UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 20
Issue 5 *Online Issue*

Article 1

12-1-2018

Carpenter v. United States: A New Era for Protecting Data Generated on Personal Technology, or a Mere Caveat?

Aaron L. Dalton

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 20, ONLINE: DECEMBER 2018

CARPENTER V. UNITED STATES: A NEW ERA FOR PROTECTING DATA GENERATED ON PERSONAL TECHNOLOGY, OR A MERE CAVEAT?

Aaron L. Dalton*

In deciding Carpenter, a majority of United States Supreme Court Justices recognized that, at a fundamental level, historical cell-site location information (CSLI) differs from other categories of business records in terms of deserving Fourth Amendment protection. However, the majority's opinion is unclear about the precise source of this distinction, and about how, or whether, to protect other data generated from personal technology in the future. Although the majority opinion purports to be limited to CSLI, this narrow scope is not in the best interest of consumers. At best, Carpenter presents the opportunity to establish a predictable and comprehensive system for protecting personal data from warrantless search. However, the majority's approach also risks becoming a mere caveat, drawing artificial distinctions between CSLI and other types of data that may be equally, or more, sensitive. Now that the Supreme Court has recognized some forms of data held by businesses are protected from warrantless search, this holding should be expanded to protect the increasingly comprehensive consumer data that companies acquire. Although Justice Kennedy's dissent in Carpenter highlighted the risks of the majority's unstructured approach, Justice Sotomayor's concurrence in United States v. Jones provided an aspirational glimpse of how personal data could be protected in the future. Courts should read Carpenter in conjunction with Justice Sotomayor's Jones concurrence to provide a predictable standard for evaluating personal data protections and avoid the uncertain approach that the Carpenter majority's opinion risks establishing.

* J.D. Candidate, University of North Carolina School of Law, 2020. The author would like to thank Professor Jolynn Dellinger for her insightful commentary during the writing process, and the NC JOLT team for their assistance and support.

I. INTRODUCTION

What protections do consumers operating cell phones or other personal devices that generate comprehensive data on users have from that data being obtained without a warrant and used in a criminal prosecution against them? For years, the answer has been "little or none," an alarming state of affairs in a data-driven society.[1]

[1] *See* Daniel Zwerdling, *Your Home is Your . . . Snitch? When Your Appliances Work as Police Informants*, THE MARSHALL PROJECT (May 24, 2018), https://www.themarshallproject.org/2018/05/24/your-home-is-your-snitch

Law enforcement may access consumer data without a warrant due to the third-party doctrine, which holds that consumers lack a reasonable expectation of privacy in personal data contained in business records, since this information has been disclosed to, and is held by, third parties.[2] With the explosion of personal technology,[3] scholars have questioned the validity of the third-party doctrine, as business records now consist of highly detailed information about consumers, who may not be aware of the scope of information collected and stored by companies through consumer use of ubiquitous devices.[4]

(describing law enforcement's ability to use data obtained from "smart" appliances in criminal investigations).

[2] United States v. Miller, 425 U.S. 435, 442–43 (1976) ("[W]e perceive no legitimate 'expectation of privacy' in their [banking record's] contents . . . . This Court has repeatedly held that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, 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.") (citations omitted).

[3] This Recent Development uses the term "personal technology" as a shorthand for the wide array of consumer electronic devices that send or receive signals and the programs on these devices, such as internet browsers and applications. Rather than provide an exhaustive list of connected consumer devices, the services that power them, and the applications they contain, the term "personal technology" is intended to encompass both older technologies (such as cell phones and computers), newer technologies (such as Internet of Things devices), and future connected consumer technologies, along with data-generating programs on these devices. For a discussion of Internet of Things devices, *see* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH., no. 6, 2015, at 1, 4–17; *see also* Ian Bogost, *Amazon Is Invading Your Home with Micro-Convenience*, THE ATLANTIC (Sept. 21, 2018), https://www.theatlantic.com/technology/archive/2018/09/amazon-is-invading-your-home-with-micro-convenience/571015/ (discussing Amazon's developing line of Alexa-compatible smart home appliances).

[4] *See, e.g.*, 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, 54 (2016) ("New technologies challenge many of the basic assumptions underlying such principles as the third-party doctrine. Specifically, there may be no way for a user to know or even discover what kind of information she shares with third parties, many of whom are invisible to her. Similarly, traditional models of what constitutes content and what might be considered mere transactional, non-

In *Carpenter v. United States*,[5] the United States Supreme Court issued a landmark decision for technology and privacy, as the Court reconsidered the third-party doctrine in light of technological developments.[6] The technology at issue in *Carpenter* was cell-site location information (CSLI), a form of data generated by cell phones and held by telecommunications companies.[7] When a cell phone connects to a cell tower, the connection is time-stamped and recorded, creating a detailed record of the cell phone user's movements.[8] Given the increased capabilities of cell phones, and the expanded networks of cell towers used to power them, CSLI provides detailed, location-based information on any consumer carrying a cell phone.[9] Any cell phone generates CSLI when it receives or sends a call or text message,[10] and smartphones generate CSLI "several times a minute whenever their signal is on,"[11] even when the consumer is not actively using the smartphone.[12]

Although the majority opinion discussed both the conceptualization of reasonable expectations of privacy in the

---

content information often yield nonsensical, indeterminate, or unsatisfying results when applied to modern technologies."). *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 580–81 (2009) ("Just as the Fourth Amendment should protect that which technology exposes, so should the Fourth Amendment permit access to that which technology hides. From this perspective, the third-party doctrine is needed to ensure the technology neutrality of the Fourth Amendment. It ensures that we have the same rough degree of Fourth Amendment protection independently of whether wrongdoers use third-party agents to facilitate their crimes.").

[5] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[6] *Id.* at 2214–15 ("This sort of digital data—personal location information maintained by a third party—does not fit neatly under existing precedents. Instead, requests for cell-site records lie at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake.").

[7] *See id.* at 2211–12 (discussing the technology behind CSLI).

[8] *See id.*

[9] *See id.*

[10] Robert M. Bloom & William T. Clark, *Small Cells, Big Problems: The Increasing Precision of Cell Site Location Information and the Need for Fourth Amendment Protections*, 106 J. CRIM. L. & CRIMINOLOGY 167, 172–73 (2016).

[11] *Carpenter*, 138 S. Ct. at 2211.

[12] *See id.* at 2211–12.

digital age[13] and the limitations of the third-party doctrine,[14] this Recent Development focuses primarily on the third-party doctrine aspects of the majority's opinion. The majority's decision to limit the third-party doctrine by protecting CSLI from warrantless searches[15] could drastically alter the future of consumer data privacy. By reading *Carpenter* alongside Justice Sotomayor's concurrence in *United States v. Jones*,[16] courts in future cases should find that other forms of aggregated data generated by personal technology and held by third party companies are similarly protected from warrantless searches. Alternatively, the majority's opinion could be construed narrowly,[17] representing a missed opportunity for enhanced protection of sensitive aggregated consumer data in the digital age.

After providing a brief overview of how CSLI technology records consumer data and discussing newer technology that presents additional problems in Section II, this Recent Development reviews the major cases leading up to *Carpenter* in Section III, and provides an analysis of the *Carpenter* majority holding and Justice Kennedy's dissent in Section IV. Finally, this Recent Development recommends in Section V that courts read *Carpenter* alongside Justice Sotomayor's *Jones* concurrence to establish a framework for greater Fourth Amendment protection of consumer data held by third-party businesses before contrasting this approach with one based on reading *Carpenter* alone.

II. TECHNOLOGY BACKGROUND

Although the widespread use of cell phones makes CSLI especially concerning,[18] other forms of consumer data held by third parties may be equally, or more, sensitive. Comparing CSLI with other forms of aggregated consumer data generated on personal

---

[13] *See id.* at 2215.

[14] *See id.* at 2216.

[15] *See id.* at 2223.

[16] United States v. Jones, 565 U.S. 400 (2012).

[17] *See Carpenter*, 138 S. Ct. at 2220 ("Our decision today is a narrow one. We do not express a view on matters not before us.").

