American University Law Review

Volume 68 | Issue 6 Article 4

2019

Carpenter v. United States and the Emerging Expectations of Privacy in Data Comprehensiveness Applied to Browsing History

Daniel de Zayas
American University Washington College of Law

Carpenter v. United States and the Emerging Expectations of Privacy in Data Comprehensiveness Applied to Browsing History

COMMENTS

CARPENTER V. UNITED STATES AND THE EMERGING EXPECTATION OF PRIVACY IN DATA COMPREHENSIVENESS APPLIED TO BROWSING HISTORY

DANIEL DE ZAYAS*

The third-party doctrine has transcended the shift from analog to digital technology. Despite judicial cautions that the doctrine is unfit for the digital age, it persists as one of privacy's greatest limitations. However, in Carpenter v. United States*, the Supreme Court significantly circumscribed the third-party doctrine. Although the Court explicitly limited its holding to historical cell-site location information,* Carpenter *paves the way for enhancing expectations of privacy in many types of data.*

This Comment argues that Carpenter *applies to browsing history collected by third-party cookies; therefore, individuals have a reasonable expectation of privacy in their browsing history that is unabridged by the third-party doctrine. Like historical cell-site location information, browsing history collected by third-party cookies is comprehensively detailed and collected involuntarily and pervasively. In arguing that* Carpenter *applies beyond the Court's feeble restraints, this Comment derives an emerging expectation of privacy in the comprehensiveness of data from the Court's repeated focus on how granular*

* Note & Comment Editor, *American University Law Review*, Volume 69; J.D. Candidate, May 2020, *American University Washington College of Law*; B.A., International and Global Studies, 2017, *University of Central Florida*. I would like to thank Professor Jennifer Daskal for fostering my interest in privacy law and for advising my Comment. I am grateful for Andrew Urueta's guidance throughout the Comment process and for the *Law Review* staff's diligent edits and contributions. I owe so much to my family and friends whose encouragement propelled this piece. Finally, a special thank you to my parents for their unconditional love and for always supporting my passions.

data can reveal personal information. An expectation of privacy that turns on the comprehensiveness of data offers new grounds to strengthen privacy online and in the digital age.

TABLE OF CONTENTS

The internet is the most liberating tool for humanity ever invented, and also the best for surveillance. It's not one or the other. It's both.

—John Perry Barlow[1]

INTRODUCTION

When internet users think about their internet profiles, they typically think about their social media profiles on sites like Facebook and Twitter. But what about their profiles with online advertising and marketing companies like Google AdSense and DoubleClick or Acxiom? These profiles may include information that internet users have shared publicly, such as their age and sex,[2] but may also contain information that internet users have never shared nor wished to share, such as political affiliations, religious beliefs, or sexual orientation.[3] What feeds these databases? The answer is short and sweet: cookies.[4] Specifically, tracking cookies[5] allow third-party companies without any direct relation to internet users to collect, inter alia, internet users' browsing history to ascertain or infer information about them.[6]

Although these profiles and databases serve legitimate purposes for internet advertising,[7] they raise significant privacy concerns because

---

1. James Ball, *Hacktivists in the Frontline Battle for the Internet*, GUARDIAN (Apr. 20, 2012, 8:00 AM), https://www.theguardian.com/technology/2012/apr/20/ hacktivists-battle-internet [https://perma.cc/XCR9-WKWJ].

2. ALEECIA M. MCDONALD & LORRIE FAITH CRANOR, BELIEFS AND BEHAVIORS: INTERNET USERS' UNDERSTANDING OF BEHAVIORAL ADVERTISING 9–10 (2010), http://aleecia.com/authors-drafts/tprc-behav-AV.pdf [https://perma.cc/WWD5-P6LJ].

3. *See infra* notes 39, 42–45 and accompanying text (explaining how Facebook "Like" buttons can be used to infer information).

4. A cookie is a small text file that an internet user's internet browser or software program saves to the user's computer. TOBY MENDEL ET AL., GLOBAL SURVEY ON INTERNET PRIVACY AND FREEDOM OF EXPRESSION 14 (2012); *Online Tracking*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/0042-online-tracking#understanding_cookies [https://perma.cc/X978-RRFQ] [hereinafter *Online Tracking*].

5. Throughout this Comment, "tracking cookie" refers specifically to *third-party* tracking cookies. *See infra* Section II.A (distinguishing first-party cookies and third-party cookies); *see also* FRANZISKA ROESNER ET AL., DETECTING AND DEFENDING AGAINST THIRD-PARTY TRACKING ON THE WEB 7 3–4 (2012) (noting that a tracking cookie can be a first-party or third-party cookie depending on what website the user is currently accessing).

6. *See infra* notes 35–45 and accompanying text (explaining how third-party advertising companies and data brokers use third-party cookies).

7. *See, e.g.*, Sophie C. Boerman et al., *Online Behavioral Advertising: A Literature Review and Research Agenda*, 46 J. ADVERT. 363, 363 (2017) (noting that monitoring and collecting internet users' online behavior allows advertisers to solicit individually targeted advertisements to optimize a business's returns on digital advertisements); *Google Analytics Cookie Usage on Websites*, GOOGLE,

they become "one-stop shops" for the government to mine internet users' browsing history and other personal information.[8] Internet users and companies are legally restrained and financially disincentivized from challenging these government practices, marring the privacy landscape with a void of privacy protections.[9]

Generally, the government must obtain a search warrant to acquire the contents of electronic communications;[10] however, the same requirement does not apply to browsing history collected by tracking

---

https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage?hl=en [https://perma.cc/NSS9-LT3A] (last updated Aug. 9, 2018) (noting that first-party cookies identify new users, count user re-visits, log which sites visitors come from, and track how long they use a website). *But see* Robert Heaton, *How Does Online Tracking Actually Work?*, ROBERT HEATON (Nov. 20, 2017), https://robertheaton.com/2017/11/20/how-does-online-tracking-actually-work [https://perma.cc/W38B-6MVQ] (arguing that cookies are unnecessary because website server logs generate the same information).

8. Ashkan Soltani et al., *NSA Uses Google Cookies to Pinpoint Targets for Hacking*, WASH. POST (Dec. 10, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/?utm_term=.5364b200ccbe [https://perma.cc/9YMV-RPWZ] ("'[W]e need to track everyone for advertising' translates into the government being able to track everyone everywhere." (quoting Chris Hoofnagle, Professor, University of California Berkeley School of Law)).

9. *See* Jennifer Daskal, *Notice and Standing in the Fourth Amendment: Searches of Personal Data*, 26 WM. & MARY BILL RTS. J. 437, 439–41 (2017) (observing that the government may delay notifying an individual that his information has been searched, as well as obtain a gag order to enjoin third-party providers from notifying the individual); *EU "e-Evidence" Proposals Turn Service Providers into Judicial Authorities*, (Apr. 17, 2018), https://edri.org/eu-e-evidence-proposals-turn-service-providers-into-judicial-authorities [https://perma.cc/WEL7-XRAL] (highlighting that companies, unlike states, are not legally obligated to defend individuals' privacy rights); Eleni Kyriades, *Digital Free for All Part Deux: European Commission Proposal on E-Evidence*, JUST SECURITY (May 17, 2018), https://www.justsecurity.org/56408/digital-free-part-deux-european-commission-proposal-e-evidence [https://perma.cc/NY47-WGWD] (noting that companies are not economically incentivized to protect individuals' privacy rights). A recent study highlights the vulnerability of internet users' privacy, reporting that 45% of the 600 websites analyzed did not require the government to obtain a subpoena or warrant before disclosing users' personally identifiable information. RAZIEH NOKHBEH ZAEEM & K. SUZANNE BARBER, A STUDY OF WEB PRIVACY POLICIES ACROSS INDUSTRIES 10 (2018).

10. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511(3)(a) (2012) (prescribing that any "person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient"); *see also In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106–07 (9th Cir. 2014) (interpreting "content" under 18 U.S.C. § 2511(3)(a) as excluding browsing history).

cookies and possessed by third-party companies.[11] This discrepancy can be attributed to the third-party doctrine, which mandates that a person does not have a reasonable expectation of privacy in information voluntarily conveyed to third-parties.[12] Courts developed the third-party doctrine in a series of cases during the age of analog technology and left it almost undisturbed as society transitioned into the modern digital age.[13] However, scholars, Supreme Court Justices, and even the attorney who successfully argued a seminal third-party doctrine case, have questioned the doctrine's viability in the digital age.[14]

On June 22, 2018, the Supreme Court loosened the third-party doctrine's antiquated grasp over the digital-age when it decided *Carpenter v. United States*,[15] declining to extend the third-party doctrine to a phone user's historical cell-site location information ("CSLI") conveyed to third-party cell-phone providers.[16] The Court denoted historical CSLI as a "distinct category of information" in which phone users enjoy an unabridged expectation of privacy and recognized that historical CSLI is not voluntarily conveyed to cell-phone providers.[17]

---

11. *See infra* Section II.C.2 (identifying the privacy frameworks applicable to browsing history and tracking cookies).

12. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that even if one exhibits a subjective expectation of privacy in information voluntarily conveyed to a third party, such an expectation "is not one that society is prepared to recognize as 'reasonable'" (quoting Katz v. United States, 389 U.S. 347, 361 (1967))).

13. *Infra* Section II.B.2.

14. *See, e.g.*, United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (advancing that the third-party doctrine is "ill suited to the digital age"); Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1252 (2009) (scrutinizing several justifications and explanations of the third-party doctrine and suggesting a reconceptualized third-party doctrine that requires the government to obtain a warrant to access an individual's private disclosures to a third-party); Stephen H. Sachs, *The Supreme Court's Privacy Precedent Is Outdated*, WASH. POST (Nov. 26, 2017), https://www.washingtonpost.com/opinions/the-supreme-courts-privacy-precedent-is-outdated/2017/11/26/fe9d1dd0-cfb2-11e7-81bc-c55a220c8cbe_story.html?utm_term=.0c0f9658495a [https://perma.cc/7XVH-TTUY] (statement of Stephen H. Sachs, Counsel for Maryland, *Smith v. Maryland*) (stating that "[*Smith v. Maryland*] has long since outlived its suitability as precedent" and that "no one involved in the case could foresee the digital revolution that was to come").

15. 138 S. Ct. 2206 (2018), *rev'g* 819 F.3d 880 (6th Cir. 2016).

16. *Id.* at 2217 n.3, 2219 (holding that the government must obtain a search warrant to access seven days of historical CSLI).

17. *Id.* at 2219.

Despite the Court's monumental decision, its broad reasoning left several questions unanswered—including the decision's true scope.[18]

This Comment argues that courts should interpret the holding in *Carpenter v. United States* to require the government to obtain a warrant before acquiring browsing history collected by tracking cookies because internet users have a reasonable expectation of privacy in their browsing history, and browsing history is not subject to a reduced expectation of privacy nor voluntarily conveyed by tracking cookies.

Part I.A explains the nuances and functions of cookies, and Part I.B highlights practical concerns about tracking cookies.[19] Part II.A.1 briefly surveys various conceptualizations of privacy before Part II.A.2 reviews the evolution of the Fourth Amendment, specifically from its early precepts to recent technology-oriented jurisprudence.[20] Parts II.B–C delineate how the misplaced trust doctrine influenced the third-party doctrine and identifies how the third-party doctrine limits privacy interests online.[21] Next, Parts II.D–E unpack *Carpenter v. United States* and its implications, positing that the Court's reasoning indicates that *Carpenter*'s scope reaches far beyond its limited holding.[22] Part III.A draws upon technology-oriented Fourth Amendment jurisprudence to advance an emerging expectation of privacy in the comprehensiveness of the information sought and illustrates how this expectation remedies complex, nuanced, and inadequate privacy frameworks while affording privacy interests to browsing history.[23] Part III.B.1–2 argues that the third-party doctrine does not apply to browsing history collected by tracking cookies.[24] Finally, Part III.C recommends interpreting the third-party doctrine more closely to its misplaced trust doctrinal roots to inhibit the government from appropriating the private sector for retrospective information and to reform the third-party doctrine.[25] This Comment concludes that courts should interpret *Carpenter* as rendering the third-party doctrine inapplicable to browsing history collected by tracking cookies to revitalize Fourth Amendment protections in the digital age.

---

18. *Infra* Section II.E (highlighting how courts have navigated applications of the third-party doctrine post-*Carpenter* to other types of data beyond historical CSLI).
19. *Infra* Sections II.A; II.B.
20. *Infra* Section II.A.1–2.
21. *Infra* Section II.B–C.
22. *Infra* Section II.D–E.
23. *Infra* Section III.A.
24. *Infra* Section III.B.1–2.
25. *Infra* Section III.C.

I. WHAT ARE COOKIES AND ONLINE PROFILING?

Strengthening online privacy rights first requires identifying and understanding how information is collected online. The following sections explain how internet users encounter and acquire cookies and proceeds to distinguish between distinct types of cookies. Not every cookie threatens internet users' privacy; in fact, many cookies provide benign conveniences that facilitate online activity. Understanding cookies will help identify when and how cookies hinder internet users' control over their personal information.

A. Cookies and Online Tracking

A cookie is a small text file that an internet user's internet browser or software program saves to the internet user's computer.[26] Generally, an internet user's browser acquires cookies during the technological exchange between the user's browser and a webpage that the user directs the browser to access. When a user attempts to access a webpage, the user's browser sends the website's server a message, called a Hypertext Transfer Protocol ("HTTP") request, asking the server to provide the content of the webpage for the user's browser to load, thus providing "access" to the webpage.[27] While providing the requested content, the website's server also provides "any cookies it would like [the user's] browser to have," which are stored in a cookie file in the user's browser.[28] Each cookie generates a unique ID number for the user and records the website to which the cookie belongs.[29] When the user revisits the website, the user's browser attaches the cookies to every future HTTP request the browser makes to the website.[30]

There are three main types of cookies: first-party cookies, third-party cookies (tracking cookies),[31] and Flash cookies. In 1994, Netscape engineer Lou Montulli invented the first-party cookie—a cookie

---

26. MENDEL ET AL., *supra* note 4; *Online Tracking*, *supra* note 4.

27. Heaton, *supra* note 7.

28. Marshall Brain, *How Internet Cookies Work: How Do Web Sites Use Cookies?*, HOWSTUFFWORKS, https://computer.howstuffworks.com/cookie3.htm [https://perma.cc/RA39-EY7J]; Heaton, *supra* note 7.

29. Heaton, *supra* note 7; *see also What Information Is in a Cookie?*, ALLABOUTCOOKIES.ORG, http://www.allaboutcookies.org/cookies/what-information-in-cookie.html [https://perma.cc/M9T8-6DMT] (noting that cookies containing personal identifying information are generally encrypted for protection).

