2021

Carpenter, the Fourth Amendment, and Third-Party Workarounds

Jillian Chambers

CONNECTICUT
LAW REVIEW

VOLUME 53 MAY 2021 NUMBER 1

Note

Carpenter, the Fourth Amendment, and Third-Party Workarounds

JILLIAN CHAMBERS

The Supreme Court's 2018 decision, Carpenter v. United States*, seemed to signal a shift in the Court's Fourth Amendment jurisprudence to acknowledge and adapt to developments in technology. It was a hollow victory. Per* Carpenter*, if a telecommunications company collected and held your cell phone location data, and law enforcement asked for it, they would need a warrant. But if the location data was repackaged and sold to another company or data broker, and then law enforcement bought the data: no warrant necessary. Why is one exchange of cell phone location data subject to stringent warrant requirements while the other has absolutely no Fourth Amendment protection? This is a glaring omission that fails to reflect the reality of modern data sharing practices, and an easy loophole for law enforcement to take advantage. This Note argues that these two scenarios are functionally equivalent and that the Court should treat like cases alike. Otherwise, transactional smoke and mirrors will bar the meaningful application of Fourth Amendment protections to cell phone location data.*

NOTE CONTENTS

Carpenter, the Fourth Amendment, and Third-Party Workarounds

JILLIAN CHAMBERS [*]

> *Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible.*[1]

INTRODUCTION

On December 19, 2019, Stuart A. Thompson and Charlie Warzel of the New York Times published a bombshell report that detailed how an anonymous source provided them with a massive data file that contained fifty billion cell phone location pings, from twelve million Americans, over a period of months between 2016 and 2017.[2] The data came not from a telecommunications company like AT&T or Verizon, nor from government sources; instead, the data was compiled by a location data company that collected the information from software installed quietly onto cell phone applications.[3] When someone downloaded an application and hit "agree" on the terms of service, companies obtained their consent to send and sell location data to "dozens of other technology companies, ad networks, data brokers and aggregators."[4]

The supposedly anonymous location data was so precise that Thompson and Warzel, with help from public records, were able to identify scores of people based on their movements, including a Secret Service agent assigned

[*] University of Connecticut School of Law, J.D. Candidate 2020. Thank you to Professor Molly Land for inspiring me to write this Note, Professor Kiel Brennan-Marquez for untangling my many disparate theories, and endless gratitude to both for being incredible mentors and providing unwavering support. Thanks also to the *Connecticut Law Review* for their diligent edits and excellent company. I would be remiss not to mention Cait Barrett, Demery Ormrod, Samuel Shapiro, Amanda Farrish, Shana Hurley, Mallori Thompson, Jessica Zaccagnino, Carolyn Rennie, and Alexandria Madjeric, not only for their friendship but for selflessly reading numerous drafts. And finally, thank you to Chris—none of this would have been possible without you.

[1] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

[2] Stuart A. Thompson & Charlie Warzel, Opinion, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [hereinafter Thompson & Warzel, *Twelve Million Phones*].

[3] *Id.*

[4] Charlie Warzel, Opinion, *The Loophole that Turns Your Apps into Spies*, N.Y. TIMES (Sept. 24, 2019), https://www.nytimes.com/2019/09/24/opinion/facebook-google-apps-data.html.

to President Trump and senior Pentagon officials.[5] The data also revealed routine commutes of everyday Americans.[6] But Thompson and Warzel could just as easily trace the most intimate and private movements of people: to church, counseling sessions, and chemotherapy treatments.[7] Thompson and Warzel noted that connecting the anonymous location pings to an actual person felt "like reading someone else's diary."[8]

While this particular data cache landed in the hands of reputable reporters, and was provided by someone who was worried about how the data "might be abused and urgently wanted to inform the public and lawmakers,"[9] it is not difficult to imagine a scenario in which the data was given to law enforcement by someone or some company with less altruistic desires in mind.[10] In fact, law enforcement has and does obtain sensitive location data through chains of companies selling, sharing, and repackaging location data.[11]

The four largest cell phone carriers in the United States—AT&T, Verizon, T-Mobile, and Sprint,[12] accounting for 98.8% of the wireless

[5] Thompson & Warzel, *Twelve Million Phones*, *supra* note 2; Stuart A. Thompson & Charlie Warzel, Opinion, *How to Track President Trump*, N.Y. TIMES (Dec. 20, 2019), nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html.

[6] *Id.*

[7] The Editorial Board, Opinion, *Total Surveillance Is Not What America Signed Up For*, N.Y. TIMES (Dec. 21, 2019), https://www.nytimes.com/interactive/2019/12/21/opinion/location-data-privacy-rights.html.

[8] Thompson & Warzel, *Twelve Million Phones*, *supra* note 2.

[9] *Id.*

[10] That is not to say that location data can be and is given to law enforcement with altruistic desires in mind; privacy rights are implicated regardless. For example, local and state governments and the federal government received location data not from cell phone carriers, but from mobile advertisers, in order "to better understand the movements of Americans during the coronavirus pandemic and how they may be affecting the spread of the disease." Byron Tau, *Government Tracking How People Move Around in Coronavirus Pandemic*, WALL ST. J. (Mar. 28, 2020), https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202. Researchers were able to use the data, garnered from mobile applications that users installed on their phones, to identify large numbers of people congregating "in Brooklyn's Prospect Park and handed that information over to local authorities." *Id.* The Centers for Disease Control and Prevention coordinated with universities, technology companies, and data providers—"in conjunction with the White House and others in government"—to get location data. *Id.* Other location data companies like X-Mode Social also tracked cellphones, and by extension, people, who gathered at Florida beaches despite growing concerns about the spread of the disease, and published a video on Twitter depicting the paths and travel of those devices. Aaron Holmes, *Thousands of Spring Breakers Traveled from One Florida Beach to Cities Across the US. Mapping Their Phone Data Shows the Importance of Social Distancing Amid the Coronavirus Outbreak*, BUS. INSIDER (Mar. 27, 2020, 12:04 PM), https://www.businessinsider.com/coronavirus-florida-spring-break-location-data-spread-social-distancing-2020-3.

[11] *See generally* Will Oremus, *The Privacy Scandal That Should Be Bigger than Cambridge Analytica*, SLATE (May 21, 2018, 12:51 PM), https://slate.com/technology/2018/05/the-locationsmart-scandal-is-bigger-than-cambridge-analytica-heres-why-no-one-is-talking-about-it.html (telling how one Missouri sheriff used Securus Technologies to track the locations of eleven people, "including fellow officers and a judge, without their knowledge and without a warrant.").

[12] While T-Mobile and Sprint have completed their multi-year merger, T-Mobile stated "it will take about three years to fully integrate Sprint into its operations and network setup." Chaim Gartenberg, *What's Next for Sprint Customers Now that the T-Mobile Merger has Gone Through?*, VERGE (Apr. 1, 2020, 3:01 PM), https://www.theverge.com/2020/4/1/21203146/tmobile-sprint-customers-plans-network-billing-carriers-merger.

subscription market in 2019[13]—facilitate and participate in the location data market. The location data market is an increasingly lucrative venture with a value projected to exceed $250 million by 2020.[14] These companies frequently utilize data aggregators to coordinate requests for location data, as it is more efficient than if they processed the requests in-house.[15]

LocationSmart was one such company that bought access to the four cell phone carriers' location data and then turned around and sold that same data to, among many others, a small mobile marketing company called 3Cinteractive.[16] Like LocationSmart, 3Cinteractive took the location data and sold it; this time to the largest inmate communications company in the United States, Securus.[17]

Securus's main business stems from their prison video visitation technology, which "allows friends, family members, attorneys, and public officials to schedule and participate in video sessions" with inmates.[18] On the side, Securus was selling a product that allowed local law enforcement agencies to track people's cellphones.[19] Securus required law enforcement to upload a legal document, such as a warrant or affidavit, to certify that the use was authorized. In a not-altogether-surprising twist of fate, Securus never actually reviewed any of the uploaded documents.[20] Securus's phone tracking service specifically targeted law enforcement as potential customers: Securus advertised testimonials of detectives who used their service to successfully find suspects.[21]

This particular apparatus of location data shuffled from major telecommunications companies, through a series of obscure companies that no one in the general public could probably name, and finally to law enforcement, was only revealed as a result of a Missouri sheriff being

---

[13] *See* S. O'Dea, *Wireless Subscriptions Market Share by Carrier in the U.S. from 1st Quarter 2011 to 3rd Quarter 2019*, STATISTA, https://www.statista.com/statistics/199359/market-share-of-wireless-carriers-in-the-us-by-subscriptions/ (last visited Apr. 6, 2020) (noting in quarter three of 2019, Verizon accounted for 29.2% of the market; AT&T accounted for 39.9%; T-Mobile accounted for 16.4%; and Sprint accounted for 13.3%).

