NEW YORK LAW SCHOOL

NYLS Law Review

Volume 65
Issue 2 *Volume 65, Issue 2, 2020/21: A CENTURY OF TARGETING IMMIGRANTS: FROM THE RED SCARE TO THE TRAVEL BAN*

Article 5

January 2020

The Outdated Third-Party Doctrine and the Need for Modernization

Shawn Bass

VOLUME 65 | 2020/21

SHAWN BASS

The Outdated Third-Party Doctrine and the Need for Modernization

65 N.Y.L. Sch. L. Rev. 259 (2020–2021)

ABOUT THE AUTHOR: Shawn Bass was a Staff Editor of the 2019–2020 *New York Law School Law Review*. He received his J.D. from New York Law School in 2020.

I. INTRODUCTION

The Fourth Amendment to the U.S. Constitution protects the "privacy and security of individuals against arbitrary invasions by" the government.[1] But under the third-party doctrine, first articulated in the 1970s,[2] when someone voluntarily provides information to a third party, they risk losing that protection because the government is permitted to access the information from the third party without a warrant.[3] In today's digital world, personal information maintained by third parties is all-encompassing and voluminous;[4] until relatively recently, access to information of this nature and in such volume by third parties was unimaginable.[5]

---

1. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (quoting Camara v. Mun. Ct. of City & Cnty. of S.F., 387 U.S. 523, 528 (1967)) (internal quotations omitted); *see also* Katz v. United States, 389 U.S. 347, 350 (1967) (recognizing that the Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion"). The Fourth Amendment provides

   > [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

   U.S. Const. amend. IV. Although the Constitution does not directly provide for a fundamental right of privacy, "[t]he Court used the personal protections expressly stated in the First, Third, Fourth, Fifth, and Ninth Amendments to find that there is an implied right to privacy in the Constitution." *Privacy*, Legal Info. Inst., https://www.law.cornell.edu/wex/privacy (last visited Apr. 13, 2021). This Note focuses on the Fourth Amendment.

2. Richard M. Thompson II, Cong. Rsch. Serv., R43586, The Fourth Amendment Third-Party Doctrine 9 (2014), https://fas.org/sgp/crs/misc/R43586.pdf. *See generally* Smith v. Maryland, 442 U.S. 735 (1979) (reviewing whether the third-party doctrine applied to phone call records maintained by a telephone company); United States v. Miller, 425 U.S. 435 (1976) (analyzing bank documents under the third-party doctrine).

3. *See Carpenter*, 138 S. Ct. at 2219–20 ("The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another.").

4. John Villasenor, *What You Need to Know about the Third-Party Doctrine*, The Atlantic (Dec. 30, 2013), https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/. For example, Facebook collects personal data obtained through artificial intelligence that analyzes the behavior of Facebook's users and non-users to provide targeted advertisements. Natasha Singer, *What You Don't Know About How Facebook Uses Your Data*, N.Y. Times (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html. Similarly, retailers track their customers' online activities, including whether customers "click on any of the links inside the email[s]" they sent, the number of visits to their websites, purchases through their loyalty card programs, and even customer shirt sizes and preferences. *Your Data Is Shared and Sold… What's Being Done About It?*, Knowledge @ Wharton (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/.

5. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (citations omitted) (noting that "it may be necessary to reconsider the [1970s] premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" because, in today's digital age, "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks").

In *Carpenter v. United States*, the Supreme Court held in 2018 that the government must obtain a warrant to access historical cell-site location information (CSLI),[6] but opted not to extend that requirement to other, similar types of location-based tracking data maintained by many third parties.[7] Specifically, the Court in *Carpenter* did not extend Fourth Amendment privacy protections to emerging forms of real-time data or tracking technologies, which convey private information to third parties such as Apple.[8] *Carpenter* was the perfect opportunity for the Court to eradicate the third-party doctrine, as necessitated by the development of novel technologies.[9] Instead, the Court tackled the narrow issue of CSLI only, leaving other voluminous private information potentially exposed to warrantless searches by the government.[10]

The third-party doctrine is outdated and undermines Fourth Amendment protections as applied to today's digital technologies, which, often more coercively than voluntarily, convey so much of our information to third parties.[11] The mere fact

6. "Cell phones perform their . . . functions by connecting to a set of radio antennas," typically mounted on towers, flagpoles, or buildings, called "cell sites." *Carpenter*, 138 S. Ct. at 2211. "Cell phones continuously scan their environment for the signal, which generally comes from the closest cell site." *Id.* "Each time a phone connects to a cell site, it generates a time-stamped record [of its location,] known as cell-site location information (CSLI)." *Id.* CSLI data may be generated by a user's intentional actions (e.g., calling, texting, or even just turning the phone on), or automatically without an intentional action (e.g., "when a phone receives a text message or when the phone sends periodic updates to the network"). Sabrina McCubbin, *Summary: The Supreme Court Rules in* Carpenter v. United States, Lawfare (June 22, 2018), https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states.

7. *See Carpenter*, 138 S. Ct. at 2220 (describing the decision as "a narrow one" that focuses on "the unique nature of cell phone location information" and does not address "real-time CSLI or 'tower dumps,'" "conventional surveillance techniques and tools, such as security cameras," or "other business records that might incidentally reveal location information"). Specifically, the Court stated that "accessing seven days of CSLI constitutes a Fourth Amendment search." *Id.* at 2217 n.3. "Because *Carpenter* involved records acquired from cell phone companies, the third-party doctrine was [essential] to the government" to obtain the information without a warrant. McCubbin, *supra* note 6.