30. Heaton, *supra* note 7.

31. First- and third-party cookies are both technically Hypertext Markup Language (HTML) cookies. PETER SWIRE & DEBRAE KENNEDY-MAYO, U.S. PRIVATE-SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS 119 (Julia Homer ed., 2d ed. 2018).

placed on a computer from the website visited[32]—to give e-commerce stores the personal touch they lacked compared to real stores.[33] First-party cookies allow a website to remember a user's name, login information, preferences, and items in an online shopping cart.[34]

Third-party cookies are cookies belonging to a website other than the website the user is currently accessing.[35] Infamously known as "tracking cookies," companies without any direct relationship to an internet user, such as advertising companies or web analytic firms, use these cookies to monitor users' browsing history across different websites.[36] By placing their tracking cookies on websites within their advertising network, these companies can track internet users across websites and record their browsing history.[37] Companies then use this information to identify a user's interests and to tailor advertisements to those interests, ultimately enhancing the likelihood that a user will purchase a good or service, and consequently increasing revenue for advertisers and advertisement publishers.[38]

---

32. ROESNER ET AL., *supra* note 5, at 3–4.

33. *See* Solveig Singleton, *How Cookie-Gate Crumbles*, CATO INST. (July 11, 2000), https://www.cato.org/publications/commentary/how-cookiegate-crumbles [https://perma.cc/5PDW-7AJS] (stating that, without information about visitors, websites view return customers as anonymous strangers); *see also* Viktor Mayer-Schönberger, *Demystifying Lessig*, 2008 WIS. L. REV. 713, 741 (positing that the original cookies were invented to remedy short-term, single session problems like website "statelessness" and lack of personalization, as well as to facilitate voting).

34. *Online Tracking*, *supra* note 4.

35. ROESNER ET AL., *supra* note 5, at 2.

36. Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273, 276 (2012); Benjamin Strauss, *Online Tracking: Can the Free Market Create Choice Where None Exists?*, 13 CHIC.-KENT J. INTELL. PROP. 539, 541 (2014); *see* ROESNER ET AL., *supra* note 5, at 3 (explaining that "tracker" cookie is more technically accurate because "a given cookie can be considered a first-party or a third-party cookie depending on the current browsing context").

37. GERTJAN FRANKEN ET AL., WHO LEFT OPEN THE COOKIE JAR? A COMPREHENSIVE EVALUATION OF THIRD-PARTY COOKIE POLICIES 153 (2018).

38. *See Back to the Basics: What is Behavioral Targeting?*, LOTAME (Sept. 17, 2018), https://www.lotame.com/what-is-behavioral-targeting [https://perma.cc/BM6C-AZEY] (explaining how targeted advertising, or "behavioral advertising," benefits the advertising technology industry and consumers); *see also* J. HOWARD BEALES & JEFFREY A. EISENACH, NAVIGANT ECONS., AN EMPIRICAL ANALYSIS OF THE VALUE OF INFORMATION SHARING IN THE MARKET FOR ONLINE CONTENT 1, 8–9 (2014), http://images.politico.com/global/2014/02/09/beales_eisenach_daa_study.pdf [https://perma.cc/4HGW-YUMG] (concluding that advertisers may pay advertisement publishers 200% more to deliver a tailored advertisement to a user). *But see* VERONICA MAROTTA ET AL., ONLINE TRACKING AND PUBLISHERS' REVENUES: AN EMPIRICAL ANALYSIS 20, 27 (forthcoming 2019), https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf

Generally, an internet user acquires a tracking cookie without ever visiting the third-party's website. For example, when an internet user visits a website featuring a Facebook "Like" button, tracking cookies embedded in the button automatically prompt Facebook's servers to check whether the user's HTTP request contains its tracking cookie.[39] If the request does not contain Facebook's tracking cookie, the user's browser saves a new tracking cookie on the user's computer, and Facebook creates an advertising profile for the user.[40] When the internet user next submits an HTTP request to that website or another website featuring Facebook tracking cookies, Facebook's server recognizes the user's tracking cookie and records the user's browsing history in its profile of the user.[41]

After recording the user's browsing history, companies analyze the data to ascertain or infer personal information, such as the user's age, sex, sexual orientation, physical location, occupation, educational level, and interests, to supplement the user's profile.[42] These seemingly innocuous individual inferences gradually paint detailed profiles about users.[43] Companies may also infer personal

---

[https://perma.cc/4DNH-BHMG] (challenging the economic efficacy of behavioral tracking and reporting that behavioral advertising increases advertisement publishers' revenues by 4% per advertisement).

39. *See* Daniel Kahn Gillmore, *Facebook Is Tracking Me Even Though I'm Not on Facebook*, ACLU (Apr. 5, 2018), https://www.aclu.org/blog/privacy-technology/internet-privacy/facebook-tracking-me-even-though-im-not-facebook [https://perma.cc/5AER-8DPC] (noting that a Facebook "Like" button on another website enables Facebook to record the website on which a user encountered the "Like" button as well as additional browsing history); *see also Facebook, Social Media Privacy, and the Use and Abuse of Data, Before the S. Comm. on Commerce, Science, and Transport. and the S. Comm. on Judiciary*, 115th Cong. 23 (2018), https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf [https://perma.cc/6T6A-6UH7] (statement of Mark Zuckerberg, CEO, Facebook) (disclosing that, in addition to the "Like" button, the Facebook "Share" button, which is embedded on 931,000 non-Facebook websites, also sets tracking cookies).

40. Gillmore, *supra* note 37.

41. *Id.*

42. MCDONALD & CRANOR, *supra* note 2, at 2; *see* Michal Kosinski et al., *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 PROC. NAT'L ACAD. SCI. U.S. 5802, 5803 (2013) (reporting that, by analyzing participants' Facebook "Likes," researchers correctly discerned 88% of the participants' sexual orientation and 85% of participants' political associations).

43. *See* FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 46, 48–49 (2014) (acknowledging that data brokers collect, analyze, and utilize information about an internet user to create valuable, "detailed composite[s] of the consumer's life"); Soltani et al., *supra* note 8 (reporting that the NSA has used cookies to identify and target a suspect for remote hacking).

information and associations that an internet user has not otherwise shared by cross-referencing their compiled user profiles with information from other companies.[44]

Most consumers are unaware of these data practices;[45] however, websites are increasingly notifying internet users about their cookie practices, as well as requiring them to "opt-in," to comply with the recently implemented General Data Protection Regulation ("GDPR").[46]

Finally, Flash cookies, referring to Adobe Flash Player, are special cookies that regenerate deleted tracking cookies.[47] Flash cookies are saved in a location separate from tracking cookies,[48] shielding Flash

---

44. EMILEE RADER, AWARENESS OF BEHAVIOR TRACKING AND INFORMATION PRIVACY CONCERN IN FACEBOOK AND GOOGLE 59 (2014); *see* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/64JU-W572] (recalling that Target marketing employees asked a Target statistician, "If we wanted to figure out if a customer is pregnant, even if she didn't want us to know, can you do that?").

45. FTC, *supra* note 43, at 46.

46. Council Regulation (EU) 2016/679, pmbl., of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) ¶ 1, ¶ 32 [hereinafter GDPR] (requiring websites to give clear, concise, and non-disruptive notice and to receive affirmative and unambiguous consent from an internet user before collecting "personal data" about the internet user). Under the GDPR, "personal data" refers to, in relevant part, any information about an identifiable natural person who may be directly or indirectly identified by an identification number or online identifier. *Id.* art. 4, ¶ 1. The GDPR explicitly recognizes "cookie identifiers" under the "personal data" umbrella, noting that cookie identifiers "may be used to create profiles of the natural persons and identify them." *Id.* pmbl. ¶ 30.

47. Elspeth A. Brotherton, *Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine*, 61 EMORY L.J. 555, 564 (2012); *Online Tracking*, *supra* note 4. Likened to "a normal browser cookie on steroids," Flash cookies have greater capacity and more features than first and third-party cookies. *See An Introduction to Flash Cookies; How to Manage Them*, PRACT. ECOMMERCE (Mar. 16, 2011), https://www.practicalecommerce.com/An-Introduction-to-Flash-Cookies-How-to-Manage-Them [https://perma.cc/P39M-93VE]. For example, Flash cookies generally store twenty-five times more data than first- and third-party cookies. ALEECIA M. MCDONALD & LORRIE FAITH CRANOR, A SURVEY OF ADOBE FLASH LOCAL SHARED OBJECTS TO RESPAWN HTTP COOKIES 3 (2011).

Additionally, unlike first- and third-party cookies that may eventually expire, Flash cookies do not expire or delete unless an internet user finds and deletes the cookies. *Id.*

48. Flash cookies are stored offline in Adobe Flash Player. *Online Tracking*, *supra* note 4. One of the only ways to manage and delete Flash cookie is to visit Adobe's website. *Flash Player Help*, ADOBE, http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html [https://perma.cc/YG5R-U8U9].

cookies from most users' attempts to delete their cookies and ensuring the Flash cookies can regenerate deleted tracking cookies in all internet browsers on a computer.[49]

B. Practical Concerns Raised by Tracking Cookies

Tracking cookies have fundamentally diverged from the original purpose of cookies and now raise significant privacy concerns as Americans increasingly use the internet.[50] First, tracking cookies have enabled websites and advertisers to track internet users and to create concentrated databases of profiles of billions of people.[51] While some databases may be obvious, such as Facebook's collection of profiles of 1.65 billion individuals, other databases, like AddThis's profiles of 1.9 billion people, are less apparent.[52] Similarly, tracking cookies are rampant across the internet, thus ensuring that internet users' browsing history will be tracked.[53]

---

49. ASHKAN SOLTANI ET AL., FLASH COOKIES AND PRIVACY 158 (2009) (advising that erasing a browser's cookies, cache, search history, and private data will not delete Flash cookies); *see* MCDONALD & CRANOR, *supra* note 47.

50. *See* Monica Anderson et al., *10% of Americans Don't Use the Internet. Who Are They?*, PEW RES. CTR. (Apr. 22, 2019), http://www.pewresearch.org/fact-tank/2018/03/05/some-americans-dont-use-the-internet-who-are-they [https://perma.cc/9QMQ-35G3] (documenting that 90% of Americans now use the internet compared to only 52% in 2000); *see also* Andrew Perrin & Jingjing Jiang, *About a Quarter of U.S. Adults Say They Are "Almost Constantly" Online*, PEW RES. CTR. (Mar. 14, 2018), http://www.pewresearch.org/fact-tank/2018/03/14/about-a-quarter-of-americans-report-going-online-almost-constantly [https://perma.cc/DWB7-2B5S] (reporting that 77% of Americans use the internet daily, 43% use the internet several times a day, and 26% use the internet "almost constantly"). *Compare, e.g.*, Shayndi Raice & Julia Angwin, *Facebook 'Unfair' on Privacy*, WALL ST. J. (Nov. 30, 2011), https://www.wsj.com/articles/SB10001424052970203441704577068400622644374 ("The very fundamental business model of Facebook is to collect information about you and use it to sell ads."), *with supra* note 33 (explaining how cookies initially only brought personalization to a business model).

51. *See* Ibrahim Altaweel et al., *Web Privacy Census*, J. TECH. SCI. (Dec. 15, 2015), https://techscience.org/a/2015121502 [https://perma.cc/SYK6-NZ75] (finding Google tracking technology on "92 of the top 100 most popular websites and on 923 of the top 1,000 websites").

52. Boerman et al., *supra* note 7, at 364; *see also* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1412 (2001) (recalling that, in 1999, Google DoubleClick had profiles for eighty million customers). *See generally* Nurie Mohamed, *You Deleted Your Cookies? Think Again*, WIRED (Aug. 10, 2009), https://www.wired.com/2009/08/you-deleted-your-cookies-think-again [https://perma.cc/BS9V-E29J] (noting that 300,000 companies use AddThis for ad placement).

53. *See* Altaweel et al., *supra* note 51 (finding that the top 100 internet sites contained 6280 cookies—83% of which were third-party cookies); MCDONALD &

Similarly, the inability to opt out of tracking cookie data collection exacerbates privacy concerns raised by these databases. If internet users read a website's privacy policy and wish to remove the tracking and Flash cookies lodged in their computers, most website privacy policies do not identify or disclose discreet third-party data collectors, thus rendering most internet users' choices about their data sharing "[i]nvisible and [i]ncomplete."[54] Moreover, most attempts to remove or inhibit the collection of tracking cookies are futile. This futility is due, in part, to Flash cookies that regenerate deleted cookies, unbeknownst to users.[55] Similarly, "Do Not Track" settings[56] in internet browsers have failed because companies are not legally required to honor "Do Not Track" requests.[57] Accordingly, many companies explicitly state in their privacy policies that they do not honor "Do Not Track" requests.[58]

CRANOR, *supra* note 2, at 2 (highlighting that Google tracks about 90% of internet users).

54. TIMOTHY LIBERT, AN AUTOMATED APPROACH TO AUDITING DISCLOSURE OF THIRD-PARTY DATA COLLECTION IN WEBSITE PRIVACY POLICIES 211 (2018) (reporting that, while an average of 22% of website privacy policies disclosed that user information would be conveyed to Google, Facebook, or Twitter, only 0.3% of privacy policies disclosed that user information would be conveyed to Acxiom); *see* FTC, *supra* note 43, at 49.

55. *See supra* notes 47–49 (detailing the discreet and strategic use of Flash cookies); *see also* Brotherton, *supra* note 47, at 563 (noting that ad networks have implemented mechanisms to prevent users from removing tracking cookies). Furthermore, even if astute internet users visit third-parties' websites to opt out of their cookie practices, their efforts may be stymied by unclear and confusing opt-out choices. *See* FTC, *supra* note 43, at 49 (noting that data brokers' websites are not "consumer-facing," obfuscating internet users' ability to control whether or how their information is collected).

56. When activated, the "Do Not Track" setting prompts an internet user's browser to request that each website that an internet user visits does not track the user. *See* Brotherton, *supra* note 47, at 569 (comparing the "Do Not Track" setting to the Do Not Call list for telemarketing).

57. *See Online Tracking*, *supra* note 4 (noting that a company is only legally obligated to fulfill "Do Not Track" requests if the company commits to honoring them). Although there have been coordinated efforts to standardize and regulate "Do Not Track" requests, these too have proven unsuccessful. *See Do Not Track*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/do-not-track [https://perma.cc/2M7V-SWBA] (noting that negotiations to standardize "Do Not Track" practices collapsed when the Digital Advertising Alliance—to which companies, such as Google, Facebook, and Microsoft belong—withdrew from the negotiations); *see also* Consumer Watchdog *Petition for Rulemaking to Require Edge Providers to Honor 'Do Not Track' Requests*, 30 FCC Rcd. 12424 (2015) (dismissing a petition to regulate edge providers [suppliers of content], reaffirming that "[t]he [FCC] has been unequivocal in declaring that it has no intent to regulate edge providers").