[14] Syagnik Banerjee, *Geosurveillance, Location Privacy, and Personalization*, 38 J. PUB. POL'Y & MKTG. 484, 485 (2019).

[15] Letter from Timothy P. McKone, Exec. Vice President, Fed. Rels., AT&T Servs., Inc., to Ron Wyden, U.S. Sen. 1–2 (June 15, 2018), https://www.wyden.senate.gov/imo/media/doc/at&t%20letter%20to%20RW%206.15.pdf.

[16] 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 [hereinafter Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*].

[17] *Id.*

[18] SECURUS TECH., https://securustech.net/ (last visited Apr. 4, 2020).

[19] Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, *supra* note 16.

[20] Letter from Ron Wyden, U.S. Sen., to Ajit Pai, Chairman, Fed. Comm. Comm'n 1 (May 8, 2018), https://www.wyden.senate.gov/imo/media/doc/wyden-securus-location-tracking-letter-to-fcc.pdf [hereinafter Wyden Letter].

[21] Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, *supra* note 16.

charged with using Securus's service to track a judge and other police officers without a court order.[22]

As LocationSmart had a direct contractual relationship with the telecommunications companies, it was required to obtain affirmative consent from individual customers before sharing location data.[23] Senator Ron Wyden of Oregon described the chain of contracts between each company as "the legal equivalent of a pinky promise."[24] Unlike LocationSmart, Securus did not have the same direct contractual relationship, and thus, was not obligated to obtain consent before sharing data with police.[25] "The relationship between Securus and LocationSmart impacted almost all U.S. cell phone users,"[26] and there was no way for an individual to opt out.[27]

Following public efforts of Senator Wyden to push the Federal Communications Commission ("FCC") to investigate the role of the telecommunications company in this scheme,[28] each cell phone carrier pledged to end the sale of location data to location aggregators.[29] Nearly two years after this particular breach of customer privacy was revealed to the public, the FCC approved a proposal to fine the four cell phone carriers $200 million for selling the location data to companies that allowed it to be misused.[30] One FCC Commissioner dissented from the proposal on the grounds that it was too little, too late, while FCC Chairman Ajit Pai lauded the action as protecting American consumers.[31]

And while law enforcement must obtain a warrant when seeking historical cell site location information ("CSLI") directly from a cell phone provider,[32] no legal protection attaches when the data is shuffled through a

---

[22] *Id.*

[23] Letter from Timothy P. McKone to Ron Wyden, *supra* note 15, at 2.

[24] Wyden Letter, *supra* note 20, at 1.

[25] Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, *supra* note 16.

[26] Paige M. Boshell, *The Power of Place: Geolocation Tracking and Privacy*, BUS. L. TODAY (Mar. 25, 2019), https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/#_ftn1.

[27] Oremus, *supra* note 11.

[28] *Id.*

[29] Frank Bajak, *Mobile Carriers Cut Off Flow of Location Data to Brokers*, ASSOCIATED PRESS (June 19, 2018), https://apnews.com/8582857aff8146f8ac81d247533b2177.

[30] Jennifer Valentino-DeVries, *Cellphone Carriers Face $200 Million Fine for Not Protecting Location Data*, N.Y. TIMES (Feb. 28, 2020), https://www.nytimes.com/2020/02/28/technology/fcc-cellphones-location-data-fines.html [hereinafter Valentino-DeVries, *Cellphone Carriers Face $200 Million Fine for Not Protecting Location Data*]. Under the proposal, the FCC is seeking "more than $91 million from T-Mobile, $57 million from AT&T, $48 million from Verizon and $12 million from Sprint[;]" reflecting "the length of time the carriers failed to safeguard the data and the number of companies with which they shared it." *Id.* T-Mobile's fine is significantly higher than the other three companies in part because it shared the data with over eighty companies. *Id.*

[31] *Id.* (noting that the while the proposed fine is "an unusually large penalty," the judgment "is modest compared with the companies' revenue, which totaled more than $350 billion last year"). Interestingly, FCC Chairman Pai "represented Securus while working at a law firm in 2011; he also worked as a lawyer for Verizon." *Id.*

[32] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

chain of companies and eventually lands in the hands of the police. Location data is largely unregulated; the only reason why the FCC was able to impose a fine on the cell phone carriers is because they are "subject to more stringent regulations than technology companies."[33] The location data market is rife with loopholes just waiting to be exploited.

Part I analyzes the Supreme Court's inconsistent—and shaky-at-best—Fourth Amendment jurisprudence. In particular, Part I describes why the Court's third-party doctrine, the primary barrier to extending Fourth Amendment protection, is particularly ill-suited to the rapidly developing technological era the country is in. Part I also introduces the Court's recent case granting Fourth Amendment protection to historical CSLI, *Carpenter v. United States*.

Part II argues that *Carpenter* should be applied to historical CSLI obtained by law enforcement from an entity that did not conduct the initial data collection, and thus plug the loophole created by the reality of modern data sharing practices. Absent a warrant supported by probable cause, the passage of historical CSLI to law enforcement is an unreasonable search under the Fourth Amendment.

Part III applies this framework and explains why a warrant requirement to obtain historical CSLI serves prosecutorial interests. Part III also addresses and dismisses potential counterarguments for affording historical CSLI complete Fourth Amendment protection from law enforcement acquisition absent a warrant.

I. THE FOURTH AMENDMENT'S SLOW BEND TOWARD TECHNOLOGY

The Fourth Amendment of the Constitution protects:

> The 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.[34]

The Supreme Court has repeatedly reaffirmed that the "basic purpose of this Amendment . . . is to safeguard the privacy and security of individuals

---

[33] Valentino-DeVries, *Cellphone Carriers Face $200 Million Fine for Not Protecting Location Data*, *supra* note 30.

[34] U.S. CONST. amend. IV. The Supreme Court has defined the distinction between a "search" and a "seizure" as thus: "A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed. A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." United States v. Jacobsen, 466 U.S. 109, 113 (1984) (internal quotation marks and footnotes omitted).

against arbitrary invasions by governmental officials."[35] Absent this basic coda, however, Fourth Amendment jurisprudence is largely unsettled and full of contradictory rules that have exceptions to their exceptions. As Justice Scalia noted, "every case is so fact-specific that any particular opinion merely answers 'variation 3,542.'"[36]

A. *Third-Party Doctrine*

The Fourth Amendment is generally understood to protect "people, not places," meaning that although publicly presented information is not subject to Fourth Amendment protection, what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[37] To receive the protection of the Fourth Amendment, a person must have a reasonable expectation of privacy.[38] The reasonable expectation of privacy test has two requirements: (1) a person exhibited an actual, subjective expectation of privacy, and (2) the expectation is one that society recognizes as "reasonable."[39] Following the articulation of the reasonable expectation of privacy test, the Court has steadily narrowed the Fourth Amendment protection it affords against government searches, particularly in the area of information given voluntarily to third parties.