8. *Carpenter*, 138 S. Ct. at 2220; Daniel R. Stroller, *Location Data Privacy Protection Expanding in Judges' Hands*, Bloomberg (Aug. 21, 2019), https://news.bloomberglaw.com/privacy-and-data-security/location-data-privacy-protection-expanding-in-judges-hands. For example, enabling location services on your Apple Watch allows Apple and other third-party apps and websites to automatically collect and use information based on your current location. *Location Services & Privacy*, Apple (Sept. 18, 2020), https://support.apple.com/en-us/HT207056 (last visited Apr. 13, 2021).

9. *See* Daniel Solove, Carpenter v. United States*, Cell Phone Location Records, and the Third Party Doctrine*, TeachPrivacy (July 1, 2018), https://teachprivacy.com/carpenter-v-united-states-cell-phone-location-records-and-the-third-party-doctrine/ ("[T]he Supreme Court finally took a step forward to bring the Fourth Amendment more in line with the digital age. But this was only a step in the year 2018, when the Court should have walked more than a mile.").

10. *Carpenter*, 138 S. Ct. at 2217 n.3. The Court should have broadened its holding to find that an individual maintains a legitimate expectation of privacy in the record of their physical movements as captured through all location-based data, such as that generated by an Apple Watch. *But see id*. at 2217 ("[A]n individual maintains a legitimate expectation of privacy in the recording of his physical movements as captured through CSLI [only].").

11. Solove, *supra* note 9; *see also* Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 Nw. J. Tech. & Intell. Prop. 321, 326 (2013) (recognizing that when companies notify consumers that their information may be disclosed, "this notice . . . comes in the form of a blanket opt-in/

that a third party holds someone's information should not supersede constitutional protections.[12] The Founders' "papers" and "effects" in the Fourth Amendment have been interpreted as flexible, all-encompassing terms, and the third-party doctrine should not apply to their modern-day equivalents.[13] Further, the purpose of the Fourth Amendment is to limit the government's information gathering abilities when serious privacy considerations are involved.[14] However, the third-party doctrine does not require the government to establish probable cause when many novel technologies are at play.[15] The courts should reconstruct the third-party doctrine to accommodate the realities of our time.[16]

This Note contends that courts should eliminate the outdated third-party doctrine and apply a modern-day version of the reasonable expectation of privacy test, as articulated in 1967 in *Katz v. United States*, with respect to (1) information that could infringe upon privacy inside the home and (2) real-time location-based tracking data.[17] Part II of this Note provides a historical overview of the third-party

opt-out approach" that leaves consumers "with little to no control over their information"). For example, individuals wishing to use social media provide data to companies like Facebook and Instagram by agreeing to their complex user agreements; however, no one can negotiate these agreements and rarely anyone reads them. *See* David Berreby, *Click To Agree With What? No One Reads Terms of Services, Studies Confirm*, The Guardian (Mar. 3, 2017), https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print. As a result, users are faced with a "take it or leave it" choice of either forgoing their expectations of privacy in exhange for access to these platforms or prioritizing their privacy interests and forgoing access to these platforms. *See* Asay, *supra*.

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

13. *See* Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. of Nat'l Sec. L. & Pol'y 247, 271 (2016) (arguing that "the history and purpose of the Fourth Amendment require a flexible reading of 'papers' that would encompass clear categories of potentially expressive and associational data" and that should include "personal files stored in the cloud, . . . communications data[,] and metadata"); *see also* Solove, *supra* note 9 ("The fact that the Fourth Amendment mentions physical things . . . is because there weren't digital records at the time. The list of 'persons, houses, papers, and effects' is meant to be a broad inclusive list . . . .").

14. Solove, *supra* note 9.

15. *See id.* ("[T]he Third Party Doctrine is deeply flawed and eviscerates Fourth Amendment protection in today's digital age where so much of our information is in the hands of third parties."); *see also* Steven J. Arango, *The Third-Party Doctrine in the Wake of a "Seismic Shift"*, Am. Bar Ass'n (June 13, 2019), https://www.americanbar.org/groups/litigation/committees/privacy-data-security/practice/2019/third-party-doctrine-wake-of-seismic-shift/ (arguing that "Congress needs to address cloud privacy with legislation" by "[r]equiring probable cause and a warrant to access this information").

16. *See* United States v. Carpenter, 819 F.3d 880, 894–96 (6th Cir. 2016) (Stranch, J., concurring) (agreeing with Justice Sonia Sotomayor's concurrence in *United States v. Jones*, 565 U.S. 400 (2012), that it is for the courts to design an updated Fourth Amendment doctrine, not the legislature), *rev'd and remanded*, 138 S. Ct. 2206 (2018).

17. *See* 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (articulating the reasonable expectation of privacy test, which was subsequently adopted by the Supreme Court). To determine whether government conducts a search under the Fourth Amendment, there are two requirements to establish a reasonable expectation of privacy: first, "that a person . . . exhibited an actual (subjective) expectation of privacy and, second, that the expectation [is] one that society is prepared to recognize as 'reasonable.'" *Id.* (parenthesis in original).

doctrine and Part III discusses the ways in which the doctrine is outdated today. Part IV sets forth the modern-day test and Part V concludes this Note.