58. *See, e.g.*, *Privacy Policy*, TWITTER, https://twitter.com/en/privacy [https://perma.cc/8HUT-C3TZ] ("We do not support the Do Not Track browser option.");

II. LEGAL FRAMEWORKS APPLICABLE TO BROWSING HISTORY AND COOKIES

To understand the privacy interests in browsing history, Part II.A briefly surveys evolving conceptions of privacy before charting the sea changes in Fourth Amendment jurisprudence between privacy grounded in property rights versus "expectations of privacy." Part II.B identifies the limitations on privacy rights under modern interpretations of the Fourth Amendment and the third-party doctrine, and Part II.C.1–2 explores the privacy interests recognized within the doctrine's confines. Part II.D–E unpacks the Supreme Court's recent decision in *Carpenter v. United States*, explaining the Court's curtailment of the third-party doctrine as applied to historical CSLI and stoking the debate that *Carpenter*'s holding applies to additional types of information.

A. Privacy and the Fourth Amendment

Defining "privacy" has long eluded precise resolve. Despite its perennial value that predates the United States' founding, "[f]ew values so fundamental to society as privacy have been left so undefined."[59] Although privacy remains undefined today, surveying various conceptualizations of privacy in American history may elucidate its core tenets.

1. Evolving conceptions of privacy

In the colonial era, privacy safeguarded four aspects of individualism: "personal autonomy, emotional release, self-evaluation, and limited and protected communication."[60] In 1890, Samuel Warren and Louis Brandeis

---

Privacy Statement, NETFLIX, https://help.netflix.com/legal/privacy [https://perma.cc/YXY8-KP2K] ("At this time, we do not respond to Web browser 'do not track' signals"); *Target Privacy Policy*, TARGET, https://www.target.com/c/target-privacy-policy/-/N-4sr7p [https://perma.cc/T98X-YGCC] (disclosing that "we do not respond to browser 'do not track' signals," but users may "opt out of interest-based advertising"). Additionally, Google and Facebook have both announced that they do not honor "Do Not Track Requests" because internet users do not understand what "do not track" actually means. Elise Ackerman, *Google and Facebook Ignore "Do Not Track Requests, Claim They Confuse Consumers*, FORBES (Feb. 27, 2013), https://www.forbes.com/sites/eliseackerman/2013/02/27/big-internet-companies-struggle-over-proper-response-to-consumers-do-not-track-requests [https://perma.cc/SC3C-JE4P] (identifying concerns that honoring "Do Not Track" requests may impede features that consumers did not intend to change and, consequently, not meet users' expectations).

59. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967). While no definitive answer explains why privacy is not mentioned in the Constitution, "[t]o define is to limit" and perhaps its absence is an intentional safeguard for the right to privacy. *See* OSCAR WILDE, THE PICTURE OF DORIAN GRAY 148 (1890).

60. DAVID H. FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND 3 (1972). More specifically, privacy protected colonists from having to disclose their personalities,

(later Justice Brandeis) defined the right to privacy as the "right of the individual to be let alone."[61] Seventy years later, William Prosser categorized privacy cases into four distinct torts: intruding into another's solitude, publicly disclosing another's embarrassing private details, misrepresenting another's public image, and advantageously appropriating another's likeness.[62] In 1967, Professor Alan Westin denoted privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[63]

Recently, Daniel Solove has posited that privacy touches many facets of life as pluralistic protections against a set of problems that "do not share one element in common but that nevertheless bear a resemblance to each other."[64] While privacy persists as a "Cheshire cat of values," it continues to indelibly influence American jurisprudence and society.[65]

---

thus "expos[ing themselves] to the shame of total understanding." *Id.* at 4. Privacy also championed the sanctity of emotional release, providing a colonist refuge from the stresses of daily life and social norms. *See id.* at 4 (quoting DIARY AND AUTOBIOGRAPHY OF JOHN ADAMS, I, 96 (L. H. Butterfield ed., 1961)).

> I must converse and deal with Mankind, and move and stir from one scene of Action and Debate and Business, and Pleasure, and Conversation, to another and grow weary all before I shall feel the strong Desire of retiring to contemplation on Men and Business and Pleasure and Books. After hard Labour at Husbandry, Reading and Reflection in Retirement will be a Relief and a high refined Pleasure.

Id. (quoting John Adams). In addition, privacy safeguarded an individual's ability to reflect upon experiences, events, and religious engagements. *Id.* Finally, privacy fostered open and safe communication with others without fear that the communications would be leaked to the public, thus allowing an individual to maintain distinct interpersonal relationships. *Id.* at 4–5.

61. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 200, 211 (1890) (identifying the inadequacies of the existing privacy protections afforded by contract law and property law).

62. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

63. WESTIN, *supra* note 59.

64. *See* Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 756, 763 (2007) (reconciling conceptualizations of privacy that disregard that "not all privacy problems are equal" and that privacy's values depend on the problem or harm at issue).

65. *But see* JONATHAN FRANZEN, *Imperial Bedroom*, *in* HOW TO BE ALONE: ESSAYS 42 (2002) (describing privacy as "the rallying cry of activists fighting for reproductive rights, against stalkers, for the right to die, against a national health-care database, for stronger data-encryption standards, against paparazzi, for the sanctity of employer e-mail, and against employee drug testing," but "[o]n closer examination, though, privacy proves to be the Cheshire cat of values: not much substance, but a very winning smile").

2. Evolution of the Fourth Amendment

Although neither the Constitution nor the Bill of Rights mention the word "privacy," the Fourth Amendment is one implicit manifestation of the amorphous notion of privacy.[66] The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" absent a warrant issued upon a showing of probable cause.[67]

The Court's early Fourth Amendment jurisprudence interpreted the Fourth Amendment through a property-rights framework.[68] However, in 1967, Fourth Amendment jurisprudence evolved when the Court decided *Katz v. United States*,[69] introducing the reasonable expectation of privacy test in holding that the government conducted an unreasonable search when it recorded the contents of the defendant's phone conversation in a public telephone booth.[70] In rejecting the defendant's property-based privacy arguments,[71] the Court clarified that "the Fourth Amendment protects people, not places."[72]

In his concurrence, Justice Harlan introduced the two-pronged "reasonable expectation of privacy" *Katz* test that has become the

66. *See id.* (recognizing that the Third and Fifth Amendments also implicitly address privacy).

67. U.S. CONST. amend. IV.

68. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 456–57, 465–66 (1928) (declining to extend the Fourth Amendment to wiretapped telephone lines located outside the defendants' properties, holding that the government did not conduct a search or seizure because the government did not search or seize any person, papers, or "tangible material effects"), *overruled by* Katz v. United States, 389 U.S. 347 (1967); Boyd v. United States, 116 U.S. 616, 634–35, 638 (1886) (invoking both the Fourth and Fifth Amendments to hold that the compulsory production of a person's papers to substantiate a criminal charge against that person constitutes an unreasonable search and seizure).

69. 389 U.S. 347, 359 (1967), *superseded by statute*, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968).

70. *See id.* at 348, 351–53 (finding that the recording of the contents of Katz's conversation "violated the privacy upon which [Katz] justifiably relied while using the telephone booth"); *id.* at 360–61 (Harlan, J., concurring) (introducing the reasonable expectation of privacy test to clarify the majority's holding); *see also* Peter C. Ormerod & Lawrence J. Trautman, *A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age*, 28 ALB. L.J. SCI. & TECH. 73, 116 (2018) (denoting *Katz* as the source of the "content and non-content" distinction in third-party doctrine precedent).

71. On appeal, the defendant argued that a public telephone booth constitutes a constitutionally protected area and that physical trespass is not necessary to conduct an unconstitutional search and seizure. *Katz*, 389 U.S. at 347, 349–51 (majority opinion).

72. *Id.* at 351.

touchstone of Fourth Amendment privacy rights.[73] Under the *Katz* test, the Fourth Amendment recognizes and protects an expectation of privacy when an individual has "exhibited an actual (subjective) expectation of privacy" and that "expectation [is] one that society is prepared to recognize as 'reasonable.'"[74]

Although some have lauded the *Katz* reasonable expectation of privacy test,[75] others have severely criticized it.[76] Nevertheless, the Supreme Court has generally applied the *Katz* test using a normative framework,[77] balancing several factors; including, inter alia, assumption of risk, property interests, location, and expectations of privacy; to determine whether the Fourth Amendment protects a specific privacy interest.[78] Therefore, understanding these limitations and normative factors may clarify the current scope of the Fourth Amendment.

---

73. *Id.* at 360–61 (Harlan, J., concurring); *see* California v. Ciraolo, 476 U.S. 207, 211 (1986) (identifying Justice Harlan's two-pronged test in *Katz* as the touchstone of Fourth Amendment privacy rights).

74. *Katz*, 389 U.S. at 361.

75. *See, e.g.*, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 382 (1974) (championing *Katz* as the "watershed in fourth amendment jurisprudence"); James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 649 (1985) (recognizing the decision as "[t]he Katz Revolution").

76. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2265 (2018) (Gorsuch, J., dissenting) ("[W]e still don't even know what [*Katz*'s] 'reasonable expectation of privacy' test *is*. Is it supposed to pose an empirical question . . . or a normative one . . . ? Either way brings problems."); United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring) ("[The *Katz* test] involves a degree of circularity, and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks. In addition, the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations."); ANDREW E. TASLITZ ET AL., CONSTITUTIONAL CRIMINAL PROCEDURE 107 (4th ed. 2010) (noting that the Supreme Court has never defined "reasonableness" pertaining to expectations of privacy nor stated whether the Court evaluates reasonableness through a majoritarian or normative framework); Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 114 (2015) (arguing that subjective expectations of privacy are irrelevant under *Katz*); Erik Luna, *The* Katz *Jury*, 41 U.C. DAVIS L. REV. 839, 846 (2008) (scrutinizing the Court's post-*Katz* decisions as "outcome-based jurisprudence" that use "haphazard" and inconsistent analyses).

77. *See Carpenter*, 138 S. Ct. at 2246 (Thomas, J., dissenting) (stating that, despite *Katz*'s majoritarian framing, the Court's jurisprudence can only be understood through a normative framework that asks "whether a particular practice *should* be considered a search under the Fourth Amendment").

78. *See* TASLITZ ET AL., *supra* note 76, at 107–09, 135–45 (noting that the Court becomes "society's representative" when determining whether an expectation of privacy is objectively reasonable and identifying additional factors, such as social custom and legality or intimacy of activities involved).

B. Limitations on Expectations of Privacy: The Third-Party Doctrine

Amongst one of the most controversial aspects of the *Katz* reasonable expectation of privacy test is the third-party doctrine. Principled upon an assumption of the risk theory, the third-party doctrine mandates that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[79] The third-party doctrine has evolved from its misplaced trust doctrinal roots and now serves as an invaluable tool for the government to obtain records from third parties.[80] This section briefly explains misplaced trust doctrine jurisprudence before exploring the third-party doctrine's evolution and rationale.

1. Misplaced trust doctrine

The misplaced trust doctrine states that an individual waives his Fourth Amendment protections when he confides his wrongdoing to another person whom he mistakenly believes will not reveal it.[81] The misplaced trust doctrine arose from cases, many decided before *Katz*, involving assertions of privacy interests in information confided to informants and undercover government agents. For example, in *On Lee v. United States*,[82] the Court held that the government did not violate the Fourth Amendment by equipping the defendant's friend with a recording device, finding the recording device indistinguishable from an agent "eavesdropping outside an open window."[83] A decade later, in *Lopez v. United States*,[84] the Court upheld an IRS agent covertly recording the defendant's attempts to bribe the agent, concluding that the defendant risked that the bribe would be "accurately reproduced in court, whether by faultless memory or mechanical recording."[85] Similarly, in *Hoffa v.*

---

79. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that even if one exhibits a subjective expectation of privacy in information voluntarily conveyed to a third party, such an expectation "is not one that society is prepared to recognize as 'reasonable'" (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring))).

80. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CALIF. L. REV. 1083, 1084–86 (2002) (arguing that, *inter alia*, the government should regulate the transfer of personal information from the private sector to the government in a way that balances privacy and effective law enforcement).

81. Chris J. Chasin, *The Revolution Will Be Tweeted, but the Tweets Will Be Subpoenaed: Reimagining Fourth Amendment Privacy to Protect Associational Anonymity*, 2014 U. ILL. J.L. TECH. & POL'Y, 1, 18–19.

82. 343 U.S. 747 (1952).

83. *Id.* at 753–54.

84. 373 U.S. 427 (1963).

85. *See id.* at 439 (rejecting that the defendant had a right to rely on the IRS agent's fallible memory).

United States,[86] the Court held that the government did not violate the Fourth Amendment when the defendant confided in a colleague who, unbeknownst to the defendant, worked for police, and the colleague subsequently testified about the defendant's statements.[87] The Court noted that, as is "inherent in the condition[] of human society," whenever an individual speaks he risks that he may be "eavesdropp[ed] or betrayed by an informer or deceived as to the identity of one with whom one deals."[88]

Post-*Katz*, the Court again upheld the misplaced trust doctrine in *United States v. White*,[89] warning that an individual committing crimes assumes the risk that his companions may be reporting to the government.[90] The following section explores how the misplaced trust doctrine served as a foundation for the third-party doctrine and delineates the rationales contouring this distinct doctrine.

2. Third-party doctrine

The modern third-party doctrine emerged from the misplaced trust doctrine. In *United States v. Miller*,[91] government agents subpoenaed the defendant's bank records to investigate tax crimes.[92] The United States Court of Appeals for the Fifth Circuit suppressed the bank records on the grounds that the government circumvented the defendant's constitutional rights by obtaining the records from a third party,[93] but the Supreme Court reversed in favor of the government.[94] First, the Court examined the nature of the records and concluded that the bank records were not "private papers" but rather negotiable instruments exposed to bank employees during the ordinary course of business.[95] Second, the Court cited the entire line of misplaced trust jurisprudence and held that the defendant could not reasonably expect privacy in records voluntarily conveyed to a third party, even if they conveyed the records only for a limited purpose.[96]

---

86. 385 U.S. 293 (1966).
87. *Id.* at 303.
88. *Id.* (quoting *Lopez*, 373 U.S. at 465 (Brennan, J., dissenting)).
89. 401 U.S. 745 (1971) (plurality opinion).
90. *Id.* at 751–52.
91. 425 U.S. 435 (1976).
92. *Id.* at 437.
93. United States v. Miller, 500 F.2d 751, 757 (5th Cir. 1974) (citing Boyd v. United States, 116 U.S. 616, 622 (1886)), *rev'd*, 425 U.S. 435, 436 (1976).
94. *Miller*, 425 U.S. at 440.
95. *See id.* at 440–42 (noting that the defendant did not possess or own the bank records).
96. *See id.* at 443 (first citing United States v. White, 401 U.S. 745, 751–52 (1971) (plurality opinion); then citing Hoffa v. United States, 385 U.S. 293, 302 (1966); and then citing Lopez v. United States, 373 U.S. 427, 439 (1963)).