In *United States v. Miller*, the Court held that a person has no legitimate expectation of privacy in information given voluntarily to a third party, even if the information would ordinarily be protected by the Fourth Amendment—bank records clearly falling within the definition of "papers"—had the government obtained it directly from the person claiming the right.[40] In *Miller*, the defendant was convicted of "possessing an unregistered still, carrying on the business of a distiller without giving bond and with intent to defraud the Government of whiskey tax, possessing 175 gallons of whiskey upon which no taxes had been paid, and conspiring to defraud the United States of tax revenues."[41] Miller's bank records were not presented to the grand jury that indicted him; rather, they were used by federal agents to further their investigation.[42] The Court found that a person takes a risk in revealing

---

[35] Camara v. Mun. Ct. of S.F., 387 U.S. 523, 528 (1967). *See also* Schmerber v. California, 384 U.S. 757, 767 (1966) ("The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State.").

[36] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011) (quoting Interview by Susan Swain with Antonin Scalia, Assoc. Just. U.S. Sup. Ct., in Wash., D.C. (June 19, 2009), http://supremecourt.c-span.org/assets/pdf/AScalia.pdf).

[37] Katz v. United States, 389 U.S. 347, 351 (1967).

[38] *Id.* at 360 (Harlan, J., concurring).

[39] *Id.* at 361.

[40] United States v. Miller, 425 U.S. 435, 443 (1976).

[41] *Id.* at 436.

[42] *Id.* at 438.

information to a bank "that the information will be conveyed by [the bank] to the Government."[43] Thus, the third-party doctrine was born.

Three years later, the Court similarly held that the installation of a pen register to discern the numbers dialed on a particular phone line by a telephone company suffered from the same Fourth Amendment defects as the bank records in *Miller*.[44] Smith robbed a home and then began placing "threatening and obscene phone calls" to the house.[45] At the request of the police, the telephone company installed a pen register on Smith's home and found that he called the victim's home.[46] Law enforcement was able to get a warrant to search Smith's home on the basis of the phone call.[47] In particular, the Court in *Smith v. Maryland* found it persuasive that pen registers "do not acquire the *contents* of communications" and were thus distinguishable from the listening devices used by police in *Katz*.[48] The Court "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial" and that "[a]ll subscribers" know that their phone company has the ability to make records of the numbers they have dialed because the numbers are listed on their bills.[49] Further, pen registers, and the records they produced, served an important business function: "checking billing operations, detecting fraud and preventing violations of law."[50]

B. *Third-Party Doctrine in the Digital Era*

Presciently, Justice Brandeis, in his famous dissent in *Olmstead v. United States*, wrote that "time works changes, brings into existence new conditions and purposes. Subtler and more far-reaching means of invading privacy have become available to the government."[51] Of course, the Supreme Court could not have known in the 1920s, let alone the 1960s when the Court handed down *Miller* and *Smith*, just how unworkable the third-party doctrine and Fourth Amendment jurisprudence would become in the Digital Era.[52]

The basis of third-party doctrine reasoning—that people understand what information they are handing over, and to whom—was more justifiable in the era of local, in-person bank transactions and home telephones. Rarely,

---

[43] *Id.* at 443.

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

[45] *Id.* at 737.

[46] *Id.*

[47] *Id.*

[48] *Id.* at 741.

[49] *Id.* at 742.

[50] *Id.* (internal quotation marks and citation omitted).

[51] Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting) (internal quotations omitted).

[52] *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002) (discussing how "an increasing amount of personal information is contained in records maintained by" third parties, and that this data "increasingly flows from the private sector to the government, particularly for law enforcement use").

if ever, do people know what data they submit when they agree to terms of service or download an application, even though actual, subjective knowledge is a crucial aspect of whether someone has a reasonable expectation of privacy.[53]

Cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[54] Cell phones function as a navigational tool, a bank, a library, a diary, and a photo album, not to mention the myriad of ways to communicate such as texting, calling, or video chatting. Most Americans own a cell phone—96% and rising—with 81% owning smartphones.[55] Smartphone ownership is up from just 35% in 2011.[56] Low-income Americans are among those who rely the most on smartphones: "26% of adults living in households earning less than $30,000 a year are 'smartphone-dependent,'" meaning the primary way in which they access the internet is through their smartphone.[57]

Going hand-in-hand with the ubiquitous use of cell phones is the use of cell phone location data by law enforcement. In 2015, AT&T received 76,340 requests for CSLI from law enforcement, Verizon received 50,066 requests, and Sprint received 64,854—the majority of which were warrantless.[58]

Because of this, criticism of the third-party doctrine has intensified. Countless scholarship has been dedicated to the scope of the Fourth Amendment, being described "as confusing, illogical, chaotic, and inconsistent across cases."[59] Regarding the third-party doctrine, critics point to the fact

---

[53] *See* Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 152 (2016) ("People's knowledge about surveillance technologies, police practices, existing laws, and the behavior of private entities shapes their expectations of privacy.") [hereinafter Tokson, *Knowledge and Fourth Amendment Privacy*].

[54] Riley v. California, 573 U.S. 373, 385 (2014).

[55] *Mobile Fact Sheet*, PEW RSCH. CTR. (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile/ [hereinafter *Mobile Fact Sheet*]. Smartphones are cell phones that connect to the internet and run applications. Laura Silver, Aaron Smith, Courtney Johnson, Jingjing Jiang, Monica Anderson & Lee Rainie, *Mobile Connectivity in Emerging Economies*, PEW. RSCH. CTR. (Mar. 7, 2019), https://www.pewresearch.org/internet/2019/03/07/use-of-smartphones-and-social-media-is-common-across-most-emerging-economies/.

[56] *Mobile Fact Sheet*, *supra* note 55.

[57] Monica Anderson & Madhumitha Kumar, *Digital Divide Persists Even as Lower-Income Americans Make Gains in Tech Adoption*, PEW RSCH. CTR. (May 7, 2019), https://www.pewresearch.org/fact-tank/2019/05/07/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/. "Reliance on smartphones for online access is especially common among younger adults, non-whites and lower-income Americans." *Mobile Fact Sheet*, *supra* note 55.

[58] Brief of Amici Curiae Electronic Frontier Foundation, Brennan Center for Justice, Center for Democracy & Technology, The Constitution Project, & National Coalition to Protect Civil Freedoms as in Support of Petitioner at 12–14, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).

[59] Tokson, *Knowledge and Fourth Amendment Privacy*, *supra* note 53, at 144 (collecting sources) (footnotes omitted). *See also* Anna Lvovsky, *Fourth Amendment Moralism*, 166 U. PA. L. REV. 1189, 1208 (2018) ("The [Supreme] Court has provided no coherent test of reasonableness, and a common criticism of the *Katz* test denigrates it as too open-ended, unpredictable and easily manipulated.") (footnotes omitted); Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 555 (1996) (describing end of the twentieth

that it gives license to entities to collect "vast amounts of personal online data at very low cost," while also favoring the interests of law enforcement.[60]

The Supreme Court's Fourth Amendment jurisprudence has long had cracks in its foundation; over the last twenty-five years, the Court has been reluctant to apply a strong third-party doctrine.[61] Justice Sotomayor specifically called into question the continued feasibility of the third-party doctrine in the Court's Fourth Amendment jurisprudence, writing that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," in part because the doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[62]

Thus, there was little surprise when the Court's frustration with the third-party doctrine and CSLI came to a head in the 2018 case, *Carpenter v. United States*.