[18] *See id.* at 2211 (noting that while the United States has a population of 326 million, the nation is home to 396 million cellular service accounts).

technology reveals that CSLI is merely one example out of the myriad forms of sensitive consumer data held by businesses. Internet of Things (IoT) or "smart" devices, defined as objects with networked sensors that can communicate amongst themselves, present unprecedented opportunities for mass data collection from everyday objects.[19] Although the Court's decision to protect CSLI from warrantless searches represents a positive first step for consumer privacy protection, aggregated consumer data generated through other personal technologies is equally deserving of Fourth Amendment protection.

A. *What is CSLI and How Does It Work?*

Cellular networks are supported by cell towers, which are arranged in a hexagonal pattern typically featuring three antennas that provide cell coverage to a circular area surrounding the tower.[20] When a cell phone connects to a tower, the consumer's telephone number and the product number of the consumer's cell phone are recorded along with the time; CSLI describes this set of data.[21] Although a traditional cell tower in an urban area provides coverage within a radius ranging from half a mile to two miles surrounding the tower, the precise antenna that provides the connection is recorded.[22] Thereby, the consumer's location is traceable to one specific wedge within the cell tower's coverage area.[23] Depending on the size of the cell tower's radius and the number of antennas, this places the user in an area ranging from one-eighth to four square miles.[24] Because smartphones rely on internet connections to power a host of applications, even when not in active use,[25] "[v]irtually any

---

[19] *See* Dalmacio V. Posadas, Jr., *After the Gold Rush: The Boom of the Internet of Things, and the Busts of Data-Security and Privacy*, 28 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 69, 75–78 (2017) (describing IoT devices, such as driverless cars, "smart" pill bottles, and wearable devices, while warning that these technologies gather and analyze vast quantities of consumer data, often with few security protections designed to thwart hackers).

[20] *See* Bloom & Clark, *supra* note 10, at 172.

[21] *See id.* at 172–73.

[22] *See Carpenter*, 138 S. Ct. at 2225 (Kennedy, J., dissenting).

[23] *Id.* at 2218 (majority opinion).

[24] *See id.*

[25] *Id.* at 2211–12.

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."[26]

The telecommunications company that owns the cell tower stores the CSLI data for up to five years,[27] and frequently sells aggregated CSLI data to third-parties as part of a market worth billions of dollars.[28] To illustrate this point, major cell service providers have contracts with data aggregators that can allow consumers to receive virtual coupons from nearby businesses or receive roadside assistance.[29] In addition to marketing ploys, these contracts allow data aggregators to market real-time CSLI tracking services to law enforcement agencies.[30]

The *Carpenter* case illustrates one of the problems with taking a haphazard approach to developing technologies: by the time a case reaches the Supreme Court, the underlying technology has been refined to the point of presenting different questions than the technology at issue in the case.[31] The CSLI data used to convict

---

[26] *Id.* at 2220.

[27] *See id.* at 2218.

[28] *See id.* at 2225 (Kennedy, J., dissenting) ("This data can be used, for example, to help a department store determine which of various prospective store locations is likely to get more foot traffic from middle-aged women who live in affluent zip codes.").

[29] *See* Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. TIMES (May 10, 2018), https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html?module=inline.

[30] *See id.* (describing Securus Technologies, a data broker that used a location aggregator stocked with CSLI records from AT&T, Sprint, T-Mobile, and Verizon to sell real-time tracking services to law enforcement); *see also* Jennifer Valentino-DeVries, *Largest Cell Phone Carriers to Limit Sales of Location Data*, N.Y. TIMES (June 19, 2018), https://www.nytimes.com/2018/06/19/technology/verizon-att-cellphone-tracking.html (describing promises by major cell service providers to reform CSLI marketing practices in response to public outcry regarding location aggregators).

[31] *See Carpenter*, 138 S. Ct. at 2219 ("While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision.").

Carpenter was generated in 2011,[32] and cell tower technology has developed significantly since then.[33] As the majority in *Carpenter* noted: "[w]hile the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision . . . wireless carriers have the capability to pinpoint a phone's location within 50 meters."[34] This increased precision is due primarily to the use of "small cell" technology, which refers to a variety of small-scale cell tower locations that supplement networks of traditional cell towers.[35] Small cells can be installed in homes with poor coverage, in public spaces that have high demand for coverage in a relatively compact area (such as stadiums), or on lampposts in densely-populated urban areas.[36]

Given the enthusiasm with which urban areas have been installing, or developing plans to install, small-cell technologies,[37] some estimates state that CSLI generated from a small-cell location could accurately record consumer location to within ten feet.[38] This ten-foot area is significantly more alarming than the one-eighth of a mile to four square mile area generated by traditional cell towers, and represents location-tracking capabilities that can match or surpass those of GPS devices.[39] This demonstrates the inherent problems with an unstructured approach to protecting data generated by new technology: without a predictable framework, the

---

[32] *See id.* at 2212.

[33] *See id.*

[34] *Id.*

[35] Bloom & Clark, *supra* note 10, at 174 ("Small cells are miniature base stations that provide a small range of cellular signal in areas that are either overburdened or underserved by traditional cell networks.").

[36] *Id.* at 174–75.

[37] *See* Allan Holmes, *5G Cell Service Is Coming. Who Decides Where It Goes?*, N.Y. TIMES (Mar. 2, 2018), https://www.nytimes.com/2018/03/02/technology/5g-cellular-service.html (describing plans to place small-cells 500 feet apart in urban areas in order to facilitate 5G network coverage).

[38] Bloom & Clark, *supra* note 10, at 176.

[39] *Id.* (explaining that although GPS technology can track location to within fifty feet, small-cell systems could lead to CSLI that is accurate to within ten feet or less).

technology at issue in the case becomes outdated, perhaps even obsolete, before the case reaches the Supreme Court.

B. *New Technologies Present New Challenges for Privacy Protection*

Although CSLI is an undoubtedly powerful type of data that deserves protection from warrantless search, it is merely one form of data generated on personal technology that presents challenges to traditional applications of the third-party doctrine. Indeed, given the ever-increasing capabilities of smartphones, CSLI may not even be the most sensitive data collected from cellular devices.[40] The host of "sensors, accelerometers, cameras, microphones, and other capabilities that can be used to collect and transmit various types of user information"[41] that come standard on modern smartphones means that CSLI is merely one of many types of sensitive data generated from smartphones.[42] Additionally, the capability of smartphones to connect with "smart" devices threatens to expose ever-increasing aspects of everyday life to collection by third-party businesses, and, thus, law enforcement.[43]

Internet of Things (IoT), or "smart" devices, can be broadly defined as objects with sensors that communicate amongst themselves via the internet.[44] These devices rely on embedded computer chips to generate data, which is then shared with other "smart" devices by using Wi-Fi, Bluetooth, cell phone networks, or other means of connection to access the internet.[45] By connecting to a plethora of everyday objects, IoT devices have the potential to create "an almost inescapable data web that monitors many aspects of one's life."[46] For example, smart utility meters can monitor water

---

[40] *See* Thierer, *supra* note 3, at 21.

[41] *Id.*

[42] *See id.*

[43] *See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. 805, 807 (2016) ("Today, with the advent of the 'Internet of Things,' objects in your house, car, office, and smartphone communicate, interact, report, track, and provide vast amounts of data about the activities of their owners.").

[44] *See* Posadas, *supra* note 19, at 75.

[45] *See id.* at 76–77.

[46] Ferguson, *supra* note 43, at 819.

or electricity usage by the hour and compare that usage with past trends.[47] One utility company reported receiving subpoenas from law enforcement for the smart meter data of 480 customers in 2017.[48] Smart refrigerators can track food consumption, reordering items as they are used, while smart mattresses can monitor sleep patterns.[49] Amazon has recently unveiled a line of everyday devices, including analog wall clocks and microwaves, that are responsive to voice commands through Alexa, the company's virtual voice assistant.[50] Additionally, the insurance company, John Hancock, has announced plans to encourage life-insurance policyholders to wear fitness tracking devices in exchange for policy discounts.[51]

The rapid expansion of connected IoT devices[52] highlights the importance of establishing a predictable framework for protecting data held by third-parties from warrantless search, as data generated by IoT devices could dwarf that generated by CSLI.[53] Rather than leaving lower courts without guidance regarding how to evaluate each individual IoT device, the Supreme Court should adopt a comprehensive interpretive stance that provides predictable protection for data generated by these technologies.