Three years later, in *Smith v. Maryland*,[97] the Court held that the defendant lacked a reasonable expectation of privacy in telephone numbers dialed and subsequently intercepted by a pen register.[98] Applying the third-party doctrine refined by *Miller*, the Court held that the defendant voluntarily conveyed and exposed the dialed numbers to the telephone company and its operating equipment and, therefore, assumed the risk that the telephone company would disclose the dialed numbers to the police.[99] Addressing the technological innovation of automatic call routing and billing, the Court refused to "make a crazy quilt of the Fourth Amendment" by grounding the reasonableness of an expectation of privacy in a company's decision to use a human or automated operator.[100]

In his dissent, Justice Marshall rebuked the majority's holding, submitting that "[p]rivacy is not a discrete commodity, possessed absolutely or not at all."[101] Moreover, he doubted whether a person who knows that a telephone company records calls for billing purposes assumes that the company will convey his call information to the government.[102] Justice Marshall asserted that "[i]mplicit in the concept of assumption of risk is some notion of choice" and noted that an individual lacks such choice where the individual must accept surveillance or forgo technology essential to modern life.[103] Justice Marshall warned that making assumption of risk dispositive in determining reasonable expectations of privacy empowers the government to dictate the Fourth Amendment's scope merely by providing prior notice of surveillance.[104]

Third-party doctrine jurisprudence rests upon two underlying rationales: voluntary conveyance and reduced expectations of privacy in

---

97. 442 U.S. 735 (1979).

98. *Id.* at 745–46 (rejecting that the pen register constituted a Fourth Amendment search). A pen register is "a device that records numbers dialed from a phone line." United States v. Forrester, 512 F.3d 500, 509 (9th Cir. 2008).

99. *Smith*, 442 U.S. at 744.

100. *See id.* at 745 (rejecting the defendant's assertion that he possessed a reasonable expectation of privacy because a machine, rather than a human, ordinarily transferred his phone calls, and the machine did not record the defendant's local calls).

101. *Id.* at 749 (Marshall, J., dissenting).

102. *Id.*

103. *See id.* at 749–50 (arguing that the concept of "assumption of risk" is diluted where "individuals have no realistic alternative").

104. *See id.* (illustrating that the government could foreclose reasonable expectations of privacy in the contents of mail or phone calls merely by announcing its intent to monitor).

information knowingly shared with another.[105] Derived from *Smith* and *Miller*,[106] voluntary conveyance requires that a conveyance be intentional and presumably with the conveyor's knowledge.[107] However, consent does not subsume voluntariness,[108] thus leading several scholars to advocate that the vulnerabilities of consent in online contracting, such as agreeing to the terms of a privacy policy, militate using consent as the dispositive touchstone of fair information practices.[109] Some assert that a

---

105. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219–20 (2018) (identifying the reduced expectations of privacy and "voluntary exposure" justifications as integral to the third-party doctrine analysis).

106. *See, e.g.*, *Smith*, 442 U.S. at 745 (rejecting the defendant's expectation of privacy in the phone numbers on the grounds that they were *voluntarily conveyed* to the phone company, which had the equipment and right to record the numbers); United States v. Miller, 425 U.S. 435, 442 (1976) (observing that the defendant's bank records "contain only information *voluntarily conveyed* to the banks and exposed to their employees in the ordinary course of business").

107. *Compare* United States v. Stimler, 864 F.3d 253, 266 n.40 (3d Cir. 2017) (reaffirming *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317–18 (3d Cir. 2010), which held that CSLI is involuntarily conveyed to wireless service providers because consumers are unlikely to know that their wireless providers collect and store historical CSLI), *reh'g granted, vacated in part*, No. 15-4094, 2018 WL 4139784 (3d Cir. Aug. 30, 2018), *with* United States v. Graham, 824 F.3d 421, 430 n.12 (4th Cir. 2016) (concluding that an individual voluntarily conveys historical CSLI to wireless providers as an inherent consequence of agreeing to use and using a cell phone and noting that voluntariness, as posited by *Smith* and *Miller*, "does not require contemporaneous recognition of every detail an individual conveys to a third party"), *and* United States v. Davis, 785 F.3d 498, 512 (11th Cir. 2015) (holding that CSLI is voluntarily conveyed because users must convey CSLI, like the phone numbers in *Smith*, to complete phone calls). *But see* Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz*,* Smith*, and Electronic Surveillance Law*, 30 HARV. J.L. & TECH., 1, 30 (2016) (scrutinizing the Eleventh Circuit's interpretation of *Smith* as conflating "information that is 'necessarily' conveyed" with "knowing, voluntary conveyance").

108. *See* Schneckloth v. Bustamonte, 412 U.S. 218, 227, 248–49 (1973) (rejecting that consent alone authorizes a search of an individual not in custody and holding that the consent must be voluntarily given under the totality of the circumstances to satisfy the Fourth Amendment's reasonableness requirement).

109. *See* Lisa M. Austin, *Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 189 (Austin Sarat ed., 2015) (concluding that consent-based privacy models inadequately protect consumers considering "the emerging corporate-state nexus that has created such a striking surveillance infrastructure on the internet"); Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 956, 965–66 (2017) (arguing that fair information practices relying upon consent have ossified and must be revised). Some scholars have described consenting online as "qualitatively different" than in the real world because of the greater disparity in bargaining power between internet users and online businesses. *See* Wayne R. Barnes, *Social Media and the Rise in Consumer Bargaining Power*, 14 U. PA. J. BUS. L. 661, 661–62 (2012)

consent-based framework turns privacy rules into "formalistic exercises designed to extract consent and use the gift of control" to shift risks to consumers.[110] Others have noted that, although internet users are empowered to consent as they wish, this control may be "too much of a good thing" if users fatigue from consent requests.[111] Moreover, the consent-based framework may not adequately apply to modern information sharing practices in which the first parties with whom users interact are merely intermediaries for third parties.[112]

The second rationale—a reduced expectation of privacy in information knowingly shared—analyzes the nature of the information sought to determine whether a reasonable expectation of privacy exists in the content.[113] For example, in *Miller*, the Court held that the defendant did not have a reasonable expectation of privacy in the contents of his bank records because they were negotiable commercial instruments exposed to employees during the ordinary course of business.[114] Similarly, the Court has recognized a reduced expectation of privacy in telephone numbers dialed because the numbers alone reveal limited quantities of information voluntarily conveyed to telephone companies to use a

---

(explaining how social media bulletins have helped bridge the "complete and absolute" online bargaining disparity); Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529, 549–50, 556 (2007) (advocating for a "medium-specific contract doctrine of consent" guided by a "reasonable digital consumer standard" to reconcile contracting online and in the real world). Scholars attribute this disparity to several factors. *See, e.g.*, Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429, 480 (2002) (inability to ask an agent about terms); Matwyshyn, *supra* (easily manipulatable consent factors); Natasha Lomas & Romain Dillet, *Terms and Conditions Are the Biggest Lie of Our Industry*, TECHCRUNCH, https://techcrunch.com/2015/08/21/agree-to-disagree [https://perma.cc/4CF4-2T94] (difficulty of reading policies).

110. Hartzog, *supra* note 109, at 964.

111. *See id.* at 975 (noting that, without any alternative, consent fatigue causes internet users to consent away their privacy); *see also* Roger Brownsword, *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality*, *in* REINVENTING DATA PROTECTION? 83, 90 (Serge Gutwirth et al. eds., 2009) (warning about the dangers of the "routinisation" of consent in which internet users merely "tick the box" due to consent fatigue).

112. Hartzog, *supra* note 109, at 967–68 (noting that modern information sharing practices are predicated upon "individual-organization relationship[s]" between only two parties).

113. United States v. Miller, 425 U.S. 435, 442 (1976).

114. *Id.*

phone.[115] However, an individual may still have a reasonable expectation of privacy in information subject to a reduced expectation of privacy.[116]

C. Piecing Together the Privacy that Remains

The third-party doctrine has set bright-line boundaries constraining expectations of privacy in information voluntarily conveyed to others. However, after piecing together the privacy that remains, a disparity between the physical and virtual worlds becomes apparent. While the Supreme Court has become increasingly reluctant to extend the third-party doctrine to foreclose an expectation of privacy in one's movement and location in the physical world, other courts have not hesitated to abridge expectations of privacy in an internet user's movement from one website to another. The following sections explore this divide, setting the stage for its reconciliation.

1. Privacy interests in movements and location

The Supreme Court has recognized a limited expectation of privacy in one's location.[117] However, the Court did not originally recognize such a right. In *United States v. Knotts*,[118] the government obtained consent from a chemical seller to place a beeper inside a chemical container that the defendants, suspected of manufacturing drugs, would later purchase.[119] The government used the beeper and visual surveillance to trace the chemicals to Knotts's cabin and to obtain a search warrant.[120] The Court rejected that the warrantless monitoring violated Knotts's expectation of privacy in his movements and declined to find a reasonable expectation of privacy in one's movement where a person travels on public thoroughfares, thus voluntarily conveying his movements to anyone in

115. *See* Smith v. Maryland, 442 U.S. 735, 742–44 (1979) (noting that a pen register only collects the numbers dialed and that the defendant voluntarily exposed the numbers to the telephone company's equipment during the ordinary course of business). *But see* Riley v. California, 134 S. Ct. 2473, 2492–93 (2014) (rejecting that phone numbers accompanied by "identifying information that an individual might add" in a phone's call log are subject to a reduced expectation of privacy).

116. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (quoting *Riley*, 134 S. Ct. at 2488) ("[T]he fact of 'diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely.'").

117. *See* United States v. Jones, 565 U.S. 400, 404 (2012) (holding that the government conducts a search when it installs a tracking device on a vehicle to monitor the vehicle's movements).

118. 460 U.S. 276 (1983).

119. *Id.* at 278.

120. *Id.* at 278–79 (noting that the government did not use the beeper after locating the cabin).

sight.[121] The Court dismissed the argument that the government's use of technology could lead to pervasive surveillance of citizens, but it reserved that "different constitutional principles may be applicable" if technology eventually enables the government to conduct "dragnet-type law enforcement practices."[122]

The Court circumscribed *Knotts* in *United States v. Karo*,[123] in which a government informant notified the government that the defendants had ordered from the informant cans of chemicals for illicit drug activity.[124] Pursuant to a court order and the informant's consent, the government placed a tracking beeper in one of the cans and used the beeper and visual surveillance to follow Karo to his house and to track the can within his house.[125] Limiting *Knotts*, the Court held that monitoring a beeper in a private residence that is not open to visual surveillance constitutes an unreasonable search in violation of the Fourth Amendment.[126]

Almost thirty years after *Karo*, the Court revisited privacy interests in an individual's movements in *United States v. Jones*,[127] in which the government installed a GPS device on the defendant's vehicle and tracked its movements for twenty-eight days.[128] Writing for the Court, Justice Scalia sidestepped the *Katz* test and applied the trespass doctrine, holding that the installation of the GPS device *on* the defendant's vehicle and the monitoring of his movements constituted a search in violation of the Fourth Amendment.[129] Justice Scalia

---

121. *See id.* at 279, 281–82, 285 (equating the warrantless beeper monitoring to a government agent physically following an automobile and positing that visual surveillance would have revealed the same information conveyed by the beeper).

122. *See id.* at 283–84 (explaining that, until the government conducts such pervasive and intrusive practices, "police efficiency" does not warrant unconstitutionality).

123. 468 U.S. 705 (1984).

124. *Id.* at 708.

125. *Id.* at 708–10.

126. *See id.* at 715–17 (emphasizing that, although beepers are less intrusive than physical searches, beepers reveal important details about the "the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant").

127. 565 U.S. 400 (2012).

128. *Id.* at 402–03. The government actually obtained a warrant to install the GPS device; however, the government failed to install the device within the authorized ten-day period. *Id.* Conceding that it contravened the warrant, the government argued that it did not need a warrant to install and use the GPS tracker. *See id.* at 402, 403 n.1.

129. *See id.* at 404–05, 409 (clarifying that "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test"). The Court did not answer whether the search was unreasonable because the argument was not raised below. *Id.* at 413.

distinguished *Jones* from *Knotts* and *Karo* on the grounds that, unlike in *Knotts* and *Karo* where the government hid the beepers with the consent of third parties *before* the defendants obtained the bugged goods, Jones possessed the vehicle when the government installed and used the GPS device and, therefore, constituted a trespass.[130]

Although Justice Scalia notably resurrected property-based privacy rights, the potency of *Jones* emanates from its two concurring opinions by Justice Alito and Justice Sotomayor.[131] Justice Alito viewed *Jones* through *Katz*'s reasonable expectation of privacy test and recognized that technology can change expectations of privacy.[132] Although he acknowledged the reasonableness of the short-term monitoring of a person's public movements, Justice Alito cautioned that longer-term monitoring would violate most expectations of privacy, citing that society's expectations espouse that "law enforcement agents and others would not—and . . . could not—secretly monitor and catalogue" a person's every movement.[133]

Justice Sotomayor's concurrence doubted the utility of the majority's trespass-based holding and reliance on the third-party doctrine. Justice Sotomayor condemned the majority's reliance on the trespass-doctrine, acknowledging that modern surveillance does not require physical trespass.[134] Furthermore, Justice Sotomayor expounded upon Justice Alito's concerns about expectations of privacy against comprehensive tracking of movements, highlighting that GPS tracking produces detailed records of movements that reveal "a wealth of detail" about "familial, political, professional, religious, and sexual associations."[135] Justice Sotomayor noted that these records can be stored and mined for years,

---

130. *See id.* at 404, 409–10 (stating that the government physically occupied private property to obtain the information).

131. *See* Margot Kaminski, *Three Thoughts on* U.S. v. Jones, CONCURRING OPINIONS (Jan. 24, 2012), https://web.archive.org/web/20190219125855/https://concurringopinions.com/archives/2012/01/three-thoughts-on-u-s-v-jones.html [https://perma.cc/BR9H-YEQB] (lauding Justice Sotomayor's concurrence as having "the greatest practical impact" and denouncing Justice Alito's concurrence as "the most dangerous part of these opinions").

132. *See Jones*, 565 U.S. at 419, 427, 429 (Alito, J., concurring) (forecasting that people may eventually accept the tradeoff of increased convenience for decreased privacy).

133. *See id.* at 419, 430 (concluding that four weeks of tracking constituted "long-term monitoring" that violated the defendant's reasonable expectation of privacy); *see also* United States v. Skinner, 690 F.3d 772, 780 (6th Cir. 2012) (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)) (adding that technology has enabled the government to comprehensively track individuals in ways previously impossible).

134. *See Jones*, 565 U.S. at 414–15 (Sotomayor, J., concurring) (forecasting that the government may eventually exploit tracking devices incorporated in vehicles and smart phones).