C. *Turning Point:* Carpenter v. United States

In 2011, four men were arrested for robbing a series of T-Mobile stores.[63] One of these men gave up the name and phone number of Timothy Carpenter, an alleged accomplice. Armed with that information, law enforcement acquired a subpoena under the Stored Communications Act for the cell phone records of Carpenter.[64] The Stored Communications Act allowed the government to obtain cell phone records on "reasonable grounds"[65]—meaning, law enforcement did not have to get a warrant to access this information. Ultimately, law enforcement obtained 127 days of Carpenter's cell-site records, totaling "12,898 location points cataloging Carpenter's movements."[66] The records confirmed Carpenter was at the exact location of the robbery at the exact time of the robbery.[67] Carpenter was convicted and sentenced to over 100 years in prison for robbery and firearm charges after

---

century Fourth Amendment theory as "in tatters" and in "disarray"); Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 759 (1994) (describing Fourth Amendment jurisprudence as "a sinking ocean liner—rudderless and badly off course"); Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1468 (1985) (describing the Supreme Court's Fourth Amendment caselaw as "a mass of contradictions and obscurities"); Lloyd L. Weinreb, *Generalities of the Fourth Amendment*, 42 U. CHI. L. REV. 47, 49 (1974) (finding the body of Fourth Amendment doctrine "unstable and unconvincing").

[60] Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 585–86 (2011).

[61] *See* Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third-Party Doctrine*, 14 N.C. J.L. & TECH. 431, 438–42 (2013) (detailing cases in which the Supreme Court has declined to utilize a "mechanical application of a categorical third party doctrine").

[62] United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

[63] *Carpenter*, 138 S. Ct. at 2212.

[64] *Id.*

[65] *Id.*

[66] *Id.*

[67] *Id.* at 2213.

unsuccessfully moving to suppress the cell site records provided by the telecommunications companies.[68] In the government's view, the expert testimony that relied exclusively on the CSLI "clinched the case."[69]

From the beginning of the opinion, technology, cell phones, and the data that cell phones produce played an enormous role in the Court's decision. Chief Justice Roberts, writing for the majority, began by stating that "[t]here are 396 million cell phone service accounts in the United States—for a Nation of 326 million people."[70] The Court further noted that "cell phone location information is detailed, encyclopedic, and effortlessly compiled"[71] and that it "implicates basic Fourth Amendment concerns about arbitrary government power" more so than the historical third-party records such as bank records or pen registers.[72] Historical CSLI makes "cell phone tracking remarkably easy, cheap, and efficient compared to traditional investigative tools."[73]

The Court declined to extend *Smith* and *Miller* to historical CSLI, holding that "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[74] Supreme Court precedent of the 1970s could not "have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."[75] And even though CSLI is generated primarily for commercial purposes, "that distinction does not negate [a person's] anticipation of privacy in his physical location."[76] Thus, a warrant supported by probable cause is now needed for government searches of historical CSLI.[77]

Carpenter is a cautious and narrow decision; the Court declined to extend Fourth Amendment protection to real-time CSLI, tower dumps, conventional surveillance techniques, "business records that might incidentally reveal location information," or collection techniques used abroad or for national security.[78] The Court only addressed the question of "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements."[79]

In his dissent, Justice Gorsuch argued that the problem with the third-party doctrine is not the application but with the cases themselves.[80]

---

[68] *Id.* at 2212–13.
[69] *Id.* at 2213.
[70] *Id.* at 2211.
[71] *Id.* at 2216.
[72] *Id.* at 2222.
[73] *Id.* at 2217–18.
[74] *Id.* at 2217.
[75] *Id.*
[76] *Id.*
[77] *Id.* at 2221.
[78] *Id.* at 2220.
[79] *Id.* at 2211.
[80] *Id.* at 2262 (Gorsuch, J., dissenting).

Justice Gorsuch expressed doubt that the government can "demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights," but under *Smith* and *Miller*, the government would not run "afoul of *Katz*."[81] With that regime, Justice Gorsuch asks, "[w]hat's left of the Fourth Amendment?"[82] Justice Gorsuch inevitably advocates for a return to a "more traditional" property-based approach of the Fourth Amendment, although he agrees with the majority's "implicit but unmistakable conclusion that the rationale of *Smith* and *Miller* is wrong."[83]

Unsurprisingly, Justice Thomas also dissented. Justice Thomas advocated for throwing out *Katz* and the reasonable expectation of privacy test because it "has no basis in the text or history of the Fourth Amendment."[84] Like Justice Gorsuch, Justice Thomas would prefer to understand liberty and privacy rights "in terms of property rights."[85]

Justice Alito rounded out the dissenters by noting that while he "share[d] the Court's concern about the effect of new technology on personal privacy," he worried about "a blizzard of litigation . . . threatening many legitimate and valuable investigative practices upon which law enforcement has rightfully come to rely."[86]

Since the Court handed down *Carpenter*, lower courts have struggled to apply it. Of the first ninety or so cases to cite *Carpenter*, courts have cited to it for "ancillary reasons," distinguished *Carpenter* on the facts, or refused to suppress the CSLI based on the good faith exception.[87] This has not changed in the last year. Courts continue to decline to extend, distinguish, or cite to *Carpenter* as an aside.[88] In fact, on remand, the Sixth Circuit Court

---

[81] *Id.*

[82] *Id.*

[83] *Id.* at 2272.

[84] *Id.* at 2236 (Thomas, J., dissenting).

[85] *Id.* at 2239.

[86] *Id.* at 2246–47 (Alito, J., dissenting).

[87] Rick Aldrich, *Privacy's "Third-Party" Doctrine: Initial Developments in the Wake of* Carpenter, 15 A.B.A. SCITECH LAW. 4, 6–7 (2019). *See also* United States v. Leon, 468 U.S. 897, 913 (1984) (creating the "good-faith exception" to the exclusionary rule by holding that the search or seizure of evidence by police "reasonably relying on a warrant issued by a detached and neutral magistrate" does not violate the Fourth Amendment).

[88] *See, e.g.*, United States v. Hargett, 797 F. App'x 765, 767 (4th Cir. 2020) (declining to extend *Carpenter* to real-time CSLI); Zietzke v. United States, No. 19-cv-03761-HSG(SK), 2020 WL 264394, at *12–13 (N.D. Cal. Jan. 17, 2020) (declining to extend *Carpenter* to cryptocurrency transactions); United States v. Beverly, 943 F.3d 225, 229–30 (5th Cir. 2019) (finding that the government's search of historical CSLI fell within the good faith exception); United States v. Kidd, 394 F. Supp. 3d 357, 366 (S.D.N.Y. 2019) (declining to extend *Carpenter* to IP addresses because the defendant failed to show that the government's "ability to precisely track his daily movements necessarily follows from the fact that IP address information conveys some location information"); United States v. Morel, 922 F.3d 1, 8 (1st Cir. 2019) (declining to extend *Carpenter* to "IP address information and . . . images uploaded to Imgur"); United States v. Jenkins, No. 1:18-cr-00181, 2019 WL 1568154, at *4 (N.D. Ga. Apr. 11, 2019) (declining to extend *Carpenter* to "user and subscriber information for accounts using specific IP addresses"); United States v. VanDyck, 776 F. App'x 495, 496 (9th Cir. 2019) (declining to extend *Carpenter* to "subscriber information associated with [an] IP address"); United States v. Wellbeloved-Stone, 777 F. App'x 605, 607 (4th Cir. 2019) (declining to extend *Carpenter* to subscriber information

of Appeals affirmed the denial of Carpenter's motion to suppress the historical CSLI on the grounds that the Federal Bureau of Investigation's agents obtained the data in good faith.[89] These cases have also not dealt with situations in which law enforcement obtained location data from entities that took no part in the initial data collection. Thus, this presents a novel question of law for the Supreme Court to decide.

II. FURTHER EXTENDING *CARPENTER*'S FOURTH AMENDMENT PROTECTION OF HISTORICAL CSLI

The direct connection from a telecommunications company to law enforcement, at least when it comes to historical CSLI, is now covered by *Carpenter*'s holding. What about when law enforcement obtains historical CSLI through an extended telecommunications infrastructure? A chain of companies passing, packaging, and parsing historical CSLI, marketed specifically to law enforcement?