II. HISTORICAL OVERVIEW OF THE THIRD-PARTY DOCTRINE

The Fourth Amendment has two operative portions: (1) it protects individuals from unreasonable searches and seizures and (2) it requires the government to obtain a warrant supported by probable cause in order to search and seize.[18] Determining when these privacy protections apply is informed by the understandings of what was considered an unreasonable search at the time the Fourth Amendment was adopted.[19] Historically, law has recognized that the Fourth Amendment sought "to secure the 'privacies of life' against 'arbitrary power.'"[20] Thus, the Founders' central aim was to restrain the government from trampling on these privacies without limitation.[21]

Throughout much of America's history, the Fourth Amendment was connected to common law trespass; courts focused on whether the government physically intruded into a constitutionally protected area, triggering warrant requirements.[22] However, in 1967, the Supreme Court recognized in *Katz v. United States* that the Fourth Amendment "protects people, not places."[23] The Court expanded its interpretation of the Fourth Amendment by holding that wiretapping a public phone booth constituted an unreasonable search.[24] Importantly, Justice John Marshall Harlan's *Katz* concurrence, later adopted by the Supreme Court, articulated a two-prong test to determine whether an individual has a reasonable expectation of privacy under the Fourth Amendment, thereby restraining the government from conducting unreasonable warrantless searches.[25] That test examines (1) whether the individual had a subjective belief that they enjoyed a privacy interest, and (2) whether society

18. U.S. Const. amend. IV.

19. Carpenter v. United States, 138 S. Ct. 2206, 2213–14 (2018).

20. *Id.* at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

21. *Id.* at 2213 (quoting Riley v. California, 573 U.S. 373, 403 (2014)) ("The Founding generation crafted the Fourth Amendment as a 'response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.'").

22. *Id.* at 2213 (citation omitted).

23. 389 U.S. 347, 351 (1967).

24. *See id.* at 350–51, 358–59 (holding that a trespass was not dispositive for finding a Fourth Amendment violation). In *Katz*, the FBI suspected that Charles Katz was engaged in illegal gambling and planted a listening device outside a public phone booth from which he often placed calls. *Id.* at 348. As a result, the FBI recorded Katz's phone call conversations and subsequently convicted Katz for transmitting wagering information in violation of federal law. *Id.*

25. *See id.* at 361 (Harlan, J., concurring) (recognizing that searches of constitutionally protected areas are "presumptively unreasonable in the absence of a search warrant" and discussing the reasonable expectation of privacy test); Smith v. Maryland, 442 U.S. 735, 740 (1979) (expressly adopting the two-prong test articulated in the *Katz* concurrence).

recognizes that belief to be valid and legitimate.[26] Under this test, satisfaction of both prongs is required to establish a constitutional violation of a privacy interest.[27]

In 1976, the Supreme Court held in *United States v. Miller* that the Fourth Amendment does not prevent the government from obtaining information revealed voluntarily to a third-party bank.[28] The *Miller* Court reasoned that a depositor who reveals his business affairs to a bank assumes the risk that the information may be conveyed to the government.[29] Further, in 1979, the Court stated in *Smith v. Maryland* that "a person has no legitimate expectation of privacy in information [they] voluntarily turn over to [a third party]."[30] In *Smith*, the police, without a warrant, requested that the telephone company install a pen register[31] to record the numbers dialed from Michael Lee Smith's phone.[32] Like the *Miller* Court, the *Smith* Court reasoned that a telephone user assumes the risk that the telephone company could reveal the dialed numbers to the police.[33]

---

26. *See Katz*, 389 U.S. at 361 ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

27. *Id.* The *Katz* Court concluded that Katz expected his telephone conversation to remain private because he closed the telephone booth door behind him, and that such expectation was objectively reasonable because "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." *See id.* at 352 (majority opinion) ("One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

28. 425 U.S. 435, 442–43 (1976). The Court found that "[a]ll of the documents obtained . . . contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," and further stated that the Fourth Amendment does not prohibit the government from obtaining such information "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* Mitchell Miller was convicted of, among others, intent to defraud the government of an alcohol tax, possessing alcohol without paying taxes, and conspiring to defraud the government of tax revenues. *Id.* at 436. The government used the bank records to support its contention that Miller committed overt acts in furtherance of the conspiracy to defraud the government. *Id.* at 438. The Court concluded that the government did not violate Miller's expectation of privacy and that obtaining bank records Miller had voluntarily turned over to the bank was not a search. *Id.* at 442–45.

29. *Id.* at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971)).

30. 442 U.S. at 743–44 (citations omitted).

31. "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977).

32. *Smith*, 442 U.S. at 737. The pen register in *Smith* recorded only outgoing phone numbers dialed, not the communications themselves. *Id.* at 741 (quoting *N.Y. Tel. Co.*, 434 U.S. at 167). Police installed the pen register after a robbery victim received threatening and obscene phone calls from a man identifying himself as the robber, who fit the description of Smith. *Id.* at 737. The Court held that the police did not need a warrant to monitor Smith's outgoing call log. *See id.* at 741–46 (analyzing the warrantless installation of a pen register under the reasonable expectation of privacy test).

33. *Id.* at 744.

Miller and *Smith* formulated what is today known as the third-party doctrine:[34] when an individual "voluntarily provides information to a third party, the Fourth Amendment does not preclude the government from accessing [such information] without a warrant."[35] The rationale behind this doctrine is that the individual assumes the risk that such information will be disclosed to others and that, therefore, it need not be protected by the Fourth Amendment from warrantless government searches.[36]

The third-party doctrine remained relatively unscathed until 2012, when the Supreme Court decided *United States v. Jones*.[37] There, the Court held that the installation of a GPS tracking device on Antoine Jones' vehicle, without a warrant, constituted an unlawful trespass and therefore a search.[38] Although the holding in *Jones* did not directly address the third-party doctrine, the respective concurrences of Justices Sonia Sotomayor and Samuel Alito questioned whether the third-party doctrine is still appropriate given today's digital landscape.[39] Specifically, the Justices were concerned that the prolonged monitoring of an individual's location infringes upon our reasonable expectation of privacy in public movements.[40]

---

34. Villasenor, *supra* note 4.

35. *Id.*; *see* Carpenter v. United States, 138 S. Ct. 2206, 2219–20 (2018).