135. *Id.* at 415 (citing New York v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

allowing the government to evade practical limitations that protect privacy rights.[136] Most notably, Justice Sotomayor doubted the viability of the third-party doctrine, labeling the doctrine as "ill suited to the digital age."[137]

2. Internet users' expectations of privacy

Courts and scholars have not uniformly recognized an expectation of privacy against tracking cookies or in browsing history.[138] Generally, parties who have challenged tracking cookies as a violation of a person's expectation of privacy in browsing history have relied upon the Stored Communications Act ("SCA").[139] Enacted as part of the Electronic Communications Privacy Act of 1986 (ECPA),[140] legislators implemented the SCA to extend Fourth Amendment privacy rights into the digital realm to protect service providers' customers and

136. *See id.* at 415–16 (advancing that unchecked surveillance could "chill[] associational and expressive freedoms" and "alter the relationship between citizen and government in a way that is inimical to democratic society" (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), vacated by *Cuevas-Perez*, 565 U.S. 1189 (2012))).

137. *See id.* at 417 (suggesting reconsideration of the third-party doctrine in the digital age "in which people reveal a great deal of information about themselves to third parties" while "carrying out mundane tasks").

138. *Compare, e.g.*, *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1274–77, 1282 (C.D. Cal. 2001) (holding that the plaintiffs' complaint sufficiently claimed that placement of cookies on personal computers violated the SCA), *and In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 508, 511, 513, 519 (S.D.N.Y. 2001) (concluding that internet access constitutes an electronic communications service but dismissing the plaintiffs' claims that DoubleClick violated, *inter alia*, the SCA and the Wiretap Act by placing cookies on the plaintiffs' computers to track users across its network websites and holding that DoubleClick's clients consented to DoubleClick intercepting the plaintiffs' communications), *with In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d 922, 936 (N.D. Cal. 2015) (dismissing the plaintiffs' claims that Facebook violated the SCA by tracking users' browsing history using tracking technology on the grounds that the SCA does not apply to information locally stored on a computer and that personal computers do not constitute "facilities" or "electronic communication providers" under the SCA), *and* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1214–15 (2004) (arguing that the SCA does not apply to tracking cookies on personal computers because personal computers are not a provider of electronic communication service ("ECS")). *See also* 18 U.S.C. § 2510(15) (2012) (defining an ECS as any service that allows a user "to send or receive wire or electronic communications").

139. 18 U.S.C. § 2701–2712 (2012).

140. *Id.* § 2510.

subscribers against "unauthorized access to, and disclosure of," their stored electronic communications held by network service providers.[141]

The SCA provides hierarchical protections depending on whether the information sought constitutes "content" or "non-content" of electronic communications.[142] "Content" includes "any information concerning the substance, purport, or meaning of that communication."[143] The government must obtain a search warrant to acquire communications content.[144]

Conversely, the SCA provides less protection for non-content information, such as "dialing, routing, addressing [or] signaling" information ("DRAS information").[145] The government may obtain non-content information; such as a subscriber's name, address, communication connection records, and payment methods; pursuant to a warrant or less demanding forms of process, such as a § 2703(d)

---

141. *See id.* § 2510(12) (defining "electronic communications" as "any transfer of signs, signals, writing, images, . . . or intelligence of any nature); S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559 (noting the disparate protections afforded to electronic communications compared to traditional mail and stating that "the law must advance with the technology to ensure the continued vitality of the fourth amendment"); Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 361 (2015) (delineating the various levels of SCA protections); Kerr, *supra* note 138, at 1209–10, 1212 (explaining that the Fourth Amendment's strong privacy protections in the physical world do not necessarily transfer into the digital realm of "ones and zeroes stored somewhere on somebody else's computer"); *see also* William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1266 (1999) ("Privacy, in Fourth Amendment terms, is something that exists only in certain types of spaces; not surprisingly, the law protects it only where it exists.").

142. *See* Eric R. Hinz, Note, *A Distinctionless Distinction: Why the RCS/ECS Distinction in the Stored Communications Act Does Not Work*, 88 NOTRE DAME L. REV. 489, 499 (2012) (delineating the various levels of protections afforded to the content of communications); *see also* Ormerod & Trautman, *supra* note 70, at 116 (denoting *Katz* as the source of the "content and non-content" distinction in third-party doctrine precedent).

143. 18 U.S.C. § 2510(8) (2012); *see also In re* Zynga Privacy Litig., 750 F.3d 1098, 1106 (9th Cir. 2014) (defining "contents" under the ECPA as "the intended message conveyed by the communication," excluding message characteristics generated during the communication).

144. § 2703(a).

145. *See id.* § 3121(c) (authorizing the government to install and use pen registers or trap and trace devices to capture non-content information); Smith v. Maryland, 442 U.S. 735, 743, 745–46 (1979) (holding that the government's use of a pen register to record telephone numbers dialed, but not the content of the communications, did not constitute an unreasonable search); H.R. REP. NO. 107-236(I), at 53 (2001) (affirming *Smith v. Maryland*'s distinction between content and non-content information).

order or a subpoena.[146] Thus, under the current legal framework, statutory privacy protections primarily turn on whether browsing history or individual Universal Resource Locators ("URLs") constitute content or non-content.

Several courts have recognized that a URL may *include* search terms that constitute content.[147] In *United States v. Forrester*,[148] the Ninth Circuit held that the government's collection of IP addresses of visited websites using a mirroring device was indistinguishable from the pen register surveillance upheld in *Smith*.[149] The court explained that IP addresses, like the telephone numbers in *Smith*, are affirmatively and voluntarily conveyed to third parties when a user navigates the internet, and that an IP address does not reveal the contents of the websites viewed.[150] However, the court excluded from its holding techniques that allow the government to collect both the IP address and the URL of webpages visited because, unlike an IP address, a URL identifies specific webpages that a user visited, thus providing a more precise and revealing picture of the user's internet activity.[151]

Similarly, in *In re Zynga Privacy Litigation*,[152] the Ninth Circuit reaffirmed that a URL may include content if search terms are

---

146. 18 U.S.C. §§ 2703(c)(1)(A)–(B), 2703(c)(2)(A)–(F) (2012); *see, e.g.*, *id.* § 2703(d) (delineating that the government may obtain a § 2703(d) order from a magistrate judge upon a mere showing of "specific and articulable facts" that the subscriber information sought is "relevant and material to an ongoing criminal investigation").

147. *See, e.g.*, *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 137–38 (3d Cir. 2015) (citing [Redacted], No. PR/TT [Redacted], at 32 (FISA Ct. 2010), https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf [https://perma.cc/8NVK-CWDQ]) (surveying the sea changes in the classification of location identifiers as content or non-contents and acknowledging the "growing chorus" of judicial recognition that "some, if not most, queried URLs do contain content"); *In re* Zynga Privacy Litig., 750 F.3d at 1108–09 (acknowledging, in dicta, that "[u]nder some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication"); United States v. Forrester, 512 F.3d 500, 510–11 n.6 (9th Cir. 2008) (stating, in dicta, that surveillance techniques that collect both the IP addresses and URLs of webpages visited "might be more constitutionally problematic").

148. 512 F.3d 500 (9th Cir. 2008).

149. *Id.* at 505, 511.

150. *Id.* at 510.

151. *See id.* at 510–11 n.6 (illustrating that IP addresses reveal "only that a person visited the New York Times' website at http://www.nytimes.com," whereas URLs "divulge the particular articles the person viewed").

152. 750 F.3d 1098 (9th Cir. 2014).

contained within the URL.[153] The plaintiffs alleged that defendants Facebook and Zynga disclosed the contents of their electronic communications when they shared with third parties the internet users' unique Facebook identifiers and the webpage from which the users clicked to play a Zynga social media game.[154] Relying on the court's holding in *Forrester*, the plaintiffs argued that the webpage addresses revealed contents because they disclosed what webpage the user previously viewed, proffering that "if a Facebook user who was gay and struggling to come out of the closet was viewing the Facebook page of a gay support group, and then clicked on an ad, the advertiser would know . . . that s/he was viewing the Facebook page of a gay support group just before navigating to their site."[155] However, the court rejected this argument on the grounds that webpage addresses alone "constitute addressing information" that does not reveal the contents of the communications.[156] Although the Ninth Circuit acknowledged its dicta in *Forrester*, recognizing that a URL may contain search terms that constitute content, it rejected the plaintiffs' argument that the Facebook identifier and addressing information in *Zynga* resembled the search terms contemplated in *Forrester*.[157]

Additionally, a recently declassified Foreign Intelligence Surveillance Court (FISC) opinion explicitly rejected that "DRAS information and contents are 'mutually exclusive.'"[158] The FISC recognized that a URL may include search terms that constitute contents.[159] Moreover, the Second Circuit recently held that plaintiffs may sue companies that use cookies to profile and sell anonymized browsing history—even if it does not contain personally identifiable information.[160] Despite the

---

153. *See id.* at 1108–09 (citing *Forrester*, 512 F.3d at 509–11) (affirming the district court's dismissal of the plaintiffs' claim for failing to allege that contents of electronic communications were divulged).

154. *Id.* at 1100, 1102–03.

155. *Id.* at 1108.

156. *See id.* (restating that, unlike the "contents of a communication," the Fourth Amendment does not protect "record information about those communications").

157. *Id.* at 1108–09.

158. [Redacted], No. PR/TT [Redacted], at 31 (FISA Ct. 2010), https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf [https://perma.cc/8NVK-CWDQ].

159. *See id.* at 32 (quoting *In re* Application of the United States for an Order Authorizing the Use of a Pen Register and Trap, 396 F. Supp. 2d 45, 49 (D. Mass. 2005)) (noting that the search terms embedded in the URL reveal "'the substance' and 'meaning' of the communication . . . that the user is conducting a search for information on a particular topic").

160. *See* Mount v. PulsePoint, Inc., 684 F. App'x 32, 34–35 (2d Cir. 2017) (concluding that neither case law nor the "common law tort of intrusion upon

United States' small strides toward strengthening online privacy rights,[161] U.S. courts have enhanced Fourth Amendment protections to address other facets of evolving technology.

The Supreme Court has extended Fourth Amendment privacy rights to constrain the government's use of technology to obtain new types of information about individuals. In *Kyllo v. United States*,[162] the Court held that the warrantless use of a thermal imaging device to detect heat emitted by heat lamps within a house constituted an unconstitutional search of the home.[163] Writing for the majority, Justice Scalia opined that the holding preserved the "degree of privacy against government that existed when the Fourth Amendment was adopted" by limiting the government's use of a device capable of obtaining information otherwise unascertainable without physical trespass into a constitutionally protected area.[164] The Court declined to find the thermal imaging constitutional merely because it did not capture "'intimate' details," refusing to partake in

---

seclusion" require information to be personally identifiable to establish standing), *aff'g* No. Civ. 6592 (NRB), 2016 WL 5080131, at *1 (S.D.N.Y. Aug. 17, 2016).

161. European courts have also cultivated an emerging expectation of privacy in browsing history. A Belgian court enjoined Facebook from tracking non-Facebook users before they could even read its privacy policy and denoted the nonconsensual practice as "unfair and unlawful processing of personal data" contravening "the reasonable expectations of the non-registered user." Rechtbanken van Eerste Aanleg [Civ.Rb.] [Court of First Instance] Brussels, Nov. 9, 2015, Nederlandstalige Rechtbank van Eerste Aanleg, 2015, 25–26, 32 (Belg.), https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/Judgement%20Belgian%20Privacy%20Commission%20v.%20Facebook%20-%2009-11-2015.pdf [https://perma.cc/2698-M53X]. Although a court of appeals later overturned the decision against Facebook on other grounds, another Belgian court recently ruled that Facebook again violated Belgian privacy laws by collecting and selling users' information obtained pursuant to inadequate, if any, consent. Court of Appeals Brussels, Feb. 16, 2018 (Nl.) (18e k.) Nr. 2016/153/A, 64 (Belg.), https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/Facebook_judgment_16022018.pdf [https://perma.cc/ZH8Q-W4FR] (holding that Belgian courts did not have jurisdiction over Facebook and finding that Belgium's claim for injunctive relief was not urgent because Facebook had used tracking technology for three years by the time of filing); Natasha Lomas, *Facebook's Tracking of Non-Users Ruled Illegal Again*, TECH CRUNCH (Feb. 2018), https://techcrunch.com/2018/02/19/ facebooks-tracking-of-non-users-ruled-illegal-again [https://perma.cc/TL7H-SU73] (scrutinizing Facebook's use of tracking pixels and tracking cookies to collect browsing history).

162. 533 U.S. 27 (2001).

163. *See id.* at 29, 34, 40 (holding unconstitutional the government's warrantless use of sense-enhancing technology not in general public use that allowed the government to obtain information otherwise unascertainable without physical trespass into a constitutionally protected area).

164. *Id.* at 34, 40.

any jurisprudential odyssey to determine "which home activities are 'intimate' and which are not."[165] Moreover, the Court reaffirmed that inferences may constitute a search.[166]

In *Riley v. California*,[167] the Supreme Court recognized that searching a cell phone implicates privacy concerns not raised by searching physical records and held that the search incident to arrest doctrine does not permit warrantless searches of an individual's phone, including the phone's call logs and media storage.[168] The Court recognized an expectation of privacy in non-content information call logs, distinguishing them from the phone numbers in *Smith* on the grounds that the call logs included "identifying information that an individual might add."[169] Furthermore, the Court highlighted that phones contain troves of different information that can reconstruct an individual's private life back to even before an individual purchased the phone.[170] The Court acknowledged that internet-enabled phones contain "qualitatively different" information, such as browsing history, which raise distinct privacy concerns.[171]

Modern technology continues to test the bounds of precedent, and in *Carpenter v. United States*,[172] the Court again recognized new technology and data that "does not fit neatly under existing precedents."[173]

---

165. *See id.* at 38–39 (condemning such a rule as unworkable because the government could not discern in advance whether surveillance would capture "intimate" information).

166. *See id.* at 35–37 (citing United States v. Karo, 468 U.S. 705 (1984)) (refusing to "leave the homeowner at the mercy of advancing technology"). *But see* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012) (arguing that the "mosaic theory requires courts to apply the Fourth Amendment search doctrine to government conduct as a collective whole rather than in isolated steps").

167. 573 U.S. 373 (2014).

168. *Id.* at 378–80, 386, 395, 403.

169. *See id.* at 400 (rejecting the government's argument that *Smith v. Maryland* permits an officer to always search call logs).

170. *See id.* at 394–95 (citing Ontario v. Quon, 560 U.S. 746, 760 (2010)) (highlighting that, because of the pervasiveness of phones in modern society, phones safeguard "a digital record of nearly every aspect of [individuals'] lives—from the mundane to the intimate").

171. *Id.* at 395–96 (observing that physical records do not contain browsing history that reveals private traits and details, such as medical well-being).

172. 138 S. Ct. 2206 (2018).

173. *Id.* at 2214–16 (acknowledging that historical CSLI touches upon precedent regarding expectations of privacy in physical movement and the third-party doctrine).