Carpenter was decided correctly, but the Court again did not articulate any sort of workable model for analyzing Fourth Amendment claims going forward. Instead, the Court should look at the nature of the transaction between the cell phone company and police. Certainly, the Fourth Amendment is at least, at the outset, implicated by personal information passing to law enforcement. Making the transaction of information from private parties to law enforcement the focus of the Fourth Amendment makes the analysis easier to apply to a wide variety of information—so there is not one line of jurisprudence for pen registers and another for placing microphones in telephone booths.

Ultimately, the majority in *Carpenter* failed to recognize the reality of data sharing and a popular avenue for government acquisition of historical CSLI. The Court should expand the protections that *Carpenter* affords historical CSLI and provide courts with the flexibility and framework to address it. Otherwise, data sharing apparatuses will simply become another unworkable loophole like *Miller*, *Smith*, and the third-party doctrine.

In a Fourth Amendment analysis, there are two questions to be asked: (1) was there a search or seizure, and if yes, (2) was it unreasonable? Law enforcement acquisition of historical CSLI through a chain of companies implicates both inquiries. It is a search protected by the Fourth Amendment because of the Supreme Court's precedent in *Carpenter*: the apparatus is functionally the same as a cell phone carrier sharing data directly with law enforcement. Further, the search is unreasonable absent a warrant supported

---

and IP addresses); United States v. Walsh, 774 F. App'x 706, 708 (2d Cir. 2019) (finding that the search of historical CSLI fell within the good faith exception).

[89] United States v. Carpenter, 926 F.3d 313, 318 (6th Cir. 2019), *reh'g granted*, 788 F. App'x 364, 364 (6th Cir. 2019) (rehearing granted on the grounds that "the district court erred when it sentenced him for his robbery convictions without considering the 1,260-month mandatory-minimum sentence to which he was already subject").

by probable cause. The search is unreasonable, and thus needs a warrant, because of the current state of unfettered data collection and private entities collaborating with law enforcement absent any meaningful legal constraints.

A. *A Search Under the Fourth Amendment*

Currently, Fourth Amendment doctrine "focuses on the degree of governmental influence over initial collection."[90] Instead, the Fourth Amendment analysis should focus on the final link of the chain: did law enforcement acquire location data from a private entity? When police accept, seek, buy, or are given historical CSLI, the Fourth Amendment should recognize it as a search. To find otherwise would be a failure to meaningfully effectuate *Carpenter*'s holding.

Chief Justice Roberts's majority opinion in *Carpenter* tells us as much. Specifically, the Court held that regardless of whether law enforcement uses its own surveillance apparatus or "leverages the technology of a wireless carrier," the location information obtained is "the product of a search."[91] Thus, the Fourth Amendment attaches because of the invasive nature of the location data that reveals the whole of someone's movements.

There is Fourth Amendment protection when law enforcement uses technology to track someone's every movement. The device might utilize some third party to transmit or store the information collected by law enforcement, but the mere introduction of a third (or fourth, fifth, et cetera) party into the surveillance process does not defeat the protections of the Fourth Amendment. The final product is the same: location data that reveals the most private aspects of someone's life, such as "familial, political, professional, religious, and sexual associations."[92] Likewise, the transmittal of location data from a cell phone carrier to law enforcement—regardless of intervening or additional parties in the process—should be afforded Fourth Amendment protection per *Carpenter*.

To put it another way, the Court has not been shy in its assertion that private contracts do not affect whether someone is entitled to their Fourth Amendment rights. A month before the *Carpenter* decision was handed down, the Court held that a car rental agreement did not override the defendant's reasonable expectation of privacy.[93] In *Byrd v. United States*, the defendant challenged a search of a rental car he was operating that resulted in law enforcement finding forty-nine bricks of heroin in the trunk.[94] The government argued that because Byrd was not listed on the rental

---

[90] Kiel Brennan-Marquez, *The Constitutional Limits of Private Surveillance*, 66 KAN. L. REV. 485, 488 (2018) [hereinafter Brennan-Marquez, *The Constitutional Limits of Private Surveillance*].

[91] *Carpenter*, 138 S. Ct. at 2217.

[92] *Id.* (quoting Jones v. United States, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (internal quotation marks omitted).

[93] Byrd v. United States, 138 S. Ct. 1518, 1529 (2018).

[94] *Id.* at 1525.

agreement, the violation of the contract "meant [that he] could not have had any basis for claiming an expectation of privacy in the rental car at the time of the search."[95] With Justice Kennedy writing for the majority, the Court found that the breach of the rental car agreement had no bearing on Byrd's reasonable expectation of privacy so long as he had lawful possession of the car.[96] *Byrd* stands for the general proposition that private contracts do not dictate how the Fourth Amendment will operate. Similarly, the fact that location data is shared with law enforcement through a chain of companies—necessarily facilitated by private contracts—does not automatically remove Fourth Amendment protection.

Copyright's fair use doctrine illustrates why the Court should consider law enforcement acquisition of historical CSLI through a third party as functionally equivalent to an acquisition directly from a cell phone carrier. The fair use doctrine is a similar form of imposing liability on one for the collective infringement of the many in the face of technological advancements. Section 106 of the Copyright Act generally protects the exclusive right of a copyright owner to, for example, reproduce works, prepare derivative works, and perform copyrighted works publicly.[97] Section 107, on the other hand, provides an exception to a copyright owner's exclusive rights: fair use.[98] Whether something is considered fair use of a copyrighted work is subject to four factors:

> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
>
> (2) the nature of the copyrighted work;
>
> (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
>
> (4) the effect of the use upon the potential market for or value of the copyrighted work.[99]

Fair use doctrine thus demands a "case-by-case analysis" by courts in line with the articulated four factors.[100]

In an illustrative case, *American Geophysical Union v. Texaco Inc.*, the Second Circuit adapted copyright jurisprudence to account for the

---

[95] *Id.* at 1529.

[96] *Id.*

[97] 17 U.S.C. § 106 (2018).

[98] *Id.* at § 107.

[99] *Id.*

[100] *See* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 577 (1994) ("The task is not to be simplified with bright-line rules, for the statute, like the doctrine it recognizes, calls for case-by-case analysis."); Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 549 (1985) ("Section 107 requires a case-by-case determination whether a particular use is fair, and the statute notes four nonexclusive factors to be considered.").

then-novel developments in photocopying technology.[101] A research scientist named Chickering at Texaco made eight photocopies of Journal of Catalysis articles to reference in his lab.[102] Instead of framing the alleged copyright infringement around a single research scientist engaging in his own research, the court considered "whether Texaco's photocopying by 400 or 500 scientists, *as represented by Chickering's example*, is a fair use."[103] The court, although noting that the nature of the user of the copyrighted material is important, emphasized "that a court's focus should be on the *use* of the copyrighted material."[104] The Second Circuit did not characterize the situation at Texaco as "photocopying for personal use by an individual," but rather, it was the "institutional, systemic, archival multiplication of copies" that persuaded the court that the Copyright Act was violated.[105]

Just as the advent of photocopying threatened "to disrupt the delicate balances established by the Copyright Act" such that courts adjusted accordingly,[106] the Supreme Court should recalibrate its Fourth Amendment jurisprudence to acknowledge and account for the different ways in which location data is obtained by law enforcement. And for Fourth Amendment purposes, the focus should not be on the fact that the data was collected by private companies; rather, the focus should be on the fact that the data is being utilized by law enforcement. And like how photocopying aggregated on a massive scale threatened the demise of adequate copyright protections without judicial intervention,[107] current data practices with historical CSLI threaten adequate Fourth Amendment protections. It should not make a difference whether the historical CSLI was obtained because of the efforts of an individual cell phone carrier or the efforts of a collection of companies; at the end of the day, law enforcement is "leverage[ing] the technology of a wireless carrier."[108] The actions of many are functionally equivalent to the actions of one, and result in the same outcome: a search under the Fourth Amendment.