36. Caitlin Campbell, *Mixed Signals: An Analysis of the Third-Party Doctrine as Applied to Warrantless Collection of Historical Cell Site Location Information*, Ark. J. Soc. Change & Pub. Serv. (Apr. 4, 2018) (footnote omitted), https://ualr.edu/socialchange/2018/04/04/mixed-signals-analysis-third-party-doctrine-applied-warrantless-collection-historical-cell-site-location-information/; *see also Smith*, 442 U.S. at 744 (noting that confiding information to a third party "on the assumption that it will be used only for a limited purpose" does not offer protection under the Fourth Amendment when that third party betrays such confidence).

37. 565 U.S. 400 (2012).

38. *See id.* at 404–05. The Court in *Jones* clarified that any situation in which there was no trespass would remain subject to the reasonable expectation of privacy analysis set forth in *Katz*. *Id.* at 411.

39. *See id.* at 414–15 (Sotomayor, J., concurring) ("In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance."); *see also id.* at 427–30 (Alito, J., concurring) (arguing that a search occurs when police surveillance of an individual's activity, even a public one, is prolonged and pervasive).

40. *Id.* at 416 (Sotomayor, J., concurring); *id.* at 430–31 (Alito, J., concurring). Justice Sotomayor stated:

> I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs [and] sexual habits . . . . I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power and prevent 'a too permeating police surveillance[.]'

Id. at 416–17 (Sotomayor, J., concurring) (citations omitted). Justice Alito observed that the best way to determine whether law enforcement infringed on an individual's expectation of privacy is to "apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated." *Id.* at 430 (Alito, J., concurring).

In 2018, the Supreme Court considered in *Carpenter* whether the Fourth Amendment requires the government to obtain a warrant before accessing historical CSLI data maintained by a third party.[41] The Court held that the government needed a warrant to access such data, but failed to extend that warrant requirement to other technologies.[42] The majority in *Carpenter* recognized that "personal location information maintained by a third party . . . does not fit neatly" into the existing *Jones*, *Miller,* and *Smith* jurisprudence.[43] However, the holding in *Carpenter* was rather limited; the Court did not address other potential forms of technology that the government could obtain data from without a warrant, such as social media accounts, dating apps, bankcards, and nanny cams, all of which penetrate deeply into an individual's intimate sphere and risk violating their privacy interests.[44]

III. THE PROBLEM WITH THE THIRD-PARTY DOCTRINE

As a result of *Carpenter*, courts have little guidance on whether real-time location data and other emerging tracking technologies deserve the same Fourth Amendment

41. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018). Prior to trial, Timothy Carpenter moved to suppress the CSLI records, arguing that the government's seizure of CSLI violated his Fourth Amendment rights because the information was obtained without a warrant supported by probable cause. *Id.* at 2212. The District Court disagreed and denied the motion. *Id.* The Court of Appeals for the Sixth Circuit affirmed the trial court's decision and held that Carpenter "lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers." *Id.* at 2213. The Sixth Circuit concluded that the business records resulting from voluntarily conveyed cell-site data to wireless carriers are not entitled to Fourth Amendment protection. *Id.*

42. *Id.* at 2219–20. Specifically, the Court acknowledged that the Stored Communications Act, which "require[s] the [g]overnment to show 'reasonable grounds' for believing the [CSLI] records [are] 'relevant and material to an ongoing investigation,'" is not a permissible mechanism for compelling a wireless carrier to turn over CSLI to the government. *Id.* at 2221 (quoting U.S.C. § 2703(d)). However, the Court did not address whether accessing less than seven days of CSLI would constitute a search under the Fourth Amendment, nor whether accessing similar data obtained via other technologies deserves any Fourth Amendment protections. *See id*. at 2234 (Kennedy, J., dissenting) (criticizing the majority for leaving it to law enforcement to "guess how much of that information can be requested before a warrant is required" and for "expressing no opinion on 'real-time CSLI,' tower dumps, and security-camera footage[,]" leaving unanswered the question of "whether greater or lesser thresholds should apply to information like IP addresses or website browsing history").

43. *See id.* at 2214–17 (majority opinion). The Court struggled to classify the information at issue and noted that it lies at the intersection of *Jones* (whether a person has a legitimate expectation of privacy in his or her location), and *Smith* and *Miller* (whether a person has a legitimate expectation of privacy once it is turned over to a third party). *Id.*

44. *See id.* at 2220 (stating that "[t]his decision is narrow" and "do[es] not express a view on matters not before [the Court,]" nor does it "disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras," "[n]or do[es it] address other business records that might incidentally reveal location information . . . [or] other collection techniques involving foreign affairs or national security"); *see also* Solove, *supra* note 9 ("The [*Carpenter*] Court treats [CSLI records] as if they were cutting-edge technological issues. In fact, they are rather old technological issues. A larger problem with the decision is that it fails to provide much guidance about when the Third Party Doctrine would apply in other contexts.").

protections as historical CSLI.[45] This uncertainty means that, by allowing third parties to access such other data, users open the door for the government to obtain it from third parties without a warrant.[46]

It would be highly impractical to participate in modern society without revealing personal data to third-party service providers.[47] Disclosures of private information are necessary to navigate our daily lives and perform basic functions like online banking, communicating via smartphones, or purchasing goods with credit cards.[48] It is difficult to argue that using such conveniences is voluntary when they are almost ubiquitous and alternatives are scarce.[49] Therefore, in essence, the third-party doctrine serves as a contract of adhesion—users may choose to either enjoy privacy protections or 'sign the contract,' forfeit privacy protections, and gain access to digital technologies.[50] Courts have held that a contract will not be enforced if it would impose an unreasonable restriction on a person's right to exercise their living.[51] But shouldn't individuals retain their Fourth Amendment protections when navigating daily life with a little help from cell phones, dating sites, or ATMs?

