internet; they make associations with political groups; they buy things; they seek legal, medical, or spiritual advice. In other corners of the internet, people are "trolls," "individual[s] who post[] false accusations or inflammatory remarks on social media to promote a cause or to harass someone."[219] Where this conduct is anonymous or is otherwise known to limited parties and does not rise to the level of major criminal activity, it promotes Westin's functions. The choice of which forum to express oneself in should not significantly modify Westin's analysis.[220] Against all odds, even internet trolls can serve a democratic function.

Carpenter's rationale appears to recognize Westin's basic functions of privacy. Facts of modern life have allowed companies to amass lengthy histories of internet users' activities, containing sensitive information about a user's beliefs, thoughts,

215. *Id.* at 36–37.

216. *Id.* at 37.

217. *Id.* at 38.

218. *See id.* at 31–32.

219. *Definition of: Internet Troll*, PCMAG.COM, https://www.pcmag.com/encyclopedia/term/68609/internet-troll [https://perma.cc/X65Y-LSQM].

220. Though, the potential existence of a privacy paradox may complicate matters. Some research has suggested that people make decisions regarding their privacy online that does not square with their attitudes and intentions toward privacy. *See* Susanne Barth & Menno D.T. de Jong, *The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review*, 34 TELEMATICS & INFORMATICS 1038 (2017). These decisions may not be entirely rational—people may be aware that the costs of their online behavior outweigh the benefits and perform risky online behaviors anyways. *Id.* at 1039.

and desires. Mere participation in communication over the internet should not mean you have forever forfeited privacy in your internet history.

III. COURTS CAN AND SHOULD EXTEND *CARPENTER* TO PROTECT INTERNET HISTORY

This Part will argue that lower courts can and should extend *Carpenter* to cover historical records of non-content internet history, real-time monitoring of the same content, and disclosure of basic subscriber information. This Part will first note that *Carpenter* is likely broader than its assertedly narrow holding and lay out a theory by which courts could extend *Carpenter* to require a warrant for certain kinds of internet history. This Part will then examine the three scenarios described above and argue that courts could reasonably extend *Carpenter* to apply to these scenarios. Finally, this Part will contend that the best way to extend *Carpenter* to cover these scenarios is to impose a warrant requirement when the government seeks to collect information falling into these categories.

A. *CARPENTER* CAN BE BROADER THAN ITS NARROW HOLDING

In *Carpenter*, Chief Justice Roberts wrote in no uncertain terms about the bounds of the Court's opinion: "Our decision today is a narrow one. We do not express a view on matters not before us."[221] Roberts says that the Court's opinion does not disturb *Smith* or *Miller* and does not "call into question conventional surveillance techniques."[222] As noted above,[223] this language has left lower courts understandably squeamish when faced with the prospect of applying the *Carpenter* factors to new factual situations. This Note freely admits that courts are well within their authority to refuse to apply *Carpenter* beyond its explicit holding.

Yet most everyone writing about *Carpenter* thinks that when the Court says seven days of historical cell-site location information,[224] it means more than seven days of historical cell-site location information."[225] Rehashing all of the arguments

221. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

222. *Id.*

223. *See supra* Part II.B.

224. *Carpenter*, 138 S. Ct. at 2217 n.3.

225. *See, e.g.*, ORIN S. KERR, THE DIGITAL FOURTH AMENDMENT (forthcoming 2019); Jennifer A. Brobst, *The Metal Eye: Ethical Regulation of the State's*

here is unnecessary. The volume of scholarship says that the Court has reiterated that digital is different, and that this decision sets out a framework which the Court will use in the future to scope Fourth Amendment searches. The Court itself has admonished lower courts that have "mechanical[ly]" adhered to precedent when applying the Fourth Amendment to digital contexts.[226] Because *Carpenter* has provided a framework for a decision that calls into question the third-party doctrine,[227] extensions beyond its explicit holding are justified—the Court has signaled a departure from precedent.[228]

But even though the extension of *Carpenter* may be justified, it does not necessarily follow that lower courts should be the actor to accomplish this task. After all, Congress could merely amend the relevant statutes[229] to require warrant protections for obtaining internet history information and provide for an exclusionary remedy. Indeed, there is a powerful argument that Congress is in the best position to balance the competing interests in the privacy analysis, especially when it comes to changing technology.[230]