---

[47] *See* Zwerdling, *supra* note 1.

[48] *See id.*

[49] *See id.*

[50] *See* Bogost, *supra* note 3.

[51] *See id.*; *see also* Angela Chen, *What Happens When Life Insurance Companies Track Fitness Data?*, THE VERGE (Sept. 26, 2018, 1:01 PM), https://www.theverge.com/2018/9/26/17905390/john-hancock-life-insurance-fitness-tracker-wearables-science-health.

[52] *See* Thierer, *supra* note 3, at 12 (citing estimates that approximately 30 billion IoT devices will be in use by 2020); *see also* Peter Newman, *There Will be More Than 55 Billion IoT Devices by 2025 — These Are the Biggest Drivers for Adoption*, BUS. INSIDER (July 27, 2018), https://www.businessinsider.com/internet-of-things-report (estimating that 55 billion IoT devices will be in use by 2025, up from 9 billion in 2017).

[53] *See* Ferguson, *supra* note 43, at 820 ("Knowing that you called a certain number (cell data), drove to a certain house (drone or camera), and repeated that trip every week (GPS) pales in comparison to knowing those facts *plus* the time the bedroom light comes on in that house (through NEST systems), the elevated heartbeat in that bedroom (through health monitors), and the opening of a particular enchanted pill bottle (smart pill bottles)—all of which might provide a much better clue about the nature of your business at the house.").

III. BACKGROUND LAW: WHERE DATA PROTECTION HAS BEEN AND WHERE IT IS GOING

Justice Harlan's concurrence in *Katz v. United States*[54] established the "reasonable expectations of privacy" test for determining if law enforcement conducted a search that required a warrant under the Fourth Amendment.[55] However, the Supreme Court later revised this test to exclude business records from Fourth Amendment protection in *United States v. Miller*,[56] which established the third-party doctrine as a limitation on *Katz*.[57] *Smith v. Maryland*[58] then applied the third-party doctrine to data generated by pen registers, which record dialed telephone numbers.[59] More recently, a majority of Supreme Court Justices in *United States v. Jones*[60] recognized that individuals may have a "reasonable expectation of privacy" in their aggregated movements, but deferred answering this question.[61] In her *Jones* concurrence, meanwhile, Justice Sotomayor recommended granting Fourth Amendment protection to aggregated movements and questioned the continued appropriateness of the third-party doctrine.[62] The specific facts of each case provide clues both to the issues that concerned the Supreme Court in *Carpenter* and to the types of privacy issues that may concern the Court in the future. The Court's comparison of CSLI to outdated technology also demonstrates the flaws of a haphazard approach to determining the scope of Fourth Amendment protections: comparing recent technology to that in use forty or fifty years ago is an inherently confounding exercise.[63]

---

[54] Katz v. United States, 389 U.S. 347 (1967).
[55] *Id.* at 361 (Harlan, J., concurring).
[56] United States v. Miller, 425 U.S. 435 (1976).
[57] *Id.* at 442–43.
[58] Smith v. Maryland, 442 U.S. 735 (1979).
[59] *Id.* at 744–45.
[60] United States v. Jones, 565 U.S. 400 (2012).
[61] *Id.* at 412.
[62] *Id.* at 413–18 (Sotomayor, J., concurring).
[63] *See* Bellovin et al., *supra* note 4, at 54.

A. *Katz v. United States Establishes Expectations of Privacy Standard*

Although this Recent Development focuses on the third-party doctrine aspects of the *Carpenter* decision, *Katz* figured so prominently in the Court's opinion that some discussion is necessary. *Katz* recognized that the Fourth Amendment protects an individual's reasonable expectations of privacy and is not strictly property-based.[64] Hence, the *Carpenter* court had to determine first whether Carpenter had a reasonable expectation of privacy in his general movements,[65] and second, whether this expectation was precluded because Carpenter allowed a third-party business to collect and retain his location information.[66]

At issue in *Katz* was the FBI's warrantless attachment of a listening and recording device to the exterior of a phone booth used by the defendant to transfer illegal gambling information.[67] Because the device was attached to the exterior of the phone booth, the government argued no search had occurred under the Fourth Amendment.[68] This argument hinged on the traditional approach that considered physical intrusion necessary to trigger Fourth Amendment protection.[69] In rejecting this argument, the Court decoupled physical intrusion and searches requiring a warrant: "once it is recognized that the Fourth Amendment protects people – and not simply 'areas' – against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[70] Because "the Fourth Amendment protects people, not places,"[71] the Court looked to see whether Katz's expectations when using the phone booth rendered his conversation protected, and

---

[64] *See* Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (citing Katz v. United States, 389 U.S. 347, 351 (1967)).

[65] *See id.* at 2215 (citation omitted).

[66] *See id.* at 2216 (citing Smith v. United States, 442 U.S. 735, 743–44 (1979); Miller v. United States, 425 U.S. 435, 443 (1976)).

[67] *Katz*, 389 U.S. at 348.

[68] *Id.* at 352–53.

[69] *Id.*

[70] *Id.* at 353.

[71] *Id.* at 351.

concluded that he acted within the scope of Fourth Amendment protection.[72] Justice Harlan's concurrence reasoned that to establish Fourth Amendment protection under this new "people, not places" inquiry, the defendant must have a subjective expectation of privacy and "the expectation [must] be one that society is prepared to recognize as 'reasonable.'"[73] Justice Harlan's formulation was quickly adopted as the test for determining the scope of Fourth Amendment protection post-*Katz*, and remains so today.[74] However, scholars have criticized *Katz* for beginning an interpretive regime that lacks clarity and encourages idiosyncratic judicial interpretations.[75] The third-party doctrine represents a flaw in the *Katz* interpretive system, serving as a somewhat arbitrary limitation on what an individual's "reasonable expectations of privacy" may be.[76]

B. *United States v. Miller Establishes the Third-Party Doctrine*

The third-party doctrine, which allows law enforcement to access business records without a warrant, was established in *Miller*.[77] During an investigation of Miller's illegal distillery, law enforcement subpoenaed Miller's financial records from two banks.[78] Investigators viewed microfilm copies of Miller's account and received copies of a deposit slip and checks from one bank, and

---

[72] *Id.* at 352 ("No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it . . . is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.") (footnotes omitted).

[73] *Id.* at 361 (Harlan, J., concurring).

[74] Luke M. Milligan, *The Real Rules of "Search" Interpretations*, 21 WM. & MARY BILL RTS. J. 1, 18 (2012).

[75] *See id.* at 23–28 (describing scholarly criticism of the *Katz* approach).

[76] *See* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1403 (2004) ("The conclusion that *Miller*, *Smith*, and like cases foreclose any claim of an expectation of privacy in communications held by a service provider fails to acknowledge . . . the doctrinal and normative underpinnings of those decisions. A broad reading of *Miller* and *Smith* is also fundamentally inconsistent with *Katz*.").

[77] Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) ("This third-party doctrine largely traces its roots to *Miller*.").

[78] United States v. Miller, 425 U.S. 435, 437 (1976).

viewed microfilm copies and received copies of checks, deposit slips, financial statements, and monthly statements from the second bank.[79] Evaluating Miller's claim that accessing the documents constituted an unreasonable search, the Court held that the banking records were neither his "private papers,"[80] nor were they protected under *Katz*.[81]

In declining to extend *Katz* to protect Miller's banking records, the Supreme Court cited the *Katz*'s assertion that public information falls outside the scope of Fourth Amendment protection.[82] The Court appeared likely to take a subjective approach when it explained that "[w]e must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."[83] The Court then reasoned that when Miller voluntarily disclosed the information contained in his bank records to a business, he assumed the risk that the business would disclose this information to the government.[84]

After finding no reasonable expectation of privacy regarding Miller's banking records, the Court's opinion denied protection for business records generally, stating:

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, 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.[85]

This unnecessarily restrictive approach to *Katz* fails to recognize both the varying degrees of sensitive information contained in business records and the varying degrees of trust a consumer may

---

[79] *Id.* at 438.