The third-party doctrine provides no protection to law enforcement seeking to obtain historical CSLI from an entity who was not involved in the initial data collection. At a minimum, the Court clearly wants to protect historical CSLI. Indeed, *Carpenter* is indicative of the Court's willingness to chip away at the logic underpinning the third-party doctrine,[109] even if a

---

[101] Am. Geophysical Union v. Texaco Inc., 60 F.3d 913, 914 (2d Cir. 1994), *cert. denied*, 516 U.S. 1005 (1995).

[102] *Id.* at 915.

[103] *Id.* at 916 (emphasis added).

[104] *Id.* at 921–22.

[105] *Id.* at 931.

[106] *Id.* at 917 (citing Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 467–68 n.16 (1984) (Blackmun, J., dissenting) (recognizing that "[t]he advent of inexpensive and readily available copying machines . . . has changed the dimensions" of the legal issues concerning the practice of making personal copies of copyrighted materials)).

[107] *Id.*

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

[109] *See id.* at 2220 (declining to extend the third-party doctrine to historical CSLI).

majority is not ready to fully overturn a fifty-year line of precedents. But for *Carpenter* to have any meaning, there must be some limit on law enforcement acquisition of historical CSLI from third parties, even if not originally anticipated by the Court. It would be perverse if after *Carpenter*, law enforcement can extinguish Fourth Amendment rights by contracting around them, and *Byrd* signals this concern. Under an anti-circumvention rationale,[110] the Court does not want to push law enforcement into sketchy practices with less judicial supervision than what was at issue in *Carpenter*. A procurement contract is even easier to get than a subpoena, let alone a warrant.

Further, the third-party doctrine rests on the assumption that information is provided voluntarily by an individual. Again, the notion of voluntariness cannot be squared with the Court's own reasoning in *Carpenter*, as Chief Justice Roberts noted that CSLI "is not truly 'shared' as one normally understands the term," as a cell phone logs location data automatically "without any affirmative act on the part of the user."[111] This reasoning holds even more sway as it is less likely that a cell phone user knows when, how much, and to whom their location data is going to than they do when the cell phone is logging the records.

B. *An Unreasonable Search Absent a Warrant*

There is an unconstitutional violation of the Fourth Amendment only when a government search is unreasonable.[112] It is not enough that a search occurred; the Constitution requires more. The Court has held that "the ultimate measure of the constitutionality of a government search is 'reasonableness.'"[113] Though like the rest of the Court's Fourth Amendment jurisprudence, what "unreasonable" means is a nebulous and logic-defying concept.[114]

Courts determine the reasonableness of a search by balancing the "intrusion on the individual's Fourth Amendment interests against [the

---

[110] Anti-circumvention plays a large role in the Supreme Court's campaign finance jurisprudence and is apt for a similar instance here of "evasion of [an] existing law through the exploitation of a loophole." Nabil Ansari, Note, *Judicial Standards for the Anti-Circumvention Rationale in Campaign Finance*, 19 N.Y.U. J. LEGIS. & PUB. POL'Y 417, 422–23 (2016) (describing how circumvention is "prevalent when sophisticated actors, especially repeat players in a regulated area, are confronted with particularly strong incentives to evade the law," and that the Court agrees that "circumvention is a valid theory of corruption") (internal quotation marks omitted). *See also* Trump v. Mazars USA, LLP, 140 S. Ct. 2019, 2035 (2020) (describing the Court's concern with Congress "sidestep[ping] constitutional requirements" to obtain a president's information from "a third party—as occurs with rapidly increasing frequency" (citing *Carpenter*, 138 S. Ct. at 2219–20)).

[111] *Carpenter*, 138 S. Ct. at 2220.

[112] U.S. CONST. amend. IV.

[113] Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652 (1995).

[114] *See* Lawrence Rosenthal, *Binary Searches and the Central Meaning of the Fourth Amendment*, 22 WM. & MARY BILL RTS. J. 881, 881 (2014) ("Few constitutional commands offer less textual guidance than the Fourth Amendment's prohibition on 'unreasonable search and seizure.'"); John D. Castiglione, *Human Dignity Under the Fourth Amendment*, 2008 WIS. L. REV. 655, 656 (2008) ("The reasonableness requirement of the Fourth Amendment is just about the most unhelpful guidepost one could have concocted. . .").

search's] promotion of legitimate governmental interests."[115] Warrantless searches are typically unreasonable when undertaken by law enforcement officials to discover evidence.[116] The intrusion of an individual's Fourth Amendment interest is especially acute when law enforcement acquires historical CSLI from an entity that did not conduct the initial data collection.

The market for location data is massive and split into two: the initial collection and a secondary market. The initial collection and use of location data are what most people are familiar with: a cell phone user downloads an application and agrees to share their location. In return, the user is provided a service. For some applications, location data is integral to its functioning, like maps, directions, or ridesharing. The application needs the user's location data to give accurate directions. This use of location data is to the benefit of the user: "the more accurate and recent the location data, the more accurate the app[lication] service."[117] The cell phone carrier shares the location data with the third-party application at the behest of the individual user, limited to specific purposes and bound by nondisclosure agreements.[118] The user consents to the use of their location data and receives a tangible, particularized, and usually temporary benefit as a result.

The secondary market for location data imposes the privacy concerns that make law enforcement acquisition through this market unreasonable for Fourth Amendment purposes. While the initial collection of location data provides a service to the cell phone user, "[t]he secondary location data market "is used to monetize location data for unrelated purposes."[119] The market for consumer data is massive: "90 percent of all consumer data that is currently in circulation" was created in the last few years.[120] The location data market is also extremely lucrative: there is $21 billion in location-targeted advertising alone.[121] A few companies "claim to track up to 200 million mobile devices in the United States—about half those in use last year."[122] They have access to location data that is accurate to within a few yards and updated "more than 14,000 times a day."[123]

Running parallel with rapid growth in the location data market is increased collaboration between law enforcement and the private sector. Private companies have recognized that traditional law enforcement means

---

[115] *Vernonia Sch. Dist. 47J*, 515 U.S. at 652–53 (quoting Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 619 (1989)).

[116] *Carpenter*, 138 S. Ct. at 2221.

[117] Boshell, *supra* note 26.

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html. In 2018, "sales of location-targeted advertising reach[ed] an estimated $21 billion." *Id.*

[122] *Id.*

[123] *Id.*

of gathering information are inadequate to match the sophistication of crime and have adapted accordingly. There is a whole private surveillance industry that has developed and advertised with law enforcement in mind; companies most frequently either (1) provide some sort of product for local law enforcement to buy or lease and use in-house, or (2) conduct some aspect of traditional law enforcement surveillance, allowing police to "contract out" aspects of their job.[124] These partnerships, motivated by money or otherwise, blur the line between Fourth Amendment-regulated "public" policing and not-subject-to-any-Fourth Amendment protection "private" policing.