Congress, however, does not appear to be up to the task. First, congressional efforts to update the ECPA have historically

Use of Surveillance Technology and Artificial Intelligence to Observe Humans in Confinement, 55 CAL. W. L. REV. 1, 24 (2018); Danielle Keats Citron, Comment, *A Poor Mother's Right to Privacy: A Review*, 98 B.U. L. REV. 1139, 1164 (2018); Christine Guest, Comment, *DNA and Law Enforcement: How the Use of Open Source DNA Databases Violates Privacy Rights*, 68 AM. U. L. REV. 1015, 1044 (2019); Grace Manning, *Alexa: Can You Keep A Secret? The Third-Party Doctrine in the Age of the Smart Home*, 56 AM. CRIM. L. REV. ONLINE 25, 26 (2019); Ohm, *supra* note 138, at 361–66; Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J.F. 943, 943–44 (2019); Wouter Zwart, Note, *Slow Your Roll Out of Body-Worn Cameras: Privacy Concerns and the Tension Between Transparency and Surveillance in Arizona*, 60 ARIZ. L. REV. 783, 799 n.112 (2018).

226. *See* Riley v. California, 573 U.S. 373, 386 (2014).

227. *See supra* Part I.D.

228. For a discussion of why lower courts are justified in "narrowing from below" outdated precedents, see Richard M. Re, *Narrowing Supreme Court Precedent from Below*, 104 GEO. L.J. 921 (2016). Though as admitted above, the "best" reading of *Carpenter* is likely its explicit holding on historical CSLI, it is still within reason to read the Court's framework as applying to other categories of digital information as it is written so broadly.

229. *See supra* Part I.C.2.

230. *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 806 (2004) (arguing that the legislative branch should create the "primary investigative rules when technology is changing").

stalled, despite strong support from industry and civil liberties groups.[231] Second, while political will may exist to provide privacy protections against corporate surveillance of user information in the wake of various scandals involving Facebook, the same may not be true of efforts to restrict government surveillance.[232] Recent changes to privacy legislation have gone in the other direction, ratifying, and in some cases, expanding government surveillance power.[233] Courts, therefore, must step in and fulfill their constitutional duty to protect against overreaches by the political branches.[234]

B. EXTENSION OF *CARPENTER*: THREE SCENARIOS

If lower courts accept that *Carpenter*'s reasoning can apply beyond seven days of historical cell-site location information, then they need a test to apply to new sets of facts. This Note proposes that if digital data sought meet the factors set out in *Carpenter*, then a court should hold that law enforcement conduct to obtain data constitutes a search.[235] Consistent with *Carpenter*, this finding should not be a case-by-case determination based on whether an invasion of privacy actually occurred, but a determination based on the type of data sought. Further, because *Carpenter* reiterates the proposition that inferences do not insulate a search,[236] a court determining whether a *Carpenter* search has

231. Mike Orcutt, *Why Congress Can't Seem To Fix This 30-Year-Old Law Governing Your Electronic Data*, MIT TECH. REV. (Feb. 17, 2017) https://www.technologyreview.com/s/603636/why-congress-cant-seem-to-fix-this-30-year-old-law-governing-your-electronic-data/ [https://perma.cc/3JED-FNVW].

232. Louise Matsakis, *SCOTUS and Congress Leave the Right to Privacy Up For Grabs*, WIRED (July 3, 2018, 11:49 AM), https://www.wired.com/story/scotus-congress-leave-right-to-privacy-up-for-grabs/ [https://perma.cc/9PV2-LRZV].

233. *See* Louise Matsakis, *Congress Renews Warrantless Surveillance—and Makes It Even Worse*, WIRED (Jan. 11, 2018, 4:19 PM), https://www.wired.com/story/fisa-section-702-renewal-congress/ [https://perma.cc/5MAH-8LAW].

234. *See* GRAY, *supra* note 199, at 14; THE FEDERALIST NO. 78, at 469 (Alexander Hamilton) (Clinton Rossiter ed., 1961) ("[T]he courts of justice are to be considered as the bulwarks of a limited Constitution against legislative encroachments . . . .").

235. There is an alternative theory based on bailment of digital information that the Court might also support, which is beyond the scope of this Note. For a brief discussion of this theory, see Ohm, *supra* note 138, at 36. Another alternative approach to remedying the problems with the third-party doctrine is considered earlier in this volume. *See* Wayne A. Logan & Jake Linford, *Contracting for Fourth Amendment Privacy Online*, 104 MINN. L. REV. 101 (2019) (arguing that contract law could inform the Fourth Amendment analysis).

236. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

occurred must look at all of the sensitive information that may be compromised by tying a person to a particular collection of internet activity.

Both Professors Ohm and Kerr have argued that implementing *Carpenter* would likely cover some internet history records.[237] Neither go far enough with their analysis. This Section will argue that while Ohm and Kerr are correct to recognize that IP addresses of the websites a user visits should be protected under the rationale of *Carpenter*, similar logic should extend this rationale to cover both real-time monitoring of the same information and basic subscriber information that can in effect tie a person to a set of internet activity.

The contours of *Carpenter* remain fuzzy even as to how it protects historical cell-site location information. Extension of the reasoning thus presents even greater challenges. The following three scenarios will attempt to provide some guidance as to what extension of *Carpenter*'s reasoning to collection of internet history could look like.

1. Scenario One: A Court Order Requires an ISP or Website To Disclose Historical Information About a User

In *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, the government sought information from Twitter about a variety of parties, including Chelsea Manning, Julian Assange, and Wikileaks.[238] The government obtained an ex parte order under 18 U.S.C. § 2703(d) requesting Twitter disclose the subscriber information for accounts "registered to or associated with" these parties (among others) as well as "records of user activity for any connections made to or from the Account[s]."[239] The Eastern District of Virginia denied a Fourth Amendment challenge to the order, holding that the parties lacked a reasonable expectation of privacy in IP address information.[240]

One could imagine similar cases where law enforcement has something more than a hunch[241] about someone's suspected criminal activity but less than probable cause. Under current

237. KERR, *supra* note 225 (manuscript at 46–48); Ohm, *supra* note 138, at 378–80.

238. 830 F. Supp. 2d 114, 121 (E.D. Va. 2011).

239. *Id.*

240. *Id.* at 138.

241. *See supra* Part I.C.2 (exploring the current standards for requesting non-content information).

law, law enforcement can subpoena large swaths of that user's internet activity from ISPs or websites to prove their case.[242]

This situation should fall squarely within the *Carpenter* factors.[243] First, the data are deeply revealing. As described above, a collection of IP addresses that a person accessed essentially provides a history of that person's internet activity.[244] This activity may reveal sensitive information about a person's life.[245] Second, the data are deep, broad, and comprehensive. ISPs may keep years of records of a user's connections to other IP addresses.[246]

Third, collection of these data is inescapable and automatic. IP addresses are assigned to computers and required to facilitate communication between computers.[247] Like cell-site location information, IP addresses operate behind the scenes such that turning them over could hardly be considered voluntary. There is a colorable argument that a user volunteers IP address information when they visit a webpage,[248] but this misreads *Carpenter*.[249] The *Carpenter* Court, noting that cell phones become "indispensable to participation in modern society," expressed a concern that "virtually any activity" on a phone would generate CSLI and thus required voluntary disclosure in a "meaningful sense."[250] Though the Court noted that automatic data connections made by the phone bolstered its argument, the Court did not so finely parse cell phone activities into voluntary and automatic. Instead, the Court swept all CSLI generated by a cell phone into its analysis. Similarly, the internet is a critical part of modern society. And, like CSLI, a user creates IP address information by virtually any activity on the internet.[251] It is difficult to distinguish between the two on this *Carpenter* factor.

Fourth, the ability to collect these data is a massive efficiency gain for law enforcement. There is no precise historical

242. *See supra* Part I.C.2.

243. *See supra* Part I.D.

244. *See supra* Part I.A.

245. *See supra* notes 17–18 and accompanying text.

246. *See* Ohm, *supra* note 17.

247. Titus, *supra* note 26.

248. *See, e.g.*, United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) ("[A]n internet user generates the IP address data . . . only by making the affirmative decision to access a website or application.").

249. *See supra* notes 144–47 and accompanying text.

250. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

251. *See supra* Part I.A.

analog to the type of information law enforcement have access to with internet histories. IP addresses may reveal detailed histories of a person's plans and predilections unobtainable by traditional surveillance tools without a warrant.

Thus, each *Carpenter* factor supports treating historical IP address information like historical CSLI. Courts should reject the myopic view of interpreting *Carpenter* as only pertaining to location information; obtaining IP address information can be as, or in many cases more, intrusive than historical CSLI.