Significant privacy issues also surround the effect that the third-party doctrine has on privacy in the home, which is intimate and should be safe from warrantless

45. *Carpenter*, 138 S. Ct. at 2220, 2222; *see also* Stroller, *supra* note 8. The Court in *Jones* solidified its holding using "a trespass theory in which attaching . . . the GPS device was a trespass to Jones's property under the Fourth Amendment, which for many observers was a convenient solution to an increasingly thorny third-party problem." Michael Bahar et al., *Third-Party Party-Crashing? The Fate of the Third-Party Doctrine*, Lawfare (Oct. 19, 2017), https://www.lawfareblog.com/third-party-party-crashing-fate-third-party-doctrine. Real-time (or live) location data has the capability of revealing an individual's specific location in real time, whereas historical data tracks and stores past movements and locations. *Live GPS Tracking vs. Historical GPS Data Logging*, XtremeTrakGPS, https://www.xtremetrakgps.com/live-gps-tracking-vs-historical-gps-data-logging.html (last visited Apr. 13, 2021).

46. Josephine Wolff, Opinion, *Losing Our Fourth Amendment Data Protection*, N.Y. Times (Apr. 28, 2019), https://www.nytimes.com/2019/04/28/opinion/fourth-amendment-privacy.html.

47. United States v. Davis, 785 F.3d 498, 525 (11th Cir. 2015) (Rosenbaum, J., concurring).

48. *Id.* (citations omitted) ("[U]nder the third-party doctrine, '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.'").

49. *See* Campbell, *supra* note 36 ("Such conveyance [of information to third-party service providers] cannot be voluntary if society does not afford the option to forego [sic] a device that automatically conveys one's sensitive location information.").

50. *See* Restatement (Second) of Conts. § 208 (Am. L. Inst. 2020) ("If a contract or term thereof is unconscionable at the time the contract is made a court may refuse to enforce the contract, or may enforce the remainder of the contract without the unconscionable term, or may so limit the application of any unconscionable term as to avoid any unconscionable result."). *See generally* Masooda Bashir et al., *Online Privacy and Informed Consent: The Dilemma of Information Asymmetry*, Ass'n for Info. Sci. & Tech (Feb. 24, 2016), https://asistdl.onlinelibrary.wiley.com/doi/epdf/10.1002/pra2.2015.145052010043 (exploring the notion that most privacy policies and terms of service agreements are adhesion contracts and proposing ways to resolve this issue).

51. Simons v. Fried, 98 N.E.2d 456, 456 (N.Y. 1951).

government intrusion.[52] In *Kyllo v. United States*, the Court held in 2001 that using sense-enhancing technology[53] to obtain information about a marijuana growing scheme inside a home, which would otherwise involve a "physical intrusion into a constitutionally protected area," constituted a search.[54] The *Kyllo* Court was concerned about advancing technology and the effect it could have on the sanctity and privacy of the home, but did not consider the third-party doctrine per se.[55] Yet, under that doctrine today, the government could essentially enter one's home without a warrant by accessing third-party records created by smart devices inside, such as nanny cams or smart pet feeders; this access could prove to be a greater intrusion into the home than the sense-enhancing technology in *Kyllo*.[56] Thus, given the nearly ubiquitous use of modern digital services and technologies, and the outdated nature of the third-party doctrine, even the sanctity of the home may no longer be sufficiently protected by the Fourth Amendment.[57]

---

52. *See* Kyllo v. United States, 533 U.S. 27, 37 (2001) ("In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.") (emphasis in original). The Court in *Kyllo* noted that there is a "minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*," when it comes to searching one's home without a warrant and to remove that minimum expectation "would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment." *Id.* at 34 (emphasis in original).

53. Sense-enhancing technology is "used to enhance the human ability to observe or recognize physical characteristics or activities." K. A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 Yale J.L. & Tech. 123, 173 (2005) (footnote omitted). This type of technology often "can be further classified as those that *amplify* the existing human senses, or those that extend these senses by making previously undetectable phenomena observable." *Id.* (emphasis in original). For example, binoculars, telescopes, cameras, drug sniffing dogs, and sensors that can hear through walls are devices that amplify human senses, while devices such as infrared or ultra-violet sensors, radars, and radio receivers are devices that extend the human senses. *Id.*

54. 533 U.S. at 34 (citation omitted). The government, suspecting that defendant Danny Kyllo was growing marijuana in his house, used a thermal imaging device to detect the amount of heat radiating from the house. *Id.* at 29. The device detected radiation amounts consistent with the use of high-intensity lamps required for growing marijuana indoors. *Id.* The government obtained a search warrant of Kyllo's home in part because of the thermal imaging scans, and found an indoor marijuana growing operation. *Id.* at 29–30.

55. *See id.* The holding in *Kyllo* was meant to preserve the degree of protection against government intrusion that existed when the Fourth Amendment was adopted. *Id.*

56. *See* Daniel Solove, *10 Reasons Why the Fourth Amendment Third Party Doctrine Should be Overruled in* Carpenter v. US, TeachPrivacy (Nov. 28, 2017), https://teachprivacy.com/carpenter-v-us-10-reasons-fourth-amendment-third-party-doctrine-overruled [hereinafter *10 Reasons Why*] ("[T]he home can be searched now through third party records, and that means the Fourth Amendment will increasingly cease to be much of a protection to privacy in the home."); *see, e.g.*, *Privacy Policy for Nest Websites*, Nest, https://nest.com/legal/privacy-policy-for-nest-web-sites/ (last updated Jan. 31, 2020) (disclosing that Nest will share personal information with third parties if it has a good faith belief that disclosing the information is reasonably necessary to meet any enforceable government request); *see also, e.g.*, *PetSmart Privacy Policy*, PetSmart, https://www.petsmart.com/help/privacy-policy-H0011.html (last updated Dec. 2020) (disclosing that PetSmart collects, uses, and discloses information about users when they access or use the company's websites, mobile applications, and other online products).