[80] *Id.* at 440–41 (finding that defendant did not have a property interest in the records because they belonged to, and were controlled by, the banks).

[81] *Id.* at 442–43.

[82] *Id.* at 442 ("But in *Katz* the Court also stressed that '[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.'") (citing Katz v. United States, 389 U.S. 347, 351 (1967)).

[83] *Id.* (citing Couch v. United States, 409 U.S. 322, 335 (1973)).

[84] *Id.* at 442–43.

[85] *Id.* at 443 (citations omitted).

have in different businesses.[86] Accordingly, the third-party doctrine as established in *Miller* serves as a categorical limitation on *Katz*, as individuals are considered to lack any reasonable expectation of privacy in business records held by third parties, even when those records contain sensitive personal data.[87]

C. *Smith v. Maryland Affirms the Third-Party Doctrine*

Smith involved a pen register, installed by a telephone company at the request of the police, to monitor outgoing calls from the defendant's telephone.[88] A pen register is a device that collects and stores the telephone numbers a customer dials, and operates from equipment located at the telephone company's offices.[89] A pen register therefore does not represent a property-based intrusion, and does not acquire the content of the telephone conversation that occurs after it records the dialed telephone number.[90] By recording the telephone numbers of Smith's outgoing calls, the pen register showed that Smith, who was suspected of stalking, had dialed the victim's number from his home telephone.[91]

The Court used the two-part test from *Katz* to evaluate Smith's claim that the pen register constituted a search requiring a warrant.[92] The Court first explained that Smith lacked any reasonable expectation of privacy in the phone numbers he dialed, since the fact that phone companies collect and store this information was

---

[86] *See* Bellia, *supra* note 76, at 1402 ("Read broadly, *Miller* suggests that the mere fact that documents are conveyed to a third party, without regard to the type of documents at issue or the purpose for which the documents were provided, eliminates any expectation of privacy.").

[87] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528–29 (2006) (citing *Miller* and *Smith* as the leading third-party doctrine cases while noting that the third-party doctrine excludes significant amounts of information from Fourth Amendment protection in the digital age).

[88] Smith v. Maryland, 442 U.S. 735, 737 (1979).

[89] *Id.* at 741.

[90] *Id.* ("Yet a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."); *see also* Bellovin et al., *supra* note 4, at 54 (explaining the protected content versus unprotected non-content distinction while arguing that this distinction is rendered irrelevant by modern technology).

[91] *Smith*, 442 U.S. at 737.

[92] *Id.* at 740–41.

considered common knowledge.[93] In reaching this conclusion, the Court attributed to all telephone users the knowledge that dialed telephone numbers are sent through the telephone company's equipment and recorded for billing purposes.[94] After making this somewhat unconvincing analysis, the Court argued that "[a]lthough most people may be oblivious to a pen register's esoteric functions, they presumably have some awareness of one common use: to aid in the identification of persons making annoying or obscene calls."[95] Thus, the Court's assertion that any consumer knows telephone companies receive and store dialed telephone numbers served to prevent a reasonable expectation of privacy from forming, despite the fact that Smith made the calls from his home telephone.[96]

Second, the Court reasoned that even if Smith had a subjective expectation that the numbers he dialed would remain private, this expectation was not "one that society is prepared to recognize as 'reasonable,'"[97] because "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[98] Under the Court's logic, voluntary activities that expose user information to third-party businesses create an assumed risk that this information will be passed along to law enforcement.[99] *Smith*, then, solidified *Miller's* assertion that *Katz* does not extend its protections to third-party business records as a class.

D. *United States v. Jones Questions the Third-Party Doctrine*

The third-party doctrine as described in the 1970s by *Miller* and *Smith* has received scholarly criticism due to the explosion of personal technology, as the volume and content of data generated by

---

[93] *See id.* at 742–43.

[94] *See id.* at 742.

[95] *Id.* (citations omitted).

[96] *Id.* at 743 ("The fact that [Smith] dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think it would.").

[97] *Id.* (citing Katz v. United States, 389 U.S. 347, 361 (1967)).

[98] *Id.* at 743–44 (citations omitted).

[99] *See id.* at 744–45.

users and held by businesses has expanded exponentially.[100] *United States v. Jones* served as the precursor to *Carpenter's* limitation of the third-party doctrine both by leaving open the possibility of a right to privacy in one's general movements,[101] and by Justice Sotomayor's concurring opinion, which questioned the continued applicability of the third-party doctrine in the digital age.[102]

At issue in *Jones* was law enforcement's attachment of a GPS tracker to a vehicle used by Jones and registered to his wife.[103] Although law enforcement obtained a warrant to place the device on the vehicle, it was installed after the warrant expired and outside of the jurisdiction where the warrant was issued.[104] The GPS showed the location of Jones' vehicle from within 50 to 100 feet, and relayed more than 2,000 pages of data over a one-month period.[105] The majority concluded that law enforcement had violated Jones' Fourth Amendment protections by committing a physical trespass on his vehicle.[106] In doing so, the majority relied on the older, property-based standard of Fourth Amendment protection.[107] However, the majority noted the possibility that "achieving the same result through electronic means, without an accompanying trespass, is an

---

[100] *See* Bellovin et al., *supra* note 4, at 54.

[101] *See* United States v. Jones, 565 U.S. 400, 412 (2012) ("It may be that achieving the same result [surveilling Jones for four weeks] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.").

[102] *Id.* at 417 (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal about themselves to third parties in the course of carrying out mundane tasks.") (citations omitted).

[103] *See id.* at 402–03 (majority opinion).

[104] *See id.*

[105] *Id.* at 403.

[106] *Id.* at 404 ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information."); *see also id.* at 410 ("By attaching the device to the Jeep, officers encroached on a protected area.").

[107] *See* Milligan, *supra* note 74, at 23 (explaining that *Jones* expanded the importance of property in determining whether a Fourth Amendment violation occurred by making property intrusions a "sufficient condition" for a search).

unconstitutional invasion of privacy,"[108] but deferred answering that question.[109]

Justice Sotomayor's concurrence provided a more feasible framework for protecting information generated by personal devices that does not hinge on physical intrusion while also calling into question the continued use of the third-party doctrine.[110] Justice Sotomayor began by noting that "[t]he Government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection."[111] Although the appropriation of Jones' property was conducted through physically attaching a GPS device, Justice Sotomayor explained that focusing on physical intrusion is increasingly irrelevant due to tracking capabilities embedded in consumer devices.[112]

Justice Sotomayor then noted the uniquely sensitive information that precise GPS monitoring may reveal, as GPS data creates a "comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[113] The cost efficiency and potential secrecy of GPS monitoring are additional causes for concern,[114] as is the chilling effect such surveillance may have, since "[a]wareness that the Government may be watching chills associational and expressive freedoms."[115] The concerns arising from GPS surveillance led Justice Sotomayor to argue that there exists a "reasonable societal expectation of privacy in the sum of

---

[108] *Jones*, 565 U.S. at 412.

[109] *Id.*

[110] *Id.* at 413–18 (Sotomayor, J., concurring).

[111] *Id.* at 413–14 (citing Silverman v. United States, 365 U.S. 505, 511–12 (1961)).

[112] *Id.* at 415 ("With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones.") (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc)).

[113] *Id.* (citation omitted).

[114] *See id.* at 415–16 (citation omitted).

[115] *See id.* at 416.

one's public movements."[116] Justice Sotomayor's concurrence, therefore, emphasized that the government should not be permitted to easily collect aggregated data that reveals sensitive personal characteristics and beliefs.[117]

Justice Sotomayor's concurrence concluded by questioning the continued relevance of the third-party doctrine in the digital age, given the broad scope of information individuals reveal to third parties "in the course of carrying out mundane tasks."[118] The information these "mundane tasks" place at risk of disclosure includes telephone numbers, websites, e-mail addresses, and items purchased online.[119] Justice Sotomayor also noted that societal expectations "can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed . . . is, for that reason alone, disentitled to Fourth Amendment protection."[120] Thus, under Justice Sotomayor's framework, the government may not coopt personal technology to replace traditional surveillance methods simply because third-parties have access to this sensitive, aggregated information.