2. Scenario Two: A Pen/Trap Device Captures Real-Time Information About a User's Internet Activities

This scenario is the one encountered in the introduction to this Note. As a part of the investigation of Ulbricht, law enforcement installed five pen/trap devices to track the internet activity to and from Ulbricht's home router.[252] The orders authorizing the installation of the devices allowed law enforcement to collect source and destination IP addresses, with "dates, times, durations, [and] ports of transmission."[253]

The information obtained is no different than the information obtained in scenario one. The difference here is that the information obtained with a pen/trap device is obtained in real time instead of as a prefigured collection.[254] An open question remains about whether the *Carpenter* factors apply to data collection in real time.[255] In the case of pen/trap devices to collect internet activity, they should; the kind of information collected is identical to that sought in Scenario One.

Even courts placing an emphasis on the durational limit expressed in *Carpenter* should find no difficulty here because a pen/trap order must specify the length of time the order will last.[256] Thus, the historical and real-time situations are function-

252. United States v. Ulbricht, 858 F.3d 71, 95 (2d Cir. 2017).

253. *Id.*

254. *See supra* Part I.C.2.

255. *Cf. Carpenter*, 138 S. Ct. at 2220 (noting that the Court is not addressing real-time CSLI).

256. 18 U.S.C. § 3123(c) (2012). But do note that the appropriate inquiry here is not whether there is some arbitrary durational limit that determines when privacy has actually been invaded, but whether the surveillance allows access to the kinds of information that fall under the *Carpenter* factors. The duration should only be relevant to the analysis if it would change the type of information requested by the government.

ally indistinguishable; a lump sum invasion of privacy is no different than a day-by-day invasion.[257] The *Carpenter* Court expressed a concern with data collected over a span of seven days.[258] Most pen/trap cases are likely to exceed this span. The statutory scheme for obtaining a pen/trap device allows and anticipates collection of up to four months of information.[259] This fact would likely obviate the need for a lower court to confront whether there is some period under seven days where a search does not occur.

In the rare case where the government seeks to obtain less than a week of real-time internet activity and the lower court was focused on the seven-day cap in *Carpenter*, courts may still be justified in finding a Fourth Amendment search. The distance someone can travel in a day is limited by their access to transportation; the distance someone can travel on the internet is limited only by how fast they can click. The average adult spends 5.9 hours a day with digital media, including smartphones, desktops, laptops, streaming devices and gaming devices.[260] It is possible to visit numerous websites in those 5.9 hours, creating a detailed picture of the person using the device. Thus, the privacy concerns still exist in real-time collection of internet history even if it is over a seemingly short amount of time.

257. In other words, seven days of information is seven days of information regardless of whether it is collected all at once or piece by piece. A few courts have already forecasted that eventually real-time and historical CSLI may be subject to the same probable cause requirement. United States v. Chavez, No. 15-CR-00285-LHK, 2019 WL 1003357, at *4–6 (N.D. Cal. Mar. 1, 2019) (stating that eventually historical and real-time CSLI may be treated similarly as real-time collection may pose a greater threat to privacy); *cf.* United States v. Gibson, No. 3:18-CR-033, 2019 WL 2265370, at *3 (N.D. Ind. May 28, 2019) (assuming that probable cause standard must be met for government to obtain order for real-time CSLI over 30-day period, just as a court would for historical CSLI).

258. *Carpenter*, 138 S. Ct. at 2234.

259. 18 U.S.C. § 3123(c) (2012); *see also* Brief of Reason Foundation et al. as Amici Curiae Supporting Petitioner at 25, Ulbricht v. United States, 138 S. Ct. 2708 (2018) (No. 17-950), 2018 WL 776098.

260. Rob Marvin, *Tech Addiction by the Numbers: How Much Time We Spend Online*, PCMAG.COM (June 11, 2018, 8:00 AM), https://www.pcmag.com/article/361587/tech-addiction-by-the-numbers-how-much-time-we-spend-online [https://perma.cc/8DQU-MTVN].