57. *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, 1925 (May 9, 2017), https://harvardlawreview.org/wp-content/

IV. REPLACING THE THIRD-PARTY DOCTRINE

The *Katz* test "rests on the assumption that . . . the reasonable person has a well-developed and stable set of privacy expectations."[58] However, dramatic technological changes may alter those expectations, resulting in a decreased sense of privacy in return for the increased accessibility that new technology brings.[59] Consequently, technological development has required the Supreme Court to articulate new ways to protect individual privacy interests.[60]

In *Carpenter*, the Court should have considered whether there is a reasonable expectation of privacy in digital real-time location data that creates a protected privacy interest despite third-party access to or possession of that data.[61] Justice Anthony Kennedy's dissent in *Carpenter* provides a glimpse into what the world might look like without such protected interest.[62] His argument that Carpenter lacked a privacy interest in CSLI data because the data was shared with a third party is troublesome, given the amount of information that is routinely—and sometimes unknowingly—handed to third parties.[63]

I propose that the courts engage in a balancing analysis and take three questions into consideration when determining whether the government is authorized to obtain information via the third-party doctrine. The first question is whether obtaining third-party records infringes upon privacy inside the home.[64] The current third-party doctrine, as it relates to smart home devices, is not compatible with the historical notions of home privacy.[65] The government should be required to obtain a

uploads/2017/05/1924-1945_Online.pdf ("Fourth Amendment jurisprudence . . . has not adequately evolved to compensate for the rapid explosion in both the quantity and sensitive quality of the information shared [with third parties].").

58. United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring).

59. *See id.* ("Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.") (footnote omitted).

60. *See, e.g.*, *Kyllo*, 533 U.S. at 34–35; *see also, e.g.*, Riley v. California, 573 U.S. 373, 373–74 (2014) (discussing the mass of personal information often contained in a cell phone and holding that, absent exigent circumstances, searching the contents of a cell phone requires a warrant).

61. *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (first citing Smith v. Maryland, 442 U.S. 735, 742 (1979); and then citing United States v. Miller, 425 U.S. 435, 443 (1976)); *see also* Solove, *supra* note 9 ("*Carpenter* would have been the ideal case to get rid of the Third Party Doctrine.").

62. *See* Carpenter v. United States, 138 S. Ct. 2206, 2224 (2018) (Kennedy, J., dissenting) ("According to today's majority opinion, the [g]overnment can acquire a record of every credit card purchase and phone call a person makes over months or years without upsetting a legitimate expectation of privacy.").

63. *See id.* at 2230; *see also* McCubbin, *supra* note 6 and accompanying text; *see also* Asay, *supra* note 11 and accompanying text.

64. *See Kyllo*, 533 U.S. at 34 ("The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.").

65. *See 10 Reasons Why*, *supra* note 56 (noting that while the Supreme Court has consistently held that "the quintessential protection of the Fourth Amendment is to protect privacy in the home," the development of

warrant to gain access to private information through smart home devices because the history and jurisprudence of the United States has always granted heightened protections to the sanctity and privacy of the home.[66]

The second question is whether the government is using third-party records to track real-time physical location and movements via one's cell phone.[67] The government should be required to obtain a warrant, absent exigent circumstances, because—in the modern age—our cell phones are always with us, almost as an extension of the human body,[68] which we take wherever we go.[69] Furthermore, an individual's location may be tracked even after they turn off their phone's location services.[70] Warrantless access to a phone's every location thus impinges on an individual's reasonable expectation of privacy because our society's expectation has always been that government agents cannot secretly monitor every movement of an individual for a long period of time using traditional investigative techniques.[71] The third-party doctrine should not allow the government to take advantage of any cell phone's location services in a way that—compared to more traditional investigative tools—is effortless, inexpensive, and

smart homes and the current third-party doctrine means that "[t]he government no longer needs to enter a person's home to learn about that person . . . [because all can] be learned from third party records").

66. *See* U.S. Const. amend. III (protecting against quartering of soldiers in private homes without the owner's consent); *see also, e.g.*, *Kyllo,* 533 U.S. at 37 (recognizing that "[i]n the home, . . . *all* details are intimate details" and should be safe from government's reach) (emphasis in original).

67. *See Carpenter*, 138 S. Ct. at 2216 (noting that "cell phone location information is detailed, encyclopedic, and effortlessly compiled"); *see also id.* at 2218 (quoting Riley v. California, 573 U.S. 373, 385 (2014)) (recognizing that a cell phone is "'almost a feature of human anatomy'" that "tracks nearly exactly the movements of its owner").

68. *See id.* at 2218. However, warrantless searches under exigent circumstances such as terrorist threats, active shootings, and child abductions should be permitted. *See id.* at 2223 (recognizing that specific threats justify a warrantless search of digital information that may reveal the physical location of an individual).

69. *See id.* at 2220 (quoting *Riley*, 573 U.S. at 385) ("[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."). Smartphones "tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the [many features of their] phone." *Id.* at 2211. "As a result, in no meaningful sense does the user voluntarily assume the risk of turning over a comprehensive [record] of his [or her location or] physical movements." *Id.* at 2220 (internal quotations omitted) (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)). Thus, the privacy interests at stake outweigh the fact that information was disclosed to a third party. *See id.* at 2217 (holding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements . . . captured through CSLI" and "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection").