IV. *CARPENTER* OPINION

Based on the sensitivity of aggregated location data that CSLI discloses,[121] and the inability to disable the collection of CSLI when using a cell phone,[122] the *Carpenter* majority held that law enforcement conducted a Fourth Amendment search requiring a warrant when officers accessed CSLI data revealing Carpenter's historic location information.[123] Although the majority's decision to not extend the third-party doctrine represents a major step forward for data privacy, the majority is unclear about the scope of the third-

---

[116] *Id.*
[117] *See id.*
[118] *Id.* at 417.
[119] *Id.*
[120] *Id.* at 418 (citing Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting)).
[121] Carpenter v. United States, 138 S. Ct. 2206, 2214–15 (2018).
[122] *See id.* at 2223.
[123] *Id.* at 2212, 2220.

party doctrine after *Carpenter* and provides little guidance about how to approach new technology in the future.[124]

A. *The Majority Opinion Has Potential for Predictable Protections, but Risks a Haphazard Approach*

In 2011, law enforcement officers accessed CSLI records from Carpenter's mobile carriers after obtaining court orders under the Stored Communications Act,[125] which allows law enforcement to access telecommunications records by showing "'reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.'"[126] This is a lower standard than that required to obtain a warrant, which requires "probable cause."[127] Consequently, although law enforcement was required to obtain a court's approval to access Carpenter's CSLI, the statutory standard of proof was easier to meet than that required to obtain a search warrant under the Fourth Amendment.[128] Officers obtained 129 days' worth of CSLI from Carpenter's two mobile carriers, totaling 12,898 location points.[129] This information was used at trial to place Carpenter near four of the robberies for which he was charged and convicted.[130] The CSLI was mentioned in the prosecutor's closing argument, and Carpenter received a prison sentence of over one hundred years.[131]

In holding that law enforcement improperly used CSLI to convict Carpenter,[132] the majority opinion relied on two separate, but related, lines of cases. In the first line of cases, the Court discussed the notion that individuals have a reasonable expectation of privacy

---

[124] *See id.* at 2234 (Kennedy, J., dissenting) ("[T]he Court fails 'to provide clear guidance to law enforcement' and courts on key issues raised by its reinterpretation of *Miller* and *Smith*.") (citing Riley v. California, 134 S. Ct. 2473, 2491 (2014))).

[125] 18 U.S.C. § 2703(d) (2018).

[126] *Carpenter*, 138 S. Ct. at 2212 (quoting 18 U.S.C. § 2703(d) (2018)).

[127] *See id.*

[128] *See id.*

[129] *See id.* at 2212–13.

[130] *See id.*

[131] *See id.* at 2213.

[132] *Id.* at 2220 ("The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.").

in their locations, relying largely on Justice Sotomayor's and Justice Alito's concurrences from *Jones*.[133] For the second line of cases, the Court considered whether the third-party doctrine precluded Carpenter's reasonable expectation of privacy in his aggregated location information, since this data was readily available to Carpenter's wireless carriers.[134] For both issues, the Court concluded that, "[w]hether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[135] Although the majority exempted CSLI from the third-party doctrine,[136] representing a significant step forward for consumer privacy rights, the opinion is unclear about how, or whether, to extend Fourth Amendment protection to other technologies that reveal detailed personal information.

A thorough analysis of the language the majority used to describe CSLI provides some clues as to the source of the perceived differences between CSLI and other types of third-party business records, such as those at issue in *Miller* and *Smith*. The majority described CSLI as: "detailed, encyclopedic, and effortlessly compiled";[137] a "qualitatively different category"[138] than bank records and telephone numbers;[139] "conveying . . . a detailed and comprehensive record of the person's movements";[140] "remarkably easy, cheap, and efficient compared to traditional investigative tools";[141] a form of "tireless and absolute surveillance";[142] "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years";[143] "not truly 'shared' as one normally

---

[133] *See id.* at 2215.
[134] *See id.* at 2216.
[135] *Id.* at 2217.
[136] *See id.* ("We decline to extend *Smith* and *Miller* to cover these novel circumstances.").
[137] *Id.* at 2216.
[138] *Id.*
[139] *Id.*
[140] *Id.* at 2217.
[141] *Id.* at 2218.
[142] *Id.*
[143] *Id.* at 2220.

understands the term";[144] and "an entirely different species of business record"[145] before concluding that "the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection"[146] render CSLI outside the scope of the third-party doctrine.[147] Although the Court used this collection of epithets to describe CSLI, it is unclear whether a different technology must meet all of these descriptions in order to be protected. Is this a list of necessary conditions that must be met before data from a different technology receives Fourth Amendment protection? Or is some minimum amount of these attributes sufficient to grant protection to non-CSLI data? By not answering these questions, the Court risks implementing a scattered approach to extending Fourth Amendment protections to new technologies.

The majority appeared to use a balancing test (without calling it such)[148] to determine that, because individuals have a reasonable expectation of privacy regarding their historical location information, and because CSLI collects this information automatically from a ubiquitous device, CSLI is therefore protected from warrantless search.[149] The majority then declined to consider any broader application than historical CSLI, leaving unclear how, or whether, to apply this logic to future technologies.[150] Rather, the

---

[144] *Id.*

[145] *Id.* at 2222.

[146] *Id.* at 2223.

[147] *See id.*

[148] *Id.* at 2231–32 (Kennedy, J., dissenting) ("The Court appears, in my respectful view, to read *Miller* and *Smith* to establish a balancing test. For each 'qualitatively different category' of information, the Court suggests, the privacy interests at stake must be weighed against the fact that the information has been disclosed to a third party.") (citing majority opinion at 2216, 2219–20).

[149] *See id.* at 2220 (majority opinion) (explaining that CSLI is not voluntarily disclosed, in part due to the necessity of cell phones to modern life and the inability to disable CSLI collection).

[150] *Id.* ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security

Court restricted its holding to historical CSLI gathered over more than six days.[151] The Court did leave a small aperture to potentially allow for future expansion of its holding by briefly stating, "[w]e hold only that a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party,"[152] but did not explain how to evaluate whether such a situation has occurred. By declining to address future applications of its holding, the Court risks implementing a haphazard approach to protecting new technologies that will draw arbitrary distinctions between types of data based on idiosyncratic analogies. Without a clear directive on the status of the third-party doctrine after *Carpenter*, "the Court fails 'to provide clear guidance to law enforcement' and courts on key issues raised by its reinterpretation of *Miller* and *Smith*."[153]

B. *Justice Kennedy's Dissent Presents the Risks and Inconsistencies in the Majority's Approach*

Justice Kennedy's dissent provided a defense of the third-party doctrine[154] and highlighted the risks and uncertainties of the majority's approach.[155] Justice Kennedy argued that "*Miller* and *Smith* set forth an important and necessary limitation on the *Katz* framework. They rest upon the commonsense principle that the absence of property law analogues can be dispositive of privacy expectations."[156] In Justice Kennedy's view, consumers have no property interest in business records and, therefore, lack any reasonable expectation of privacy under *Katz*.[157] In justifying the

---

cameras. Nor do we address other business records that might incidentally reveal location information.").

[151] *See id.* at 2224 (Kennedy, J., dissenting) ("According to today's majority opinion, the Government 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. But, in the Court's view, the Government crosses a constitutional line when it obtains a court's approval to issue a subpoena for more than six days of cell-site records . . . .").

[152] *Id.* at 2222 (majority opinion).

[153] *Id.* at 2234 (Kennedy, J., dissenting) (citing Riley v. California, 134 S. Ct. 2473, 2491 (2014)).

[154] *See id.* at 2226–28.

[155] *See id.* at 2234.

[156] *Id.* at 2228.