D. Carpenter v. United States

In *Carpenter*, police arrested several men suspected of robbing RadioShack and T-Mobile stores.[174] After one suspect identified Timothy Carpenter as an accomplice, prosecutors obtained a § 2703(d) order to compel cell-providers to disclose Carpenter's historical CSLI, which placed his phone near the robberies.[175] The district court denied Carpenter's motion to suppress the historical CSLI, rejecting that the government's warrantless acquisition of his historical CSLI constituted an unreasonable search.[176] The Sixth Circuit affirmed.[177]

After granting certiorari, the Supreme Court addressed "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements."[178] Writing for the majority, Chief Justice Roberts held that the compelled disclosure of historical CSLI constituted an unreasonable search in violation of the Fourth Amendment, and that the government must obtain a search warrant to acquire seven days or more of historical CSLI.[179] Chief Justice Roberts noted that "requests for [CSLI] lie at the intersection" of jurisprudence addressing a person's expectation of privacy in his physical movements and the third-party doctrine, and he proceeded pursuant to this dual-pronged analysis.[180]

---

174. *Id.* at 2212.

175. *Id.* at 2212–13 (noting that the government obtained 12,898 location points, charting Carpenter's movement over 127 days); *see* 18 U.S.C. § 2703(d) (2012) (permitting the government to compel the disclosure of delineated call detail records (CDRs) when it "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records or information sought "are relevant and material to an ongoing criminal investigation").

176. Order Denying Motion to Suppress at *2–3, *6, United States v. Carpenter, No. 12-20218, 2013 WL 6385838 (E.D. Mich. Dec. 6, 2013).

177. United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016).

178. *Carpenter*, 138 S. Ct. at 2211.

179. *See id.* at 2211, 2217 n.3, 2220–21 ("It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

180. *Id.* at 2214–16. Chief Justice Roberts concluded his review of physical location and movement privacy jurisprudence by acknowledging that the frameworks employed by the majority and concurring Justices in United States v. Jones, 565 U.S. 400 (2012), generally support that a person possesses a reasonable expectation of privacy in his physical location and movements. *Id.* at 2215. Conversely, Chief Justice Roberts concluded that *Miller* and *Smith* dictate that a person does not have a reasonable expectation of privacy in information voluntarily conveyed to a third party. *Id.* at 2216 (first citing Smith v. Maryland, 442 U.S. 735, 742 (1979); and then citing United States v. Miller, 425 U.S. 435, 442 (1976)).

First, the Court found that Carpenter possessed a reasonable expectation of privacy in his movements. Like the GPS tracking in *Jones*, the Court noted that historical CSLI is a "detailed, encyclopedic, and effortlessly compiled" record of an individual's every movement over several years.[181] The Court emphasized that the comprehensiveness of CSLI provides "near perfect surveillance" that can reveal intimate details of life, including "familial, political, professional, religious, and sexual associations," while circumventing practical counterbalances of government surveillance.[182] It also noted the retrospective quality of historical CSLI that enables the government to "travel back in time" to track a person who, at that earlier time, the government would not have known to track. The Court denounced the retrospective tracking of any phone in the United States since the practice is limited only by providers' retention policies.[183]

The Court proceeded to reject the government's argument that the third-party doctrine defeated Carpenter's expectation of privacy in his historical CSLI.[184] The Court faulted the government for disregarding "the seismic shifts in digital technology" that transformed phone companies into an alert and infallible "nosy neighbor" recording the movements of every phone in the United States—providing a "distinct category of information" not contemplated in *Smith* or *Miller*.[185] Furthermore, the Court found that the two rationales underlying the third-party doctrine—a reduced expectation of privacy in information shared with another and voluntary conveyance—do not apply to historical CSLI.[186]

In determining that historical CSLI is not subject to reduced expectations of privacy, the Court evaluated the nature of the historical CSLI to evaluate whether there is a reasonable expectation of privacy in its contents.[187] Accordingly, it distinguished the nature of historical CSLI from the telephone call records in *Smith* and the bank documents in *Miller* on the grounds that historical CSLI yields incomparably revealing information.[188] Moreover, the Court posited that historical CSLI conformed to the Court's reservation in *Knotts* about pervasive tracking, asserting that the comprehensive chronicling of a

---

181. *Id.*

182. *See id.* at 2217–18 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)) (comparing historical CSLI to an ankle monitor attached to all phone users).

183. *Id.* at 2218.

184. *Id.* at 2219.

185. *Id.*

186. *Id.* at 2219–20.

187. *Id.* at 2219 (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

188. *Id.* (citing Smith v. Maryland, 442 U.S. 735, 742 (1979); *Miller*, 425 U.S. at 442).

phone user's movements exonerated historical CSLI from the confines of *Smith* and *Miller*.[189]

Next, the Court found that cell phone users do not "voluntarily" share historical CSLI with providers because carrying a phone is "indispensable to participation in modern society" and users convey CSLI without any affirmative act on their part beyond powering up the device.[190] In concluding that cell phones are integral to modern society, the Court only cited *Riley v. California*, which emphasized that more than 90% of American adults always carry their cell phone.[191] Additionally, the Court acknowledged that there is almost "no way to avoid leaving behind a trail of location data" because CSLI is automatically conveyed and recorded if a phone is on.[192]

Striving to not "embarrass the future," the Court clarified that its holding did not extend to tower dumps, security cameras, investigative techniques used for national security or foreign affairs, or "other business records that might incidentally reveal location information."[193] The Court also explicitly stated that its decision did not overturn *Smith* or *Miller*.[194] Despite its efforts to mitigate the doctrinal damage done, the Court left the third-party doctrine's longevity and application dubious and doubtful.[195] Four Justices

189. *Id.* at 2220; *see* United States v. Knotts, 460 U.S. 276, 283–84 (1983) (reserving that "if such dragnet-type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable").

190. *Carpenter*, 138 S. Ct. at 2220 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

191. *Riley*, 573 U.S. at 395.

192. *Carpenter*, 138 S. Ct. at 2220.

193. *See id.* (quoting Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)) (cautioning that courts must "tread carefully" when considering the legal implications arising from new technology).

194. *See id.* at 2220 (clarifying that it only declined to extend *Smith* and *Miller* to historical CSLI).

195. *See id.* at 2272 (Gorsuch, J., dissenting) (asserting that "*Smith* and *Miller* [are] on life support"); Paul Ohm, *The Broad Reach of* Carpenter v. United States, JUST SECURITY (June 27, 2018), https://www.justsecurity.org/58520/broad-reach-carpenter-v-united-states [https://perma.cc/PD96-ATDC] (claiming that the third-party doctrine is "almost dead"). *But see* Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE (June 22, 2018), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/8NPZ-HE2M] (rejecting that the third-party doctrine is on life support and, instead, suggesting that the third-party doctrine merely has an "equilibrium-adjustment" cap on it); Harry Sandick & George LoBiondo, *Insight:* Carpenter v. United States*: An Initial Assessment*, BLOOMBERG L. (July 23, 2018), https://www.pbwt.com/content/uploads/2018/07/Carpenter-v.-

dissented, underlining the inefficacy of the Court's holding and resonating that the majority disregarded property rights, thus providing significant fodder for future Fourth Amendment challenges.[196] However, this Comment will focus on their non-property-based contributions.

Beginning the trail of dissents, Justice Kennedy scrutinized the majority for interpreting *Miller* and *Smith* as creating a balancing test in which the privacy interests of each "'qualitatively different category' of information . . . must be weighed against the fact that the information has been disclosed to a third party."[197] Justice Kennedy faulted the majority for neither explaining why it adopted a seven-day rule nor providing factors to discern whether the Court's holding extends beyond historical CSLI to information like browsing history.[198] Similarly, Justice Alito doubted the utility of the Court's holding in a society in which private companies—not the government—pose the greatest threats to privacy.[199] In the last

---

United-States-An-Initial-Assessment1-1.pdf [https://perma.cc/JXN8-56XH] (opining that interpreting *Carpenter* as nullifying the third-party doctrine would be a "stretch").

196. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2224–26 (Kennedy, J., dissenting) (asserting that the Court "unhinge[d] Fourth Amendment doctrine from the property-based concepts" delineated by *Miller* and *Smith*); *id.* at 2235, 2240, 2242 (Thomas, J., dissenting) (highlighting that Carpenter retained no right or property interest in the CSLI records and esteeming the role of common law and property law when determining Fourth Amendment privacy rights); *id.* at 2272 (Gorsuch, J., dissenting) (admonishing Carpenter's counsel for omitting all property-based and positive law-based arguments, noting that these omissions hinder "the development of a sound or fully protective Fourth Amendment jurisprudence").

197. *See id.* at 2231–32 (Kennedy, J., dissenting) (quoting Carpenter, 138 S. Ct. at 2216 (majority opinion)) (asserting that even if *Miller* and *Smith* established a balancing test, a person's privacy interest in his movements does not surmount the third-party doctrine).

198. *Id.* at 2234; *see also* Douglas Harris, Note, Carpenter v. United States*: How Many Cell Phone Location Points Constitute a Search Under the Fourth Amendment?*, 13 DUKE J. CONST. L. & PUB. POL'Y SIDEBAR 101, 115 (2018) (stating that identifying the line of the permissible amount of historical CSLI that the government may obtain is the most perplexing aspect of *Carpenter*). The Court implicitly rejected Carpenter's proposed twenty-four-hour rule without explaining whether or why the Court adopted the government's seven-day rule. *See* Reply Brief for Petitioner at 12, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (arguing that the twenty-four-hour rule would provide the government with the benefit of the doubt and certainty); Brief for the United States at 55–56, 138 S. Ct. 2206 (2018) (No. 16-402) (justifying the seven-day rule on the grounds that the government commonly surveils suspects for at least one week).

199. *See Carpenter*, 138 S. Ct. at 2261 (Alito, J., dissenting) (quipping that misleading the public to believe that the judiciary can protect it from private companies that collect and misuse personal data would be divisive and disserving compared to deferring to Congress for further legislation).

dissenting opinion, Justice Gorsuch scrutinized consent as a justification for the third-party doctrine and argued that consenting to allow a third party to access private property does not imply consent for the government to search the property.[200] Justice Gorsuch denounced the consent-based explanation as merely "assumption of risk relabeled" as "'consent[ing]' to whatever risks are foreseeable."[201]

E. Where Carpenter *Leaves the Fourth Amendment and Third-Party Doctrine*

Practitioners and scholars received *Carpenter* with mixed reviews. While scholar Daniel Solove opined that, despite being "the length of a Tolstoy novel," *Carpenter* did not sufficiently further the legal plot,[202] other scholars esteem *Carpenter* as evincing the Court's equivocal commitment to the third-party doctrine.[203] Indeed, at face value, *Carpenter* only yields that the government must obtain a search warrant before acquiring more than seven days of historical CSLI.[204] However, despite the Court's limited holding, its reliance on comprehensive detail, pervasiveness, and involuntary conveyance suggests that the scope of *Carpenter* applies to information other than historical CSLI.[205]

---

200. *Id.* at 2263 (Gorsuch, J., dissenting). Justice Gorsuch also rejected that "knowledge" or "clarity" justify the third-party doctrine. *Id.* at 2263–64.

201. *Id.* at 2263.

202. Daniel Solove, Carpenter v. United States, *Cell Phone Location Records, and the Third Party Doctrine*, TEACH PRIVACY (July 1, 2018), https://teachprivacy.com/carpenter-v-united-states-cell-phone-location-records-and-the-third-party-doctrine [https://perma.cc/5WCE-8R7B] (asserting that "a lot more was at stake in [*Carpenter*]" than the Court's narrow holding addresses). Solove argues that the Court squandered "the prime opportunity" to overrule the third-party doctrine. *Id.*

203. *See* Nat'l Constitution Ctr., *Does the Warrantless Search and Seizure of Cellphone Records Violate the Fourth Amendment*, YOUTUBE (Oct. 31, 2017), https://www.youtube.com/watch?v=hW32k7x7zE0 [https://perma.cc/2BAS-AANW] (noting that the Court in *Knotts* indicated that it is not fully wedded to the third-party doctrine by reserving whether the public view doctrine permits the government to conduct dragnet surveillance of Americans using technology).

204. *Carpenter*, 138 S. Ct. at 2217 n.3 (majority opinion).

205. *See* Kate Fazzini, *Supreme Court Ruling Requiring Warrant for Cellphone Searches Could Lead to a Flood of Lawsuits*, CNBC (June 25, 2018), https://www.cnbc.com/2018/06/25/privacy-scotus-cell-data-carpenter-v-usa.html [https://perma.cc/BCE6-M54X] (forecasting that *Carpenter* will force courts to address whether real-time CSLI should be treated differently than historical CSLI); Sharon Bradford Franklin, Carpenter *and the End of Bulk Surveillance of Americans*, LAWFARE (July 25, 2018), https://www.lawfareblog.com/carpenter-and-end-bulk-surveillance-americans [https://perma.cc/9B82-DMG2] (advocating that *Carpenter* could be extended to non-location-based CDRs); *see also* Timothy Edgar, *The Supreme Court Just Struck a Blow Against Mass Surveillance*, WASH. POST (June 25, 2018), https://www.washingtonpost. com/opinions/the-

Some courts have already grappled with applying *Carpenter* in non-historical CSLI cases.[206] Most notably, in *Naperville Smart Meter Awareness v. City of Naperville*,[207] the Seventh Circuit extended *Carpenter* to "smart meter" energy data, holding that the government conducted a search when it required residents to purchase energy from it and subsequently recorded their energy consumption every fifteen minutes.[208] In rejecting that the third-party doctrine defeated residents' expectation of privacy in their smart meter data merely because they "enter[ed] into a 'voluntary relationship' to purchase electricity from the city,"[209] the court invoked *Carpenter* to dispel that a resident "assume[s] the risk of near constant monitoring by choosing to have electricity in her home."[210] Furthermore, the court viewed the smart meter data as potentially more invasive than the thermal imaging data collected in *Kyllo* because the comprehensiveness of the smart meter data enables the government to infer more confidently the interior details of the home.[211] *Naperville* exemplifies the reality that the third-party doctrine must be reconsidered in the digital age.[212] As technology increasingly integrates into modern society, perpetuating a rigid and

---

supreme-court-just-struck-a-blow-against-mass-surveillance/2018/06/25/1b5ee510-7653-11e8-b4b7-308400242c2e_story.html [https://perma.cc/ E4FE-MA2C] (noting that *Carpenter* raises serious issues for mass surveillance of telephone metadata).

206. *See, e.g.*, United States v. Morel, 922 F.3d 1, 8–9 (1st Cir. 2019) (refusing to extend *Carpenter* to IP addresses); Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 526–27 (7th Cir. 2018) (holding the third-party doctrine inapplicable to digital "smart meter" energy data); Florida v. Sylvestre, 254 So. 3d. 986, 992 (Fla. Dist. Ct. App. 2018) (holding unconstitutional warrantless direct government surveillance of real-time CSLI); Mobley v. Georgia, 816 S.E.2d 769, 776–77 (Ga. Ct. App. 2018) (holding defendant did not have a reasonable expectation of privacy in airbag control module data).