70. *See* Ryan Nakashima, *Google Tracks and Records Your Movements Even If You Turn Off Location History*, L.A. Times (Aug. 13, 2018), https://www.latimes.com/business/technology/la-fi-tn-google-location-tracking-20180813-story.html (explaining how, even with the "location history" setting off, phones are still tracking and recording the user's location from web browsers and app activity). *See also Carpenter*, 138 S. Ct. at 2220 ("Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.")

71. United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring).

efficient, without first obtaining a warrant supported by probable cause, or without exigent circumstances.[72]

The third question is whether the location-based data retrieved by the government reveals an individual's physical location and movements by means other than through a cell phone's location monitoring system. In this situation, courts should weigh three factors.

The first factor is the voluntariness of a user's location disclosure.[73] Similar to CSLI records, which are generated for commercial purposes, certain records generated for other commercial purposes also require revealing one's location, thus reducing the expectation of privacy under the Court's outdated test.[74] For example, using a debit card to withdraw money automatically reveals an individual's location.[75] Debit cards are a near-necessity for modern life, and since there is no other way to use a debit card without revealing your location, the disclosure is not voluntary.[76] Therefore, the government should be required to obtain a warrant to access this information.[77] Similarly, browsing a dating website can track and store an individual's location

72. *See Carpenter*, 138 S. Ct. at 2217–18 (comparing the invasiveness of GPS monitoring and CSLI); *see also Jones*, 565 U.S. at 429–30 (Alito, J., concurring) (recognizing that surveilling Jones for four weeks without the "relatively easy and cheap" GPS device would have been "difficult and costly," requiring "a large team of agents, multiple vehicles, and perhaps aerial assistance"). GPS monitoring "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

73. *Carpenter*, 138 S. Ct. at 2220 (declining to extend the third-party doctrine to CSLI because "[c]ell phone location information is not truly 'shared' as one normally understands the term" and therefore, such information is not "voluntarily" disclosed to the third party). Essentially, courts should determine whether the individual was forced to enter into a contract of adhesion in order to use the service or product. *See* Restatement (Second) of Conts. § 208 (Am. L. Inst. 2020) (defining a contract of adhesion).

74. *Carpenter*, 138 S. Ct. at 2217; *see, e.g.*, *Mastercard – Global Privacy Notice*, Mastercard, https://www.mastercard.us/en-us/vision/corp-responsibility/commitment-to-privacy/privacy.html (last visited Apr. 13, 2021) [hereinafter *Mastercard*] (disclosing the various purposes for which Mastercard collects an individual's "Personal Information," including location); *see also, e.g.*, *Privacy Policy*, Bumble, https://bumble.com/privacy (last visited Apr. 13, 2021) [hereinafter Bumble] (explaining the type of personal information collected and providing to whom such information could be disclosed).

75. *See, e.g.*, *Mastercard*, *supra* note 74; *see also, e.g.*, Visa, Visa Global Privacy Notice 1, https://usa.visa.com/dam/VCOM/global/support-legal/documents/privacy-notice.pdf (last visited Apr. 13, 2021) [hereinafter Visa Notice] (disclosing that every time a Visa card is used, Visa receives the "date, time, location, and amount of the transaction and information about the merchant" and "geolocation information, browsing history and other information available via digital interactions" such as Visa "products, services, websites or apps").

76. *See* Shelle Santana, *Is the U.S. on Its Way to Becoming a Cashless Society?*, Harv. Bus. Rev. (July 23, 2019), https://hbr.org/2019/07/is-the-u-s-on-its-way-to-becoming-a-cashless-society (discussing the "rise of digital payments" and reporting that "findings suggest that the cashless trend is clear but nuanced"); *see also* Bashir et al., *supra* note 50, at 2 ("A lack of alternative service delivery models . . . or competition between providers can undermine the degree of voluntariness of users' consent.").

77. *Compare Carpenter*, 138 S. Ct. at 2217–18, 2220 (concluding that a warrant is required to obtain an individual's CSLI data because the data "is not truly 'shared'" and the amount of information revealed permits the government to "travel back in time to retrace a person's whereabouts," presenting an "even greater privacy concern[]"), *with* Visa Notice, *supra* note 75 (recording the user's location every time

information, allowing the government to access that data per the third-party doctrine; that too should require a warrant to satisfy Fourth Amendment protections.[78] Such location disclosures are required if one wants to remain engaged with modern society, and are therefore involuntary.

The second factor is whether the tracking is facilitated by (1) a rudimentary device capable of tracking for a short period of time, such as a battery-operated beeper, or (2) a more comprehensive mode of surveillance capable of tracking for a longer period of time, such as twenty-four-hour video surveillance.[79] If the former is used, then the third-party doctrine can apply because short-term tracking makes privacy a lesser concern.[80] However, if the electronic surveillance is more sophisticated and used for a longer period,[81] then the third-party doctrine should not apply because it is more likely to infringe on an individual's reasonable expectation of privacy.[82] In such instances, and absent exigent circumstances, the government should be required to obtain a warrant.[83]

---

they use their Visa card). Using a debit card thus falls into the contract of adhesion category. *See* Restatement (Second) of Conts. § 208.

78. *Compare Carpenter*, 138 S. Ct. at 2217–18, 2220, *with* Bumble, *supra* note 74 (informing users that their collected information will be disclosed to the government when it is requested). Thus, accessing dating sites also falls into the contract of adhesion category. *See* Restatement (Second) of Conts. § 208.