[157] *See id.*

third-party doctrine, Justice Kennedy focused on the lack of consumer control over CSLI once it is collected by the service provider and attributed knowledge of the commercial value and use of this data to consumers.[158] Similarly to the majority opinions in *Miller* and *Smith*, this approach makes questionable assumptions about the extent of consumer knowledge regarding data collection[159] and refuses to recognize the varied expectations a consumer may have when interacting with different businesses.[160] Justice Kennedy also argued that compelled disclosure of business records serves as a useful and legitimate resource for law enforcement while affording adequate protections to businesses, which release the data without physical government intrusion and may object to this compelled disclosure.[161]

After defending the third-party doctrine, Justice Kennedy discussed the flaws inherent in the Court's new, third-party balancing test: "[f]or each 'qualitatively different category' of information, the Court suggests, the privacy interests at stake must be weighed against the fact that the information has been disclosed to a third party . . . That is an untenable reading of *Miller* and *Smith*."[162] In Justice Kennedy's view, this approach arbitrarily

---

[158] *See id.* at 2230 ("Because Carpenter lacks a requisite connection to the cell-site records, he also may not claim a reasonable expectation of privacy in them. He could expect that a third party—the cell service provider—could use the information it collected, stored, and classified as its own for a variety of business and commercial purposes.").

[159] *See* Bellovin et al., *supra* note 4, at 54 (discussing the difficulty of knowing what information a consumer may disclose by using technology in the digital age).

[160] *See* Bellia, *supra* note 76, at 1403 ("There are at least four differences that are relevant to an assessment of an expectation of privacy: (1) the type of *information* at issue; (2) the *individual's purpose* in placing information in the hands of the third party; (3) the *relevance of the substance* of the information to the third party's activities; and (4) the limitations on the third party's *ability to gain access to or use the substance* of the information.").

[161] *See Carpenter*, 138 S. Ct. at 2228–29 (Kennedy, J., dissenting); *see also* Alan Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 112–122 (2018) (arguing that technology companies may serve as "surveillance intermediaries" by resisting governmental efforts to access the consumer data they hold).

[162] *Carpenter*, 138 S. Ct. at 2231–32 (Kennedy, J., dissenting) (citing majority opinion at 2216, 2219–20).

exempts CSLI from the third-party doctrine without convincingly distinguishing it from other sensitive types of data that remain subject to warrantless collection.[163] Additionally, Justice Kennedy critiqued the majority for considering the increasingly-precise nature of CSLI in reaching its holding, arguing that "judicial caution, prudent in most cases, is imperative in this one,"[164] before calling for deference to the statutory scheme in place.[165] However, Justice Kennedy's argument in favor of judicial caution and deference to legislative solutions largely ignored the historical cooperation between the Court and Congress in extending Fourth Amendment protections to new technologies.[166] Indeed, it was the Supreme Court that first protected the content of telephone calls in *Katz*, with Congress later passing legislation to codify this protection.[167] The Court has historically possessed an important role in applying the Fourth Amendment to emerging technologies and should continue to do so, especially when the combined jurisprudential and statutory approach becomes impracticable.[168]

Finally, Justice Kennedy provided a list of the challenges the majority's opinion poses for lower courts: the holding states that

---

[163] *Id.* at 2232–33 (Kennedy, J., dissenting).

[164] *Id.* at 2233.

[165] *See id.*

[166] *See* Bellovin et al., *supra* note 4, at 12–19 (describing the interaction between case law and statutory solutions in interpreting the Fourth Amendment); *see also* Bloom and Clark, *supra* note 10, at 182 ("In fact, Congress and the Court have often worked hand-in-hand to bring privacy protections to evolving technologies.").

[167] *See* Bellovin et al., *supra* note 4, at 12–13; *see also* Bloom and Clark, *supra* note 10, at 182 ("[A]fter the Court brought audio surveillance within the purview of the Fourth Amendment in *Katz*, Congress passed the Wiretap Act, which sought to regulate the government access to the contents of traditional phone calls. The Act provided for comprehensive and detailed regulations and procedures for wiretap orders.").

[168] *See* Bellovin et al., *supra* note 4, at 54 (describing the difficulties in applying the third-party doctrine to modern technology); *see also* Bloom and Clark, *supra* note 10, at 168 ("The late Justice Scalia in his 2001 majority opinion in *Kyllo v.* [*United States*], a case involving thermal imaging, opined that 'while the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.'") (citing Kyllo v. United States, 533 U.S. 27, 36 (2001)).

CSLI is categorically different but "does not explain what makes something a distinct category of information";[169] the holding "gives courts and law enforcement officers no indication [of] how to determine whether any particular category of information falls on the financial-records side or the cell-site-records side of its newly conceived constitutional line";[170] even after information is placed on the CSLI side, "courts and law enforcement officers will have to guess how much of that information can be requested before a warrant is required";[171] and finally, the holding undermines widely-used subpoena practices.[172] Justice Kennedy argued that this amalgamation of uncertainties "will inhibit law enforcement and 'keep defendants and judges guessing for years to come.'"[173] Although returning to a strict application of the third-party doctrine represents a worse alternative than the majority's uncertain approach, Justice Kennedy's commentary speaks to the need for a more predictable guide to applying the *Carpenter* majority's holding.

V. APPLYING *CARPENTER* IN FUTURE CASES: PROBLEMS AND SOLUTIONS

When evaluating other types of data generated on personal technology and held by third-party businesses, courts should read *Carpenter* alongside Justice Sotomayor's *Jones* concurrence to provide a predictable system that protects sensitive consumer data from warrantless searches. Justice Sotomayor's *Jones* concurrence argued that, regardless of physical intrusion, the government should not coopt personal property and turn it into a means of warrantless surveillance.[174] Although the technology at issue in *Jones* was GPS

---

[169] *Carpenter*, 138 S. Ct. at 2234.

[170] *Id.*

[171] *Id.*

[172] *Id.*

[173] *Id.* at 2234–35 (quoting Riley v. California, 134 S. Ct. 2473, 2493 (2014)).

[174] *See* United States v. Jones, 565 U.S. 400, 414–15 (2012) (Sotomayor, J., concurring) ("[P]hysical intrusion is now unnecessary to many forms of surveillance. With increasing regularity, the government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones.") (citation omitted).

tracking, this logic is applicable to other forms of sensitive data. Moreover, evaluating Fourth Amendment protections for the data generated by newer technologies, such as IoT devices, is much simpler, and more predictable, when reading *Carpenter* in conjunction with Justice Sotomayor's *Jones* concurrence than when reading *Carpenter* alone.

A. *Courts Should Read Carpenter in Conjunction with Justice Sotomayor's Jones Concurrence*

By highlighting the flaws of a haphazard approach,[175] Justice Kennedy's dissent pointed to the need for a predictable, stable standard. Although Justice Kennedy would retain the third-party doctrine,[176] Justice Sotomayor's *Jones* concurrence provided a predictable framework that would give consumers more protection in the digital age without necessitating a return to the unnecessarily constraining third-party doctrine.[177] Reading Justice Sotomayor's *Jones* concurrence in conjunction with the *Carpenter* majority's holding provides a solution for avoiding the pitfalls Justice Kennedy highlighted in his *Carpenter* dissent. To avoid a patchwork approach to third-party data that depends on obscure "category-by-category balancing,"[178] or a return to the strict third-party regime of *Miller* and *Smith*,[179] courts should adopt an interpretive stance that recognizes consumers have a reasonable expectation that the government will not coopt personal technology in order to conduct warrantless surveillance.

---

[175] *See Carpenter*, 138 S. Ct. at 2234 (Kennedy, J., dissenting).

[176] *See id.* at 2226–28 (providing a defense of the third-party doctrine).

[177] *Jones*, 565 U.S. at 413–18 (2012) (Sotomayor, J., concurring).

[178] *Carpenter*, 138 S. Ct. at 2232 (Kennedy, J., dissenting); *see also* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1528 (2010) ("We should . . . start focusing on the hard practical issue of how best to regulate government information gathering. The Fourth Amendment should cover government information gathering comprehensively rather than haphazardly.").

[179] *See* Solove, *supra* note 178, at 1532 ("It is increasingly the case that much of what we do, buy, and read generates records maintained by third parties. Regulation and oversight should not turn on the happenstance of where such records are located, and changing technology that increasingly locates them outside people's homes should not suddenly cause them to drop out of the regulatory regime.").