The Court has previously expressed that when the government encourages, endorses, and participates in the collection of information by a private entity, the Fourth Amendment is implicated.[125] That is not to say that every encouragement by law enforcement to compel private citizens or entities to assist in policing—like offering a reward for information—would be swept up in this reasoning. But again, when an entire industry evolves to support law enforcement, the warrantless search looks increasingly unreasonable.[126]

---

[124] One such company that provides both of the aforementioned services is Vigilant Solutions, a company that profits off of its license plate reader ("LPR") technology and has "the world's largest private LPR data network." *Our Passion*, VIGILANT SOLUTIONS, https://www.vigilantsolutions.com/our-passion/ (last visited Apr. 5, 2020) [hereinafter *Our Passion*]. Vigilant Solutions is a company centered around products created by former law enforcement, with law enforcement in mind; the company describes their mission as "protecting officers, families, and communities[,]" designs their products "to collect, organize and share data to credentialed law enforcement personnel," and "works with its law enforcement customers to understand their unique needs." *Id.*; *Vigilant Platesearch*, VIGILANT SOLUTIONS, https://www.vigilantsolutions.com/products/license-plate-recognition-lpr/ (last visited Apr. 5, 2020). While law enforcement can purchase physical automatic LPR to outfit their vehicles, the LPR database poses the most Fourth Amendment concerns. *Our Passion*, *supra*. The database contained 5 billion nationwide detections as of February 2017. *See* Press Release, Vigilant Solutions, Vigilant Solutions License Plate Reader Recognition (LPR) Adds 'Extra Set of Eyes' to Improve Sobriety Checkpoint Operation (Feb. 21, 2017), https://www.vigilantsolutions.com/vigilant-solutions-license-plate-recognition-lpr-adds-extra-set-eyes-improve-sobriety-checkpoint-operation/ (advertising that their commercial database contains "more than 5 billion detections"). While the database primarily contains detections shared with Vigilant Solutions from their over-1000 law enforcement agency partners, it is supplemented with commercial data supplied from Vigilant Solutions' sister company, Digital Recognition Network ("DRN"). Brian Shockley, *Vigilant Solutions Enables Over 217,000 Law Enforcement LPR Data Sharing Relationships*, VIGILANT SOLUTIONS (Oct. 23, 2015), https://www.vigilantsolutions.com/vigilant_solutions_enables_217000_law_enforcement_data_sharing_relationships/; *FAQs*, VIGILANT SOLUTIONS, https://www.vigilantsolutions.com/faqs/ (last visited Apr. 5, 2020). One such company that caught flack for their participation with Vigilant Solutions is the Irvine Company, "a real estate company that operates malls and mini-malls" in California. Dave Maass, *California Shopping Centers Are Spying for an ICE Contractor*, ELEC. FRONTIER FOUND. (July 10, 2018), https://www.eff.org/deeplinks/2018/07/california-shopping-centers-are-spying-ice-contractor. Immigration and Customs Enforcement is also a valued customer of Vigilant Solutions. *Id.*

[125] Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 615 (1989); *see also* Brennan-Marquez, *The Constitutional Limits of Private Surveillance*, *supra* note 90, at 506–11 (arguing that *Skinner* represents an "extended infrastructure" reasoning by the Court, through which the Fourth Amendment attaches when a private entity acts as an extension of law enforcement to expand "its infrastructural capability").

[126] The location data market is distinguishable from the reward scenario, at any rate. Any entity (legally) dealing in historical CSLI is perceivably knowable—the data can only come from cell phone carriers, and thus, the distribution of the data can be followed through the agreements and contracts that the cell phone carrier maintains, and so on and so forth. It is not as if a third-party, or law enforcement for that matter, can accidentally discover a cache of historical CSLI.

And like the use of a thermal-imaging device aimed at a home, historical CSLI involves law enforcement "engaged in more than naked-eye surveillance."[127] In *Kyllo*, the Court contended with "what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[128] Limiting Fourth Amendment protection to historical CSLI obtained only from cell phone carriers, like only limiting thermal-imaging to just "intimate" parts of the home, fails "to provide 'a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment.'"[129] And of particular concern to the Court in *Kyllo* was the fact that the thermal-imaging device "is not in general public use."[130] Historical CSLI is analogous: it is surveillance on a level that law enforcement simply cannot match with traditional methods;[131] it is gathered with technology not accessible to the public; and without Fourth Amendment protection extended to instances where law enforcement acquires the data from an entity that did not conduct the initial data collection, it is unworkable in society's modern data sharing practices.

Pervasive state surveillance of the country, unbound without proper Fourth Amendment controls and absent meaningful federal law,[132] also disproportionately affects those with less means. With a significant amount of the country dependent on smartphones to participate meaningfully in today's society,[133] it is not so simple to leave the phone at home or do a

---

[127] Kyllo v. United States, 533 U.S. 27, 29, 33 (2001).

[128] *Id.* at 34.

[129] *Id.* at 38 (quoting Oliver v. United States, 466 U.S. 170, 181 (1984)).

[130] *Id.* at 40.

[131] *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) ("Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user. Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polic[i]es of the wireless carriers, which currently maintain records for up to five years. Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone.").

[132] "Federal law does not directly regulate location tracking or the collection, sale, or use of personal location data." Boshell, *supra* note 26. The closest federal authority governing this area is the Federal Trade Commission, which has brought enforcement actions against location tracking for unfair and deceptive trade practices. *Id.* California recently passed the Consumer Privacy Act ("CCPA"), which provides protection for personal information—including geolocation data. *Id.* The CCPA allows California consumers "to (1) find out what types of location data are being collected and how it is used, and (2) direct companies to (a) delete location data under certain circumstances, and (b) refrain from selling location data to third parties." *Id.* Vermont is the only state to regulate the secondary location data market; the state's law governing data brokers requires "companies that collect or sell 'brokered personal information' regarding an individual that is not a customer of the company" to, among other things, "maintain information security programs and to register annually with the state." *Id.* Vermont's law does not require "data brokers to make disclosures to individuals or provide database opt-outs." *Id.*

[133] Anderson & Kumar, *supra* note 57.

"digital detox."[134] Combined with the fact that the government's surveillance of the poor is "boundless and inescapable,"[135] there are two sets of privacy rights: one for the rich, and one for the poor.[136]

There is also a lack of consent by cell phone users. Harkening back to contract law fundamentals, there is no way for a consumer to negotiate with a cell phone carrier about the amount of credit for a trade-in phone or their internet speed, let alone whether that individual customer will allow the company to sell or share their location data with other companies. There is also the fact that most Americans, nearly 75%, do not read the terms of service or privacy policies they sign.[137]

While most Americans might agree that they are generally subject to some level of surveillance,[138] that should not bear on whether they have an understanding of the particular data collection and subsequent acquisition by law enforcement at play. Indeed, that most Americans—one in six—believe that "their online and offline activities are being tracked and monitored by companies and the government with some regularity"[139] is indicative that any search of historical CSLI is unreasonable. The system is so skewed in favor of law enforcement surveillance and against individual interests that people are resigned to thinking that this is the acceptable status quo.

III. A ROBUST APPLICATION OF *CARPENTER*

If law enforcement acquires historical CSLI to find a suspect, solve a case, or build a database for later use, the answer to the question of what law enforcement must do before acquiring historical CSLI data from a private

---

[134] *See* Shirin Ghaffary, *What's All the Fuss about "Digital Detox"—and Does it Really Work?*, VOX (Jan. 28, 2019, 7:00 AM), https://www.vox.com/2019/1/28/18196379/digital-detox-fuss-about-and-how-does-it-actually-work (describing various methods to lessen a person's reliance on their smartphone, including a "30-day cleanse" in which phone use is cut so that smartphones become "a luxury object, like a fancy bike or high-end blender," app limits that give warnings after using it for a particular time and then stop you from using that app, using "dumb phones" that cannot connect to the internet or withstand heavy app use, a $2,200 retreat to Ibiza where phones are not allowed to be used, professional help in the form of technology addiction therapy, and simply "turning it off"). All the methods outlined in the article pose particular problems and hardships to those who depend on their smartphones for their livelihood, education, transportation, or banking, among many other aspects of modern life.

[135] Danielle Keats Citron, Comment, *A Poor Mother's Right to Privacy: A Review*, 98 B.U. L. REV. 1139, 1142 (2018).

[136] *See* Michele Estrin Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389, 1389–90 (2012) ("[The poor] endure a barrage of information-collection practices that are far more invasive and degrading than those experienced by their wealthier neighbors.").

[137] *See* Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RES. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (finding that only "one-in-five adults overall say they always (9%) or often (13%) read a company's privacy policy before agreeing to it").