79. *See Carpenter*, 138 S. Ct. at 2215 (discussing the reasonable expectation of privacy standard with respect to surveillance tools used in precedent); *see also* United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring).

80. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 284–85 (1983) (holding that a warrant was not required to monitor and follow signals from a beeper placed in a drum of chloroform that was being transported to a drug lab by the defendant). The Court in *Knotts* noted that the beeper signals revealed nothing more than what would have been observed by a police car following the vehicle containing the drum and beeper. *Id.* at 285. Additionally, it noted that nothing in the record indicated that the government was continuously monitoring the beeper signals after the signals indicated that the drum was no longer moving; there was "no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin." *Id.* at 284–85.

81. It is clear that seven days of CSLI data and four weeks of GPS tracking require warrants, but aside from those parameters, the Court has yet to identify the maximum length of time for which the government may obtain an individual's location without a warrant. *See Carpenter*, 138 S. Ct. at 2266–67 (Gorsuch, J., dissenting) (citing the majority opinion) ("The Court declines to say whether there is any sufficiently limited period of time 'for which the Government may obtain an individual's historical [location information] free from Fourth Amendment scrutiny' . . . [but] seven days' worth of information *does* trigger Fourth Amendment scrutiny . . . .") (emphasis in original) (alterations in original); *see also Jones*, 565 U.S. at 430 (Alito, J., concurring) ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.").

82. *See Carpenter*, 138 S. Ct. at 2219–20 (first citing *Knotts*, 460 U.S. at 281; then citing *Jones*, 565 U.S. at 430 (Alito, J., concurring); and then citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)) (recognizing that an individual has a reduced expectation of privacy in their location information knowingly shared with another, but "more pervasive tracking" and "longer term" GPS monitoring constitutes a search under the Fourth Amendment).

83. *See Carpenter*, 138 S. Ct. at 2215 (quoting *Knotts*, 460 U.S. at 281) (noting that different "'constitutional principles may be applicable'" if the suspect was undergoing twenty-four-hour surveillance). "Prior to the digital age, [the government may] have pursued a suspect for a [limited duration] but doing so 'for any

The third factor to consider is the nature of the information the third party collects.[84] If it encompasses only limited types of data, then the individual's privacy interests are not as salient, and the government need not obtain a warrant.[85] For example, information disclosed to a prospective employer for purposes of obtaining employment would be considered limited data. However, if the third party will potentially hold an exhaustive chronicle of location information, the government should be required to obtain a warrant.[86]

V. CONCLUSION

The Founders could not have fathomed the nature and volume of information potentially exposed to remote access by the government.[87] As technology rapidly evolves, so do our privacy notions.[88] We can no longer rely on outdated understandings of privacy, like the *Katz* reasonable expectation of privacy test and the third-party doctrine, to adequately effectuate Fourth Amendment protections in an era when we must share immeasurable amounts of personal data with third parties to partake in modern life.[89] With every movement we make while holding our cell phones or wearing

extended period of time was difficult and costly and therefore rarely undertaken.'" *Id.* at 2217 (quoting *Jones*, 565 U.S. at 429 (Alito, J., concurring)). Therefore, "society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual[] . . . for a very long period of time." *Id.* (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)).

84. *See id.* at 2219 (first citing Riley v. California, 573 U.S. 373, 392 (2014); and then citing United States v. Miller, 425 U.S. 435, 442 (1976)) (acknowledging that while the third-party doctrine partly derives from the idea that "an individual has a reduced expectation of privacy in information knowingly shared with another," "the fact of 'diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely' . . . [i]nstead, [precedent] considered 'the nature of the particular documents sought' to determine whether 'there is a legitimate expectation of privacy concerning their contents'").

85. *Compare id.* at 2217 (declining to extend the third-party doctrine to CSLI data because it provides "an all-encompassing record of the holder's whereabouts" which reveals "an intimate window into a person's life"), *with Knotts*, 460 U.S. at 276–77 (extending the third-party doctrine to the government's use of a beeper to track a vehicle's movement).

86. *See Carpenter*, 138 S. Ct. at 2219 (addressing the limited types of data that were collected in precedent applying the third-party doctrine); *see also Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) ("[W]hen considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements[,] . . . I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

87. *See* Brian Frazelle & David Gray, *What the Founders Would Say About Cellphone Surveillance*, ACLU (Nov. 17, 2017), https://www.aclu.org/blog/privacy-technology/location-tracking/what-founders-would-say-about-cellphone-surveillance (arguing that the purpose of the Fourth Amendment was to protect against "the government's capacity to freely exploit . . . new technologies to monitor and control 'the people'"); *see also* Arango, *supra* note 15 (citing *Carpenter*, 138 S. Ct. at 2219) (noting that when the Court created the third-party doctrine in 1976, "it was impossible for any judge—even Supreme Court justices—to appreciate how society's reliance on technology would create a 'seismic shift' in the doctrine's reach").

88. *See* Wolff, *supra* note 46.

89. *See id.*

our smart watches, making online purchases or browsing dating sites, using navigation or smart home devices, we—knowingly or not—convey information to third parties that, either alone or in aggregate, reveal our private, personal details.[90] Although the third-party doctrine is an exception to the Fourth Amendment warrant requirement, the Court has never explicitly held that this exception applies if an individual retains a reasonable expectation of privacy in their data.[91] To ensure that the government does not have unfettered access to the voluminous electronic information that we disclose to third parties in our daily lives, the third-party doctrine should yield to a modern reasonable expectation of privacy test.

90. *See Jones*, 565 U.S. at 416 (Sotomayor, J., concurring); *see also* Villasenor, *supra* note 4 and accompanying text.

91. *See Carpenter*, 138 S. Ct. at 2221 ("[T]his Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy.").