"Personal technology" is an intentionally open-ended category that includes familiar devices such as smart phones and laptops, emerging technologies such as IoT devices, and the data-generating programs that power these devices.[180] In a world where consumer devices interact with one another in complex ways to share and aggregate data on their users,[181] protecting one specific form of data generated from one specific device does little to counter the rising tide of surveillance.[182] Rather than create an exhaustive list of protected devices or forms of data, which would quickly become outdated,[183] this approach is intended to provide a flexible guiding principle against warrantless surveillance through consumer devices that will remain relevant as technology advances. Given the rapid pace at which new technologies are introduced and integrated into

[180] *See* Andrew W. Bagley & Justin S. Brown, *Limited Consumer Privacy Protections Against the Layers of Big Data*, 31 SANTA CLARA COMPUTER & HIGH TECH. L.J. 483, 490–95 (2014) (describing the "layers" of data regarding consumer behavior that accumulate from programs, such as web browsers and applications, contained on personal electronic devices, and the manner in which IoT devices add an additional layer to this system by extending internet connectivity to physical objects).

[181] *See id.* at 491–92 ("The increasing number of software applications collecting data in Web 2.0 and social media is now augmented by physical devices as part of the budding 'Internet of Things.' The layers of the broadband ecosystem are expanding as users interact with the Internet in more ways than accessing static websites and communicating over instant messaging. For example, retailers now use Wi-Fi beacons to track shoppers in the physical world, and consumers use their mobile devices to pay for real world goods. Information from such interactions can be combined with other data from Web usage to create all-encompassing marketing profiles of specific consumers.").

[182] *See id.* at 493 ("It should be noted that users may still transmit enough data to paint a comprehensive picture of their lives regardless of whether they are part of a singular company's digital ecosystem or opt to use the hardware, software, and connectivity platforms of wholly different entities.").

[183] *See* Ferguson, *supra* note 43, at 823 ("The drive for innovation, consumer efficiency, and self-awareness has turned ordinary activity into valuable data. Because of this valuable data, more and more 'things' are being created to collect that information. The proliferation of smart objects brings with it the proliferation of surveillance capabilities, a reality that statutory or constitutional law will soon need to address.").

daily life,[184] an unpredictable "category-by-category balancing"[185] approach risks isolating Fourth Amendment protection to aging technologies, while newer technologies that present greater risks of surveillance remain unprotected.[186]

Justice Sotomayor outlined an approach that recognized the risk of surveillance through personal technology, stating that "[t]he Government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection."[187] Because *Katz* recognized that "the reach of the Fourth Amendment does not 'turn upon the presence or absence of a physical intrusion,'"[188] formulating the question in terms of coopting personal technology into a means of surveillance avoids both the traditional physical trespass approach from *Jones*[189] and the contorted balancing test from *Carpenter*.[190] Justice Sotomayor recommended that, rather than strictly adhering to the third-party doctrine,[191] courts should "ask whether people reasonably expect

---

[184] *See id.* at 817–18 (describing the increased use and availability of IoT devices).

[185] *See* Carpenter v. United States, 138 S. Ct. 2206, 2232 (2018) (Kennedy, J., dissenting); *see also* Solove, *supra* note 178, at 1528 ("We should . . . start focusing on the hard practical issue of how best to regulate government information gathering. The Fourth Amendment should cover government information gathering comprehensively rather than haphazardly.").

[186] *See* Bloom and Clark, *supra* note 10, at 168 ("The late Justice Scalia in his 2001 majority opinion in *Kyllo v.* [*United States*], a case involving thermal imaging, opined that 'while the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.'") (citing Kyllo v. United States, 533 U.S. 27, 36 (2001)).

[187] United States v. Jones, 565 U.S. 400, 413–14 (2012) (Sotomayor, J., concurring) (citing Silverman v. United States, 365 U.S. 505, 511–12 (1961)).

[188] *Id.* at 414 (citing Katz v. United States, 389 U.S. 347, 353 (1967)).

[189] *Id*. at 404, 410 (majority opinion).

[190] *See Carpenter*, 138 S. Ct. at 2231–32 (2018) (Kennedy, J., dissenting) (citing majority opinion at 2216, 2219–20).

[191] *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information

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."[192] Because this question focuses on the "attributes"[193] of government surveillance (data aggregation from connected items in personal use),[194] and the sensitive information such surveillance may disclose,[195] formulating the question in this manner provides a more predictable and comprehensive means of evaluating other types of data held by third parties. This approach lends itself well to a predictable expansion of individual privacy protection.

Protecting data generated on personal devices from being coopted into a means of government surveillance would be one way to enact scholarly recommendations that "the Fourth Amendment should provide protection whenever a problem of reasonable significance can be identified with a particular form of government information gathering."[196] Law enforcement's ability to access the vast amounts of data held by third-party businesses without a warrant presents "a problem of reasonable significance"[197] that courts now have the opportunity to resolve by reading *Carpenter* alongside Justice Sotomayor's *Jones* concurrence. Protecting personal technology from being coopted and turned into a means of warrantless surveillance provides a broad, stable base for protecting consumer privacy under the Fourth Amendment in a world where "physical intrusion is now unnecessary to many forms of

about themselves in the course of carrying out mundane tasks.") (citations omitted).

[192] *Id.* at 416.

[193] *Id.* ("I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements.").

[194] *See id.* ("I do not regard as dispositive the fact that the government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques.") (citing Kyllo v. United States, 535 U.S. 27, 35, n.2 (2001)).

[195] *See generally* Michael Gentithes, *The End of Miller's Time: How Sensitivity Can Categorize Third-Party Data After Carpenter*, 5 GA. L. REV. (forthcoming 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3155644 (recommending that courts focus on the sensitivity of gathered data in determining whether a search has occurred).

[196] Solove, *supra* note 178, at 1514.

[197] *Id.*

surveillance."[198] This standard should be applied both to the real-time gathering of information at issue in *Jones* and the historical data accessed in *Carpenter*.

As Justice Sotomayor noted, the government's ability to conduct large-scale surveillance through personal technology has high costs for society: "[a]wareness that the government may be watching chills associational and expressive freedoms. And the government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[199] Location data is not unique in raising these concerns,[200] as the *Carpenter* majority suggested.[201] Rather, most activities on personal technology raise these concerns, as third parties have access to uniquely sensitive data in enormous quantities from a variety of uses.[202] Consumers should not lose Fourth Amendment protections for this aggregated data merely because it is held by a business.[203] By focusing on the means of collecting data and protecting consumers from warrantless government surveillance through their own personal technology, courts would avoid the logical contortions inherent in the *Carpenter* majority's unstructured approach. This interpretive stance would also assist in returning Fourth Amendment jurisprudence to the comprehensive standard originally envisaged by *Katz*.[204]

---

[198] *Jones*, 565 U.S. at 414 (Sotomayor, J., concurring) (citing Alito, J., concurring, 424–29).

[199] *Id.* at 416 (Sotomayor, J., concurring).

[200] *See* Carpenter v. United States, 138 S. Ct. 2206, 2232 (2018) (Kennedy, J., dissenting) (discussing the variety of business records that could match the majority's description of why CSLI is unique and deserves protection).

[201] *See id.* at 2223 (majority opinion).

[202] *See* Bagley & Brown, *supra* note 180, at 490–95.

[203] *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (listing the various ways consumers disclose sensitive information in large amounts to third-party businesses and arguing that consumers would object to warrantless government access to this data).

[204] *See* Milligan, *supra* note 74, at 23 ("This reliance on property law, along with the Court's ratification of old rules and its drift away from public expectations of privacy, make clear that *Katz* failed in its promise to reorient 'search' doctrine along the lines of an objective and evolving privacy standard.").