207. 900 F.3d 521 (7th Cir. 2018).

208. *Id.* at 527–29 (holding that the government conducted a search but, nevertheless, concluding that the search was reasonable because, *inter alia*, the government's public utility workers—not law enforcement officials—conducted the search and without prosecutorial intent).

209. *Id.* at 527.

210. *See id.* (extrapolating that, if an individual does not "voluntarily 'assume the risk'" of conveying CSLI, a homeowner does not voluntarily assume the risk of surveillance merely by having electricity).

211. *See id.* at 526 (distinguishing that, unlike the search in *Kyllo* that revealed only heat, the smart meter data can reveal when individuals are sleeping, eating, or vacationing).

212. *See id.* at 527 (holding that people do not surrender their legitimate expectations of privacy by choosing to have government supplied electricity in their homes); *see also* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (submitting that the third-party doctrine is "ill suited to the digital age" and merits reconsideration).

unqualified third-party doctrine guarantees increasingly intrusive, "absurd and problematic" government surveillance.[213]

III. APPLYING CARPENTER TO BROWSING HISTORY COLLECTED BY TRACKING COOKIES

The holding in *Carpenter* provides new fodder to establish an expectation of privacy in browsing history collected by tracking cookies. Part III applies *Carpenter*'s holding to browsing history collected by tracking cookies, advocating that courts should recognize an expectation of privacy in browsing history. First, Part III.A.1 advances an expectation of privacy in the comprehensiveness of the information sought, thus affording browsing history heightened Fourth Amendment protections. Next, Parts III.A.2–3 argue that the justifications for the third-party doctrine do not apply to browsing history collected by tracking cookies. Finally, Part III.B asserts that a reconceptualized third-party doctrine should protect the private sector from government appropriation.

A. An Expectation of Privacy in the Comprehensiveness of the Information Sought

The first step in extending *Carpenter* to browsing history collected by tracking cookies is recognizing an expectation of privacy in it. Although the United States has yet to recognize an absolute expectation of privacy in browsing history or against tracking cookies, recent technology-oriented Fourth Amendment jurisprudence supports an expectation of privacy in browsing history based on the comprehensiveness of the information sought. In construing *Carpenter* to turn on the comprehensiveness of the information sought, rather than the type of information, *Carpenter* provides a foundation to strengthen privacy rights in the digital age.

In forging an expectation of privacy in the comprehensiveness of the information sought, the concurring opinions of Justices Sotomayor and Alito in *Jones* take center stage, relegating back to understudy Justice Scalia's trespass approach.[214] In his concurrence,

---

213. *See* Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1924–26 (2018) (illustrating the unreasonableness of applying the third-party doctrine to information obtained from a smart home).

214. *See supra* notes 131–37 and accompanying text (summarizing the concurring opinions of Justice Alito and Justice Sotomayor in *Jones*). The *Jones* majority opinion, relying primarily upon trespass-based privacy rights, lends little support here because the *Carpenter* majority couches its opinion in "reasonable expectation of privacy"

Justice Alito posits that long-term monitoring would infringe society's expectation of privacy that the government would not and could not "secretly monitor and catalogue" an individual's every movement.[215] However, Justice Alito left unanswered a fundamental question: Why does society expect that the government does not and will not covertly and comprehensively monitor an individual's every movement? Justice Sotomayor answers this question, expounding that comprehensive tracking threatens to expose the very personal details and "familial, political, professional, religious, and sexual associations" at the heart of even the earliest notions of privacy.[216] Privacy does not concern general, uncontextualized location information; rather, it concerns the precise collection and aggregation of private, detailed information that an individual might not have otherwise disclosed and that no single record could have otherwise revealed.[217]

---

terms. *Compare* Carpenter v. United States, 138 S. Ct. 2206, 2214–16 (2018) (noting that *Carpenter* lies at the intersection of expectations of privacy in physical location and movements and the third-party doctrine's limitation of those expectations), *with id.* at 2224 (Kennedy, J., dissenting) (accusing the Court majority of "unhing[ing] the Fourth Amendment doctrine" from its property-based foundation), *and* United States v. Jones, 565 U.S. 400, 404 (2011) (holding that the government physically trespassed on the defendant's vehicle when it installed a GPS device on the defendant's car and, therefore, conducted a search). Furthermore, as noted by both Justices Alito and Sotomayor in *Jones*, the government can easily circumvent privacy rights grounded in property law if it uses technology to track individuals without physical trespass. *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *id.* at 425–26 (Alito, J., concurring).

215. *Jones*, 565 U.S. at 430 (Alito, J., concurring).

216. *See id.* at 415–17 (Sotomayor, J., concurring) (citing New York v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)) (questioning the reasonableness of "permeating police surveillance" that reveals this information which can be misused and subjected to associational and expressive chilling) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)); *supra* note 60 and accompanying text (recalling that privacy in colonial America safeguarded personal autonomy, emotional release, self-evaluation, and interpersonal communications, as well as the personal liberties inherently flowing from each).

217. *See* Riley v. California, 134 S. Ct. 2473, 2490 (2014) (observing that the vast storage capacities of digital records implicates distinct privacy concerns compared to the limited information within a physical record); Kyllo v. United States, 533 U.S. 27, 34–35 (2001) (holding that the government's use of sense-enhancing technology not in general public use that allowed the government to obtain, or infer, information otherwise unascertainable without physical trespass into a constitutionally protected area constituted a search and explaining that its holding preserves the "degree of privacy against government that existed when the Fourth Amendment was adopted"); United States v. Katz, 389 U.S. 347, 351 (1967) ("[T]he Fourth Amendment protects people, not places."); WESTIN, *supra* note 59 and accompanying text (defining privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others").

Chief Justice Roberts also supports this expectation of privacy in *Carpenter* when he clarified that the majority's holding turns not upon use of a phone or an individual's movements but on the "detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[218] Furthermore, the Seventh Circuit's application of *Carpenter* in *Naperville Smart Meter Awareness v. City of Naperville* also supports this expectation of privacy. As observed by one commentator, the government in *Naperville* supplied its residents with the energy and, therefore, already knew how much energy the homes used.[219] However, the government's comprehensive recording and saving of residents' energy usage in short intervals, which enabled the government to infer private details about residents, led the court to hold that the exfiltration of the energy use data constituted a search.[220] Moreover, this expectation of privacy in comprehensiveness also accounts for the "seismic shifts in digital technology" that permit the government to track not only a specific internet user, but also to retrospectively track any internet user.[221]

Admittedly, an expectation of privacy in the comprehensiveness of the information sought, and as applied to browsing history, is prone to criticisms posited by the dissenting Justices in *Carpenter*. The expectation of privacy would likely require a bright line rule, like *Carpenter*'s seven-day rule, to identify "comprehensive" information requiring a warrant.[222] However, as Justice Kennedy noted about historical CSLI, there is little reason seven days should demarcate requiring a warrant versus less demanding forms of compelled process.[223]

---

218. *See Carpenter*, 138 S. Ct. at 2220 (adding that "[s]uch a chronicle" transcends the scope of the privacy interests concerned in *Smith* and *Miller*).

219. Orin Kerr, *Public Utility's Recording of Home Energy Consumption Every 15 Minutes Is a "Search," Seventh Circuit Rules*, VOLOKH CONSPIRACY (Aug. 17, 2018), http://reason.com/volokh/2018/08/17/public-utilitys-recording-of-home-energy [https://perma.cc/5CNL-35F3].

220. *Id.*

221. *Compare Carpenter*, 138 S. Ct. at 2219 (noting that technological advancements transformed phone companies into an alert and infallible "nosy neighbor," recording the movements of every phone), *with* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 526 (7th Cir. 2018) (condemning the recording and storage of smart meter energy data every fifteen minutes, which the government could retrospectively mine to infer more confidently details of a home's interior).

222. *See supra* note 204 and accompanying text (noting that the *Carpenter* Court adopted a seven-day rule after the government proposed a seven-day rule and Carpenter proposed a twenty-four-hour rule).

223. *See Carpenter*, 138 S. Ct. at 2233–34 (Kennedy, J., dissenting) (scrutinizing the majority opinion for employing an arbitrary seven-day rule while failing to consider the reality of law enforcement investigations).

Thus, the central question becomes, "what makes information, or browsing history, comprehensive?" Is it the amount of datapoints and their accuracy, or is it the interval at which they are collected?[224]

Regardless of the final metric, the efficacy of this expectation of privacy is that it jettisons the nuanced, and oftentimes technical, analyses requiring courts to distinguish between "intimate" and "non-intimate"[225] or "content" and "non-content."[226] Departing from an "intimacy" inquiry extends privacy protections to information that an internet user may view as private but which may not qualify as "intimate."[227] Additionally, this broader expectation of privacy does not depend upon the nuances of the "content" dichotomy that has only acknowledged privacy interests when a URL contained an internet user's search terms.[228] Just as the Court refused to make an expectation of privacy depend upon a company's decision to automate its processes, an expectation of privacy in browsing history can no more justifiably turn on whether a URL is programmed to include a search term.[229] Exonerated from the confines of "intimacy" and "content" inquiries, this expectation of privacy protects browsing history, regardless of whether it reveals support group webpages or social media

224. *See id.* at 2212 (majority opinion) (highlighting that the government collected more than 12,000 datapoints that could locate an individual within fifty meters); *Naperville Smart Meter Awareness*, 900 F.3d at 525–27 (focusing on how the collection of data every fifteen minutes allowed the government to infer more confidently details of a home's interior); Harris, *supra* note 198 (noting that the identification of the permissible amount of historical CSLI that the government may obtain as the most perplexing aspect of *Carpenter*).

225. *See* Kyllo v. United States, 533 U.S. 27, 38–39 (2001) (rejecting a bright-line rule based on intimacy as unworkable for courts who would be required to determine which activities are "intimate").

226. *See supra* Section II.C.2 (detailing the fine distinctions between "content" and "non-content" under the SCA).

227. *See* Solove, *supra* note 64, at 755 (illustrating how defining privacy through "intimacy" may exclude privacy interests in information such as political affiliations and religious beliefs that may be regarded as private but not intimate).

228. *See supra* notes 138–46 and accompanying text (surveying the technical nuances governing the expectation of privacy in URLs).

229. *See* Smith v. Maryland, 442 U.S. 735, 745 (1979) ("We are not inclined to make a crazy quilt of the Fourth Amendment" where "the pattern of protection would be dictated by billing practices of a private corporation").

games,[230] simply because browsing history reveals comprehensive information about internet users.[231]

If courts recognize an expectation of privacy in browsing history based on comprehensiveness, courts must then address whether the third-party doctrine eliminates an internet user's expectation of privacy when tracking cookies collect browsing history. Parts III.B.1–2 argue that the rationales underlying the third-party doctrine—reduced expectation of privacy in information knowingly shared and voluntary exposure—do not apply to browsing history collected by tracking cookies; therefore, the third-party doctrine does not eliminate internet users' expectation of privacy in their browsing history.

B. The Third-Party Doctrine Does Not Apply to Browsing History

1. Browsing history is subject to a heightened expectation of privacy

Browsing history collected by tracking cookies is not subject to a reduced expectation of privacy because it is a comprehensive and pervasive record of an internet user's online behavior. Tracking cookies, like historical CSLI, have outgrown the confines delineated by *Miller* and *Smith* that have failed to accommodate new, "distinct categor[ies] of information" born from "the seismic shifts in digital technology."[232] In *Carpenter*, the Court found that historical CSLI conveyed troves of intimate information not found in the negotiable

---

230. *See Kyllo*, 533 U.S. at 37–39 (declining to hold that privacy rights depend on the intimacy of the information sought, condemning such a rule as unworkable); *In re* Zynga Privacy Litig., 750 F.3d 1098, 1103 (9th Cir. 2014) (declining to find an expectation of privacy based on the contents of a webpage because the IP address constituted only "addressing information" and the website URLs did not contain search terms).

231. *See* United States v. Jones, 565 U.S. 400, 415–17 (2012) (Sotomayor, J., concurring) (questioning the reasonableness of "permeating police surveillance" that reveals information which can be misused and subjected to associational and expressive chilling) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)) (citing New York v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)); *Kyllo*, 533 U.S. at 34, 40 (holding unconstitutional technology that allowed the government to obtain information about the interior of homes that was otherwise unascertainable without physical trespass into a constitutionally protected area); Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 526–27 (7th Cir. 2018) (viewing smart meter data as potentially more invasive than the thermal imaging data collected in *Kyllo* because the comprehensiveness of the smart meter data enables the government to more confidently infer the interior details of a home); *supra* notes 42–45 (discussing that browsing history is used to determine information about an internet user, such as political and religious beliefs, sex, and occupation, otherwise unavailable on the internet).

232. Carpenter v. United States, 138 S. Ct. 2216, 2219 (2018).

bank documents in *Miller* or telephone numbers in *Smith*, which without more, "reveal[ed] little in the way of 'identifying information.'"[233] Similarly, although cookies may have conceptually originated as mere tools to help a well-intentioned shopkeeper remember and relate to customers, today's tracking cookies embody a "nosy" shopkeeper who alertly and infallibly records his customers' browsing history to ensure that his shelves are always stocked with products matching each customer's interests, associations, and beliefs.[234]

The comprehensiveness of browsing history dispels any reduced expectation of privacy and supports a heightened expectation of privacy. Browsing history, like the historical CSLI in *Carpenter* and GPS monitoring in *Jones*, can reveal personal details of life, including "familial, political, professional, religious, and sexual associations."[235] Similarly, like historical CSLI, tracking cookies generate a "detailed, encyclopedic, and effortlessly compiled" record of internet users' browsing history for several years.[236] Accordingly, browsing history implicates the retrospective tracking that Chief Justice Roberts denounced in *Carpenter* regarding historical CSLI and in *Riley* regarding information in cell phones, such as browsing history, that provide glimpses into users' pasts.[237]

However, unlike the government's collection of historical CSLI, which a phone company can limit through its data retention policy, or information on a cell phone that a user may delete, companies who use cookies can mine them for years without limitation.[238] Most internet users

---

233. *Id.* (first quoting Smith v. Maryland, 442 U.S. 735, 742 (1979); and then quoting Riley v. California, 134 S. Ct. 2473, 2492–93 (2014)) (citing United States v. Miller, 425 U.S. 435, 442 (1976)) (distinguishing that *Miller* and *Smith* involved "limited types of personal information").

234. *See id.* (likening telephone providers collecting historical CSLI to an alert and infallible "nosy neighbor"); *supra* notes 32 & 33 (detailing how cookies evolved from tools that enhanced e-commerce sites' customer relations to tools that help sell the customers).

235. *Carpenter*, 138 S. Ct. at 2217 (Sotomayor, J., concurring) (quoting *Jones*, 565 U.S. at 430); *see supra* notes 42–45 and accompanying text (highlighting that third parties use browsing history to deduce information that an internet user may not have shared on the internet).