3. Scenario Three: A Subpoena Allows Law Enforcement To Obtain Basic Subscriber Information Associated with an IP Address

A common occurrence in child pornography prosecutions is that law enforcement officials will discover through investigation that a computer has viewed or downloaded illicit materials, but law enforcement will only have the IP address associated with that computer.[261] For example, in *United States v. Perez*, the FBI received a complaint from a woman who claimed a Yahoo! user had sent her images of children engaged in sexual acts.[262] The FBI subpoenaed Yahoo! for the user's IP address and was able to determine that Time Warner Cable had issued the IP address.[263] The FBI then subpoenaed Time Warner for the user information associated with that IP address, including the user's address.[264] This subpoena revealed that Time Warner had issued the IP address to Javier Perez.[265] Using this information combined with a public records check, the FBI obtained and executed a search warrant on Perez's home and found over 4,000 compact discs of child pornography.[266]

Courts applying *Carpenter* should hold that both of these requests would be searches. This is admittedly the most tenuous extension of *Carpenter*; there are good arguments that obtaining basic subscriber information alone does not reveal the same things about a person's conduct online that obtaining a record of their history does.[267] But *Carpenter* and the Court's technology exceptionalism requires that access to data following the search plays a role in deciding whether the initial conduct is a search, a concept Professor Kerr has termed "downstream analysis."[268]

261. *See, e.g.*, United States v. Perez, 484 F.3d 735, 738 (5th Cir. 2007); Commonwealth v. Martinez, 71 N.E.3d 105, 108 (Mass. 2017); Christy v. Commonwealth, No. 0169-17-3, 2018 WL 1720750, at *1 (Va. Ct. App. Apr. 10, 2018).

262. *Perez*, 484 F.3d at 738. *Perez* is not a case that challenges whether the FBI performed a search in subpoenaing Perez's records, but it is illustrative of the factual situation commonly encountered in these prosecutions.

263. *Id.*

264. *Id.*

265. *Id.*

266. *Id.*

267. *See* KERR, *supra* note 225 (manuscript at 47–48) ("A person's assigned IP address does not reveal much about them. It changes over time, but in ways that generally don't give a detailed picture of their lives.").

268. *See id.* (manuscript at 49) ("The prospect of what can be revealed when a record is combined with other unprotected records may determine if one or both of the records is something *Carpenter* protects."); *cf.* Kyllo v. United States,

This downstream analysis reveals that Professor Kerr's conclusion about subscriber records not being protected should fall. Even where the information requested from an ISP or a website does not provide a history of a person's internet activity, law enforcement can use this information to tie a person to internet activity, either through additional legal process or basic internet searches. If a person has used the same username across multiple websites or uses websites that use IP addresses as an identifier,[269] a Google search of this person's IP address or username will likely reveal a great history of that person's activity. Such a holding would not require that a court set a limit on the permissible amount of information that the downstream searches could reveal,[270] but merely to conclude that the total risk is unreasonable.

Such a holding and rationale would not be unknown in jurisprudence. In *R. v. Spencer*, a 2014 Supreme Court of Canada case, police arrested Matthew David Spencer for possessing child pornography.[271] In investigating a peer-to-peer file sharing system, police obtained an IP address that had downloaded child pornography.[272] In accordance with Canada's Personal Information Protection and Electronic Documents Act, police requested basic subscriber information from the ISP that had issued the IP address.[273] They identified the IP address as belonging to Spencer and arrested him.[274] The trial court convicted Spencer and the Court of Appeal affirmed.[275] Spencer appealed.[276]

The Supreme Court of Canada ultimately dismissed Spencer's appeal, but before they did, they concluded that Spencer possessed a reasonable expectation of privacy in his subscriber information, and thus the police conduct amounted to a

533 U.S. 27, 36–37 (2001) (finding that an inference applied to conduct does not protect the initial conduct from being a search).

269. *See, e.g.*, *Wikipedia: IP Edits Are Not Anonymous*, WIKIPEDIA, https://en.wikipedia.org/wiki/Wikipedia:IP_edits_are_not_anonymous [https://perma.cc/Q46R-HJNL] (last modified June 30, 2019).

270. For an exploration and ultimate rejection of this alternative approach to Fourth Amendment analysis called "mosaic theory," see Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

271. R. v. Spencer, [2014] 2 S.C.R. 212, 223 (Can.).

272. *Id.* at 221.

273. *Id.* at 222–23.

274. *Id.* at 223.