[138] *Id.*

[139] *Id.*

entity "is accordingly simple—get a warrant."[140] Functionally, the same warrant barrier should exist if law enforcement is getting historical CSLI directly from the cell phone carrier or from some other third party.

This framework has the ability to be applied to a wide variety of instances in which law enforcement might acquire historical CSLI. Take, for example, Amazon's ever-expanding foray into the private surveillance market. Rekognition is Amazon's facial recognition software that is being rolled out to cities and counties for testing.[141] It is cheap—Washington County pays about $7 a month to search the database—not to mention "easy to activate, [and] requires no major technical infrastructure."[142] The software allows law enforcement to run images collected through traditional means—captured through closed circuit television or pictures taken by police—through a database that provides five possible matches to each search.[143] It is Amazon-specific technology, unlike Ring, a company that Amazon bought in 2018 for more than $800 million.[144] Ring "sells a line of alarm systems, floodlight cameras and motion-detecting doorbell cameras."[145] Ring is primarily marketed to regular consumers as the "new neighborhood watch;" part of the pull of the product is the partnerships Ring has forged with more than 400 police departments.[146] These partnerships allow police to request videos recorded by homeowners' cameras through an application, Neighbors.[147] The Neighbors application "is advertised as a way to receive 'real-time crime and safety alerts' from local law enforcement."[148] Law enforcement can designate a time range and area, and then Ring will "send an automated email to all users within that range, alongside a case number and message from police."[149] Data produced by the Neighbors application has geographic coordinates connected to each post, "accurate enough to pinpoint roughly a square inch of ground."[150]

---

[140] Riley v. California, 573 U.S. 373, 403 (2014).

[141] Drew Harwell, *Oregon Became a Testing Ground for Amazon's Facial-Recognition Policing. But What If Rekognition Gets It Wrong?*, WASH. POST (Apr. 30, 2019, 5:19 PM), https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/.

[142] *Id.*

[143] *Id.* After Washington County began using Rekognition, deputies quickly incorporated it into their "daily beat policing," becoming "prolific users, eager to find a simple resolution to an otherwise-difficult hunt." *Id.*

[144] Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/?arc404=true.

[145] *Id.*

[146] *Id.*

[147] Dell Cameron & Dhruv Mehrotra, *Ring's Hidden Data Let Us Map Amazon's Sprawling Home Surveillance Network*, GIZMODO (Dec. 9, 2019, 3:32 PM), https://gizmodo.com/ring-s-hidden-data-let-us-map-amazons-sprawling-home-su-1840312279.

[148] *Id.*

[149] Harwell, *supra* note 144.

[150] Cameron & Mehrotra, *supra* note 147.

Now, imagine Amazon, with its seemingly infinite resources, acquires a theoretical company with a pre-existing contractual relationship with one of the major cell phone carriers in the United States to round out their private surveillance portfolio. It has access to historical CSLI and leverages that sensitive information with the home surveillance infrastructure created by Ring and the facial recognition software capabilities of Rekognition. The company markets itself as the next great law enforcement partner, combining the various data streams and technology that Amazon has to offer.

A local law enforcement agency contracts with this company and begins using its services to place suspects at crime scenes. There is a series of robberies in a neighborhood; some homes have Ring, and thus capture the face of the suspect. With the facial recognition software, law enforcement is reasonably sure that they have found the right person. But instead of serving a warrant on the suspect's corresponding cell phone carrier to clinch the final piece of evidence to place the suspect at the crime scene, law enforcement is able to verify the suspect using historical CSLI from this company. Using this information, law enforcement arrests the defendant, who is accordingly prosecuted.

Per *Carpenter*, the access of the defendant's historical CSLI from this theoretical company is a search under the Fourth Amendment. Further, the search was unreasonable absent a warrant, and thus, a violation of the defendant's Fourth Amendment rights. Anything gleaned from the unconstitutional search cannot be used to convict the defendant.

In fact, the preferable prosecutorial tool would be for law enforcement to obtain the historical CSLI directly from the cell phone carrier. Courts, prosecutors, and defendants should prefer historical CSLI evidence straight from the source because there is less likelihood of inaccuracies and the added bonus of true verification, rather than a shady workaround. Getting a warrant also has the added effect of prosecutors being more precise with their requests, lest the warrant be denied by the judge, and therefore the company will not divulge more personal information than truly needed. And at the end of the day, this regime might save law enforcement money: using a warrant to get the historical CSLI from the cell phone carrier, instead of spending money to purchase it from a third party. Law enforcement can still purchase third-party technology to analyze the data themselves.

This rule does not foreclose every opportunity for law enforcement to utilize historical CSLI. It does not place an impossible and insurmountable barrier in the way of law enforcement; rather, it is a necessary check against an increasingly powerful and limitless government surveillance apparatus. It also does not address other avenues of law enforcement use of general location data that the *Carpenter* majority avoided in their decision, including: "real-time CSLI or 'tower dumps[,]' . . . conventional surveillance techniques and tools, such as security cameras[,] . . . . [and] other collection techniques

involving foreign affairs or national security."[151] Further, it is entirely possible that in certain cases, warrantless searches of historical CSLI will not tread on the Fourth Amendment by falling into one of the warrant exceptions[152]—but again, this is beyond the scope of this Note.

And while this Note is focused on one potential loophole in the location data market, the protections of historical CSLI across every avenue of law enforcement acquisition have broad implications. It means that historical CSLI is protected absent a warrant—end of story. It is a bright line rule that forecloses law enforcement acquisition of historical CSLI via altruistic collection, but because the data is so "detailed, encyclopedic, and effortlessly compiled,"[153] it needs Fourth Amendment protection against law enforcement.

CONCLUSION

Currently, individual privacy rights in the whole of one's movements are being swallowed by the behemoth that is the private location data industry. Fourth Amendment rights are delicately teetering on the edge of the abyss, despite the Supreme Court's recent efforts in *Carpenter v. United States*. Without a judicial recalibration of the Fourth Amendment that takes into account the realities of how location data is created, monetized, and sold, law enforcement is bound to exploit the loophole left by the Court's piecemeal approach to changes in technology.

The third-party doctrine is unworkable in the Digital Era; the doctrine is of a time before cell phones and the Internet.[154] The Supreme Court is ready to protect historical CSLI information because of the ubiquitousness of the cell phone in modern day life. The risk of government intrusion on the privacies of life is high if law enforcement is allowed unfettered access to historical CSLI, particularly when that access is facilitated by the secondary location data market.

Thus, pursuant to *Carpenter*, law enforcement acquisition of historical CSLI from any entity—and especially from an entity who did not conduct

---

[151] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

[152] *See id.* at 2222 (noting that some warrant exceptions might apply to warrantless access to CSLI, such as exigent circumstances). Another exception likely to be argued is the special needs rule, which provides that law enforcement is allowed to use data or information originally collected for a lawful purpose and not with the intent to aid law enforcement. *See* Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 619 (1989) ("Except in certain well-defined circumstances, a search or seizure in such a case is not reasonable unless it is accomplished pursuant to a judicial warrant issued upon probable cause. . . . We have recognized exceptions to this rule, however, when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.") (internal quotation marks and citations omitted). But again, because the Court is prepared to protect historical CSLI and expressed concerned about actors circumventing constitutional requirements by utilizing third parties, this exception might not apply.

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

[154] And as some legal scholars might say, "STARE DECISIS IS FOR SUCKERS." Leah Litman (@LeahLitman), TWITTER (Mar. 23, 2020, 1:57 PM), https://twitter.com/LeahLitman/status/1242148584071540736?s=20.

the initial data collection—is a search under the Fourth Amendment. Absent a warrant supported by probable cause, the transfer of historical CSLI to law enforcement is an *unreasonable* search, and therefore an unconstitutional violation of the Fourth Amendment if used to convict a defendant.