236. *See Carpenter*, 138 S. Ct. at 2216, 2218 (concluding that historical CSLI generates more invasive records than the GPS device in *Jones*).

237. *See id.* (observing that historical CSLI allows the government to "travel back in time" to reconstruct an individual's movements); *Riley*, 134 S. Ct. at 2489 (recognizing that a phone may contain information "dat[ing]to the purchase of the phone, or even earlier").

238. *See Carpenter*, 138 S. Ct. at 2218 (noting that phone companies retain historical CSLI for approximately five years); *Riley*, 134 S. Ct. at 2486 (addressing concerns about phone users deleting information contained in a phone through remote-wiping or limiting access through encryption); GOOGLE GUIDE: MAKING SEARCHING

alone cannot stop a tracking cookie from recording their browsing history.[239] Even if an internet user requests for a third party to delete its tracking and Flash cookies, third parties are not legally obligated to comply in many instances.[240] Moreover, tracking cookies may raise greater privacy concerns than historical CSLI as new technology derives more information from browsing history.[241]

2. Browsing history is not voluntarily conveyed by tracking cookies

Tracking cookies do not voluntarily convey browsing history to third parties because using the internet is integral to modern society and browsing history is collected without any affirmative action on behalf of the user. Like cell phones, using the internet has become a "pervasive and insistent part of daily life."[242] Comparable to the 90% of American adults who always carry their cell phone,[243] 89% of Americans use the internet and 26% of Americans are "almost constantly" on the internet.[244]

EVEN EASIER, www.googleguide.com/cookies.html [https://perma.cc/S6YM-MU6E] (explaining that cookies can last anywhere from a few minutes to up to years in the future).

239. *See* SOLTANI ET AL., *supra* note 49, at 158 (explaining that erasing a browser's cookies, cache, search history, and private data will not delete Flash cookies).

240. *E.g.*, *supra* notes 56–58 and accompanying text (noting that companies are only legally obligated to fulfill "Do Not Track" requests if the company commits to honoring them). *Compare, e.g.*, Oberster Gerichtshof [OGH] [Supreme Court] Oct. 25, 2017, 6 Ob 116/17b, https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20171025_OGH0002_0060OB00116_17B0000_000/JJT_20171025_OGH0002_0060OB00116_17B0000_000.html [https://perma.cc/V4NL-WAK5] (refusing to interpret the "right to be forgotten" as requiring Facebook to proactively delete content similar to content that an individual requested be deleted), *with Data Policy: How Can I Manage Or Delete Information About Me?*, FACEBOOK, https:// www.facebook.com/about/privacy [https://perma.cc/F9HP-UBWL] (stating that Facebook retains user data "until it is no longer necessary to provide our services and Facebook Products or until your account is deleted—whichever comes first").

241. *See* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 526–27 (7th Cir. 2018) (voicing that the smart meter data raised greater privacy concerns than the thermal imaging in *Kyllo* because smart meter data allowed the government to more confidently deduce intimate details of the home); *see also Carpenter*, 138 S. Ct. at 2218–19 (concluding that, despite historical CSLI being less accurate than GPS monitoring, GPS monitoring jurisprudence governed it because the Court must, as stated in *Kyllo*, consider "more sophisticated systems that are already in use or in development" (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001))).

242. *Carpenter*, 138 S. Ct. at 2220 (internal quotation marks omitted) (quoting *Riley*, 134 S. Ct. at 2484).

243. *Riley*, 134 S. Ct. at 2490.

244. *Supra* note 50 and accompanying text.

Furthermore, tracking cookies set and convey browsing history without any affirmative act on behalf of the user.[245] For example, the pervasive Facebook "Like" button embedded on a non-Facebook website sets and reads tracking cookies in an internet user's computer without the user ever visiting the Facebook website.[246] Labeling such tracking as "voluntary" is problematic because an internet user may not know that a non-Facebook website features a Facebook "Like" button before visiting the website.[247] Moreover, as using the internet becomes increasingly central to modern society, individuals do not "voluntarily" assume the risk of surveillance through tracking cookies merely because they choose to access the internet.[248]

Moreover, internet users do not voluntarily convey their browsing history collected by tracking cookies because internet users cannot effectively manage or control the sharing of their information. Companies intentionally implement privacy practices, such as the use of Flash cookies and non-compliance with "Do Not Track" requests, that nullify internet users' control over their information online.[249]

Additionally, internet users do not give meaningful consent when agreeing to a website's cookie policy. Even if an astute internet user reads a website's privacy policy before agreeing to it, most privacy

---

245. *See Carpenter*, 138 S. Ct. at 2220 (recognizing that cell phones automatically record historical CSLI, without any affirmative act from users other than turning on their cell phone).

246. *See* Gillmore, *supra* note 39 (noting that tracking cookies embedded in Facebook "Like" buttons on other websites enable Facebook to identify the website on which users found the "Like" button and to track their browsing history).

247. *See supra* notes 106–07 and accompanying text (recalling that voluntary conveyance requires that a conveyance be intentional and presumably with the conveyor's knowledge). Additionally, European courts have rejected such tracking as "voluntary," decrying the practices as "unfair and unlawful" in violation of the "reasonable expectations of the non-registered user." *See supra* note 161 (detailing how European courts have addressed tracking cookies).

248. *See* Smith v. Maryland, 442 U.S. 735, 749–50 (1979) (Marshall, J., dissenting) (decrying that a person cannot assume a risk where "unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance"); Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018) (rejecting that individuals, by ascertaining a common utility in their homes, "assume the risk of near constant monitoring"); Bellovin et al., *supra* note 107, at 1, 28–31 (rejecting that information that must be disclosed to use a service is necessarily "voluntarily conveyed").

249. *See supra* notes 54–57 and accompanying text (noting the strategic use of Flash cookies and non-compliance with "Do Not Track" requests to perpetuate online tracking, even after internet users attempt to stop it); *see also Smith*, 442 U.S. at 749–50 (Marshall, J., dissenting) (doubting that one can assume a risk without any reasonable alternative).

policies do not sufficiently disclose how the user's information, including browsing history, will be tracked and conveyed to third parties.[250] As Justice Gorsuch noted in his *Carpenter* dissent, consent cannot be dispositive in the third-party doctrine because the doctrine then merely equates to agreeing to "whatever risks are foreseeable."[251] In the digital age, allowing the third-party doctrine to turn on consent, and thus foreseeability, effectively turns consent into a boilerplate, "formalistic exercise[]," that empowers the government to define internet users' expectations of privacy by legislating that certain notices be provided to users in privacy policies.[252] Considering that internet users are unable to negotiate the terms of privacy policies, a modern privacy framework in which the third-party doctrine can turn on consent when an internet user "[has] no realistic alternative" but to submit to surveillance or to forgo technology essential to modern life only furtherly imbalances the equilibrium of privacy rights and bargaining power online.[253]

C. Recommendation: Returning to a Misplaced Trust Third-Party Doctrine

In his dissenting opinion in *Carpenter*, Justice Alito recognized that, "today . . . some of the greatest threats to individual privacy may come" not from the government but "from powerful private companies," and that *Carpenter* would not protect the public from "this looming threat."[254] While he may have correctly identified that private companies now "collect and sometimes misuse vast quantities of data about the lives of ordinary Americans," Justice Alito understates the threat that the federal government still poses in this paradigm.[255]

---

250. *See* LIBERT, *supra* note 54, at 212 (illustrating that website privacy policies disparately disclose the conveyance of user information to certain third parties while omitting the conveyance to other discreet third parties).

251. Carpenter v. United States, 138 S. Ct. 2206, 2263 (2018) (Gorsuch, J., dissenting).

252. *See* Hartzog, *supra* note 109 (noting that the formalization of consent threatens its integrity); *see also Smith*, 442 U.S. at 750 (Marshall, J., dissenting) (arguing that the proper framework for determining what risks individuals assume is based on the "risks he should be forced to assume in a free and open society").

253. *See Smith*, 442 U.S. at 749–50 (Marshall, J., dissenting) (doubting that an individual assumes the risk of being surveilled where the individual must choose between forgoing an important service or being surveilled); Kerr, *supra* note 195 (positing that *Carpenter* placed an "equilibrium-adjustment" cap on the third-party doctrine's application to historical CSLI).

254. *Carpenter*, 138 S. Ct. at 2261 (Alito, J., dissenting); *see* Solove, *supra* note 80, at 1092 (arguing that "the Internet has the potential to become one of the government's greatest information gathering tools").

255. *Carpenter*, 138 S. Ct. at 2261 (Alito, J., dissenting).

Under the current third-party doctrine, the government views all persons and entities as prospective undercover agents or informants because the law requires only a subpoena or court order to compel them to disclose internet users' browsing history.[256] The current legal framework, encompassing the Fourth Amendment, third-party doctrine, and SCA do not reflect societal expectations that companies are not just repositories but also fiduciaries.[257] The law must recognize the distinction between the private and public sector—that not every person and entity is an informant or undercover agent—and must continue to evolve to regulate the conveyance of private individuals' information to the government.[258] Thus, the third-party doctrine has strayed too far from its misplaced trust doctrinal roots to apply the third-party doctrine in the digital age. Courts should reform the third-party doctrine to adapt and promote the information practices of the digital age.

A reconceptualized third-party doctrine should recognize the absence of retrospective surveillance in most misplaced trust cases and require the government to obtain a warrant when the government seeks to acquire information voluntarily conveyed to a third party not employed or associated with the government when the information was originally conveyed. Generally, in misplaced trust doctrine jurisprudence an informant or undercover agent conveyed the defendants' "private" information to the government.[259] However, more narrowly, these informants and undercover agents were typically already current government employees or associates.[260] These cases did not involve the government constructively employing or appropriating an individual or entity to disclose retrospective information that they would not have agreed to disclose at the time of the original conveyance. A reconceptualized doctrine need not question the principles of *Hoffa* and *White*, in which the conveyors

256. *See supra* notes 145–46 and accompanying text (delineating the various compulsory process means through which the government can obtain browsing history).

257. *See* Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 617, 619–20 (2015) (arguing that *Smith* and *Miller* are the progeny of conflating the disclosure of information to a company and the exposure of information to the public).

258. *See* Solove, *supra* note 80, at 1086–87 (arguing that the Fourth Amendment must provide new protections to protect citizens from the "digital biographies" held by third parties).

259. *See supra* Section II.B.1 (chronicling the development of the misplaced trust doctrine).

260. *See, e.g.*, Lopez v. United States, 373 U.S. 427, 428 (1963) (involving a then-employed IRS agent); On Lee v. United States, 343 U.S. 747, 749 (1952) (involving an undercover agent already working for the government).

voluntarily disclosed the information to the government despite not being associated with the government when the information was originally conveyed, because individuals and entities should be free to voluntarily convey information to the government to promote effective law enforcement.[261]

Furthermore, a more restrained third-party doctrine that recognizes that an individual does not relinquish all expectations of privacy in comprehensive browsing history disclosed to a third party mitigates the burden on companies to defend the rights of internet users. As legal reforms diminish internet users' expectations of privacy, private companies have emerged as the only party positioned to advocate for users' privacy rights.[262] However, companies may be unwilling or unable to challenge infringements upon users' privacy,[263] marring the frontiers of data privacy law with barren plains in which "there is no one who is both in the position and legally entitled to challenge the search or seizure on Fourth Amendment grounds . . . thus eliminating one of the most powerful checks on government overreach."[264] If internet users possess a cognizable expectation of privacy in their browsing history, they can challenge these government searches, consequently alleviating the vigilante burden on companies and helping to restore the equilibrium between internet users and the government.[265]

American society continues to adopt evolving technology, and a third-party doctrine that does not adapt to these changes promises to fundamentally change the relations between citizens, companies, and

---

261. *See* United States v. White, 401 U.S. 745, 746–47, 747 n.1 (1971) (plurality opinion) (involving an informant; however, the Court declined to determine whether his employ was consensual); Hoffa v. United States, 385 U.S. 293, 295 (1966) (involving a witness who conveyed the defendant's incriminatory statements to the government).

262. *See, e.g.*, Letter from Tim Cook, CEO, Apple Inc., to Apple Customers, (Feb. 16, 2016), https://www.apple.com/customer-letter [https://perma.cc/ML3S-HEF2] (reaffirming Apple's refusal to help the government circumvent its encryption safeguards because doing so would effectively compromise its customers' information privacy and security); *see also* Kyriades, *supra* note 9 (criticizing the European Union's e-Evidence proposal, which would allow European Union member states to circumvent prolonged judicial processes and to obtain digital evidence directly from service providers, as delegating the vindication of individuals' rights to private companies).

263. *Supra* note 9 and accompanying text (discussing the legal and practical restraints that hinder the vindication of privacy rights).

264. Daskal, *supra* note 9, at 441 (emphasis omitted).

265. *See* Kerr, *supra* note 195 (viewing sea changes in Fourth Amendment jurisprudence as "equilibrium adjustments").

government.[266] A third-party doctrine that distinguishes between data voluntarily conveyed, as opposed to data retrospectively obtained through the compulsion of private individuals and entities, affords privacy protections that promote trust and progress in information relationships between the private and public sectors.[267]

CONCLUSION

Although *Carpenter v. United States* represents a positive step toward strengthening privacy rights in the digital age, its holding must be extended to other digital information to adequately safeguard privacy. Currently, databases of profiles of internet users serve as "one-stop shops" for the government to fish for suspects—with nothing in its tacklebox except undemanding forms of process. However, *Carpenter* and other technology-oriented Fourth Amendment cases support an emerging expectation of privacy in the comprehensiveness of digital information that could remedy this privacy concern by extending *Carpenter*'s heightened Fourth Amendment protections to browsing history collected by tracking cookies. Like historical CSLI, tracking cookies involuntarily, comprehensively, and infallibly record browsing history that reveals, directly or indirectly, details about internet users; therefore, the third-party doctrine does not apply to browsing history collected by tracking cookies.

Extending *Carpenter* to browsing history collected by tracking cookies pioneers more than merely granting internet users additional privacy rights. It also forges order in the Wild West of the internet where legislation and regulation have consistently lagged behind advancing technology, neglecting the government's gradual appropriation of private entities. Therefore, courts and privacy advocates should interpret *Carpenter* beyond its four-corners to reclaim an equitable stake in the digital age privacy landscape.

---

266. *See* United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring) (advancing that such unchecked surveillance could "chill[] associational and expressive freedoms" and "alter the relationship between citizen and government in a way that is inimical to democratic society" (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring))); *White*, 401 U.S. at 787 (Harlan, J., dissenting) (voicing that third-party surveillance must be viewed as "undermin[ing] that confidence and sense of security in dealing with one another that is characteristic of individual relationships between citizens in a free society").

267. *See* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 434 (2016) (advocating that privacy laws should strengthen and foster trust in information relationships but commentating that modern privacy laws do not).