275. *Id.*

276. *Id.*

search.[277] The court performed a downstream analysis of the privacy risk posed by associating a person's identity with their online activity.[278] The court concluded that removing the anonymous nature of the internet would significantly harm informational privacy, linking a person to a set of online activities.[279]

Such a holding would also neatly follow from the factors and preferences laid out in *Carpenter*. Though the *Carpenter* factors likely apply better to the information gained in the second order compilation of an internet history,[280] it is the ability to associate the person with the information that renders the conduct a search and subject to the traditional Fourth Amendment protections.

C. A REASONABLE SEARCH REQUIRES A WARRANT

If lower courts hold that any of the above three scenarios constitute a search, they should additionally hold that, in most cases, the reasonableness requirement of the Fourth Amendment requires that law enforcement obtain a warrant. This conclusion derives from *Carpenter*, in which the Court reiterated a preference that a warrant be obtained when law enforcement seeks evidence of criminal wrongdoing.[281] The warrant requirement is a doctrinally-supported and superior way to safeguard internet privacy.[282]

277. *Id.* at 225.

278. *See id.* at 236 ("[T]he identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in the person's name, address and telephone number found in the subscriber information.").

279. *Id.* at 237–38.

280. *See supra* Part III.B.1.

281. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) ("[W]arrantless searches are typically unreasonable where 'a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing.'" (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652–53 (1995))); *see also* United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable.").

282. *But see* Rozenshtein, *supra* note 225, at 953–54. Professor Rozenshtein persuasively argues that instead of presumptively imposing a warrant requirement after finding a *Carpenter* search, a reasonableness test that looks at existing legislative standards could allow courts to expand Fourth Amendment coverage to more situations without infringing on legitimate government interests. While this schema may have some merit in situations beyond the scope of this Note, here it would likely reproduce the status quo by ratifying the standard set

Some may argue that the warrant requirement is ultimately toothless to protect privacy due to its ultimately flexible standard and the frequency with which magistrate judges approve warrants.[283] Even if warrants are granted with relative ease, ex ante review is superior to ex post review in the context of the warrant because ex post review cannot prevent the privacy injury.[284] That is, a warrant requirement allows a neutral magistrate to prevent the privacy injury from ever occurring rather than having to assess whether the search was reasonable after it has already occurred. Moreover, it may be more difficult for a judge to conclude probable cause did not exist when incriminating evidence sits before them. A warrant requirement, even if it is ultimately a light burden, imposes decision costs on seeking a search, which is likely to crowd out more questionable searches. Police would still be able to obtain a warrant in the vast majority of cases,[285] but fishing expeditions would be further discouraged.

CONCLUSION

The internet, for all its flaws and foibles,[286] has become an indispensable component of modern life. People use the internet to work, play, shop, learn, politically organize, find love and relationships, communicate secret thoughts and desires, and feel a little less alone in the world. The anonymity afforded by the internet allows communities to flourish and ideas to be freely exchanged. The current state of internet protections, combined with congressional inertia, threatens to clamp down on this free exchange. *Carpenter* set out a vision for how to apply the Fourth Amendment to digital privacy issues. Lower courts can and

forth in the Stored Communications Act and Pen/Trap Statutes. This is not desirable. *See supra* Part II.C.

283. *See, e.g.*, Aziz Huq, *The Latest Supreme Court Decision Is Being Hailed as a Big Victory for Digital Privacy. It's Not.*, VOX (June 23, 2018, 7:43 AM), https://www.vox.com/the-big-idea/2018/6/22/17493632/carpenter-supreme-court-privacy-digital-cell-phone-location-fourth-amendment [https://perma.cc/YYS2-HBAK]. Huq argues that law enforcement can manipulate the warrant application process to secure warrants easily. *Id.* Huq also suggests that Fourth Amendment jurisprudence surrounding the probable cause requirement, *see* Illinois v. Gates, 462 U.S. 213, 230 (1983) (establishing that probable cause is a totality of the circumstances test), and increasing criminal liability have significantly weakened the requirement, *see* Huq, *supra*.

284. *See* 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.1(a) (1987).

285. *See supra* note 186.

286. *See generally* TWITTER, https://www.twitter.com.

should begin to fulfill this vision by recognizing that collection of internet history constitutes a search. While undoubtedly the internet has nefarious uses, imposing a warrant requirement on collection of a person's internet history checks the worst uses of the internet while not chilling participation. Recognizing a Fourth Amendment interest in internet history would help preserve core privacy interests and ultimately demonstrate a commitment to a transformative technology.