B. *Future Applications*

Considering the plethora of sensitive personal data that is increasingly generated by personal technology and held by businesses demonstrates the advantages of reading *Carpenter* alongside Justice Sotomayor's *Jones* concurrence. This interpretive stance provides more predictable protections for consumer data than reading *Carpenter* alone. The hypothetical example in this section discusses the protection of data generated from IoT devices, but could also apply to less novel forms of data, such as that generated on smartphone applications or laptops. Although IoT devices offer consumers unparalleled conveniences, such as the ability to reorder grocery items as they are depleted,[205] they also present unparalleled disclosure of formerly private data to third-party businesses.[206]

A hypothetical application of *Carpenter* when read alongside Justice Sotomayor's *Jones* concurrence demonstrates the effectiveness of an interpretive stance that looks at the means of data acquisition and the sensitive personal information surveillance may disclose.[207] By preventing law enforcement from usurping data generated from personal technology to conduct warrantless surveillance, this standard protects data generated on IoT devices from warrantless search. Consider a hypothetical investigation of an individual who regularly uses an Alexa speaker device and an Alexa-compatible smart microwave located in her home.[208] Every evening at 10:35, she instructs Alexa to play her favorite radio station, while instructing the microwave to heat a cup of tea. Both devices record their respective vocal commands, translate them into action, and send the data to Amazon servers for storage.[209] Over time, this data becomes a comprehensive record of this hypothetical consumer's evening routine, which is stored and maintained by Amazon.[210] If law enforcement later suspects this consumer of

---

[205] *See* Zwerdling, *supra* note 1.

[206] *See* Ferguson, *supra* note 43, at 807–08.

[207] *See Jones*, 565 U.S. at 416–17 (Sotomayor, J., concurring) (discussing data collection and aggregation while questioning the third-party doctrine); *see also* Solove, *supra* note 178, at 1514.

[208] *See* Bogost, *supra* note 3 (discussing the use of Alexa-compatible devices).

[209] *See id.*

[210] *See* Zwerdling, *supra* note 1.

committing a crime during the time she typically instructs her Alexa speaker to play music and her smart microwave to heat a cup of tea, the data held by Amazon would reveal whether or not she was using these devices on the night in question, and perhaps, whether or not she was at home.[211] This data could quickly undermine, or support, any alibi this consumer presented, and law enforcement would be eager to access this information, along with the data from any of the consumer's other "smart" devices.[212]

Reading *Carpenter* alongside Justice Sotomayor's *Jones* concurrence would require law enforcement officers to obtain a warrant before accessing this consumer's data generated by Alexa or other "smart" devices. Because this interpretive stance requires a warrant before law enforcement may gather aggregated data generated through personal technology,[213] this consumer's evening routine as recorded by her Alexa-compatible devices would fall squarely within the Fourth Amendment's protection. The IoT devices disclose this hypothetical consumer's evening routine by collecting and aggregating data from a connected consumer device,[214] thereby presenting the means-based surveillance capability this interpretive stance is calculated to guard against.[215] The data at issue in this scenario also implicates Justice Sotomayor's concerns about data collection that reveals sensitive information about "familial, political, professional, religious, and sexual associations."[216] This consumer's Alexa devices could generate data disclosing her choice of guests and could document the questions and commands she gives the device.[217] Thus, using a combined

---

[211] *See id.*

[212] *See id.*; *see also* Ferguson, *supra* note 43, at 819 (discussing the implications of connected "smart" devices).

[213] *See* United States v. Jones, 565 U.S. 400, 416–17 (2012) (Sotomayor, J., concurring) (discussing surveillance through aggregated data).

[214] *See* Bogost, *supra* note 3; *see also* Posadas, *supra* note 19, at 75–78 (describing IoT devices and the large amounts of data they generate).

[215] *See Jones*, 565 U.S. at 413–14 (Sotomayor, J., concurring); *see also* Solove, *supra* note 178, at 1514 ("[T]he Fourth Amendment should provide protection whenever a problem of reasonable significance can be identified with a particular form of government information gathering.").

[216] *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (citation omitted).

[217] *See* Zwerdling, *supra* note 1.

interpretation of *Carpenter* and Justice Sotomayor's *Jones* concurrence that focuses on both the means of data collection and the sensitive personal information this data could disclose protects data generated on this consumer's "smart" devices from warrantless search.

Reading *Carpenter* alone, however, makes the outcome of this hypothetical less clear. First, the requested data does not directly provide aggregated location information: it can show whether this consumer was at home, but does not provide "a detailed and comprehensive record of the person's movements."[218] Second, it is unclear whether a court would consider verbal commands to be a "qualitatively different category"[219] than bank records and telephone numbers.[220] The court might consider the actual "content" of the command to be protected, but allow warrantless access to data indicating when, and whether, a command was made.[221] Finally, a court could conclude that, unlike CSLI, the collection of data from Alexa devices is not "inescapable and automatic,"[222] since the devices record data generated from commands. Therefore, a court might conclude, without the consumer's instruction to heat a cup of tea, the "smart" microwave would have no data to record.[223]

---

[218] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[219] *Id.* at 2216–17.

[220] *Id.*

[221] *See* Smith v. Maryland, 442 U.S. 735, 741 (1979) (distinguishing a pen register from listening to a protected telephone conversation because the pen register does not acquire the content of the call); *see also* Bellovin et al., *supra* note 4, at 54 ("New technologies challenge many of the basic assumptions underlying such principles as the third-party doctrine. Specifically, there may be no way for a user to know or even discover what kind of information she shares with third parties, many of whom are invisible to her. Similarly, traditional models of what constitutes content and what might be considered mere transactional, non-content information often yield nonsensical, indeterminate, or unsatisfying results when applied to modern technologies.").

[222] *Carpenter*, 138 S. Ct. at 2223.

[223] However, voice-activated devices may record and transmit background conversations that are not intended to be commands, drawing into question whether data from these devices is voluntarily disclosed. *See* Niraj Chokshi, *Is Alexa Listening? Amazon Echo Sent Out Recording of Couple's Conversation*, N.Y. TIMES (May 25, 2018), https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html.

On the other hand, a court might decide to extend protection to Alexa-generated data by relying on a different set of epithets the *Carpenter* Court used to describe CSLI. For example, a court could decide that data from an Alexa-compatible device is "detailed, encyclopedic, and effortlessly compiled,"[224] since it is generated by a commonly-used device that records and transmits verbal cues. Additionally, data generated from an Alexa-compatible device fits the *Carpenter* Court's description of CSLI as "remarkably easy, cheap, and efficient compared to traditional investigative tools,"[225] and could be considered a form of "tireless and absolute surveillance."[226]

By failing to articulate a clear standard for applying its decision to future technologies, the *Carpenter* Court risks implementing a system that protects data generated from personal devices haphazardly.[227] Without a guiding interpretive structure, protection of other forms of data held by third-party businesses could hinge on which of the *Carpenter* majority's various descriptions of CSLI a lower court chooses to use. Alternatively, lower courts could find that no other forms of data rise to this level of sensitivity, rendering CSLI an anomalous exception to the third-party doctrine. However, the *Carpenter* majority's lack of clarity also presents an opportunity to extend Fourth Amendment protection to other forms of aggregated data generated by personal technology and held by third parties. Courts should look to the *Carpenter* decision as a means to extend Fourth Amendment protections to other forms of data, while reading Justice Sotomayor's *Jones* concurrence to provide structure and breadth to this approach.

VI. CONCLUSION

Although *Carpenter* represents a significant step forward for individual privacy rights by protecting historical CSLI from

---

[224] *Carpenter*, 138 S. Ct at 2216.

[225] *Id.* at 2218.

[226] *Id.*; *see also* Chokshi, *supra* note 223.

[227] *See Carpenter*, 138 S. Ct. at 2234 (Kennedy, J., dissenting) ("[T]he Court fails 'to provide clear guidance to law enforcement' and courts on key issues raised by its reinterpretation of *Miller* and *Smith*.") (citing Riley v. California, 134 S. Ct. 2473, 2491 (2014)).

warrantless search, the opinion risks becoming a mere caveat to the third-party doctrine if interpreted narrowly. Additionally, the majority's haphazard approach risks implementing a system that requires "qualitatively different"[228] types of third-party records before Fourth Amendment protections apply, without providing guidelines to assist courts in determining which records satisfy this requirement. Rather than following this narrow, contorted approach, courts should read *Carpenter* alongside Justice Sotomayor's *Jones* concurrence, thereby protecting data generated from personal devices in order to provide a broad, stable foundation for preventing other equally concerning forms of government surveillance. CSLI, sensitive as it may be, should not be the only category of aggregated consumer information held by third-party businesses that is protected after *Carpenter*.

[228] *Carpenter*, 138 S. Ct. at 2216–17.