GOVERNMENT DATA PURCHASES: A CONSTITUTIONAL ISSUE OR PUBLIC COMMODITY?

Emilee Crocker[*]

INTRODUCTION

Data privacy is a national concern.[1] Everyday, millions of people's sensitive cellphone information is being harvested, processed, and sold to unwanted recipients on the data brokerage

[*] Associate Cases Editor (Vol. 93), *Mississippi Law Journal*; J.D. Candidate 2024, University of Mississippi School of Law.

[1] *See* STEPHEN P. MULLIGAN, WILSON C. FREEMAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 2 (2019).

market.[2] Simply put, data brokers are commercial companies bent on collecting, analyzing, and monetizing information about people.[3] The market is worth multibillions, and citizens have unwittingly become cash cows of the industry—generating profits they do not reap.

The public is concerned because the amount of personal data circulating among hands is endless, intrusive, and sensitive. With the increased sophistication of technology, people likewise generate large volumes of easily obtainable "private" data.[4] Smartphone providers promote the use of 5G wireless networks to increase internet connectivity capabilities which likewise increases concerns because interactions with devices generally produce data.[5] For example, simple actions such as checking the weather, using a fitness tracker, surfing the internet, sending an email, and navigating popular social media applications can expose a wealth of information.[6] The generated data may range from (facially) less intrusive meta data[7]—cell phone number, IP address, and location data—to more sensitive information like social security numbers, political preferences, and health data.[8] Many people either do not know their data is being aggregated and sold in such a manner or are unaware of just how much a simple Google search can reveal.

Though marketing all types of private data is generally undesirable, people have recently become particularly concerned with data privacy because brokers have been buying, selling, and trading citizens' location information with the public sector.[9] Accordingly, the government has been purchasing people's chronicled location records from brokers or other third-party

---

[2] MULLIGAN, WILSON & LINEBAUGH, *supra* note 1.

[3] Press Release, *FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices*, FED. TRADE COMM'N (Aug. 11, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices [https://perma.cc/8WRW-RMYA].

[4] MULLIGAN, WILSON & LINEBAUGH, *supra* note 1.

[5] *See Id.*

[6] Dori H. Rahbar, *Laundering Data: How the Government's Purchase of Commercial Location Data Violates Carpenter and Evades the Fourth Amendment*, 122 COLUM. L. REV. 713, 720 (2022).

[7] Ellie Farrier, *What is Metadata: Definition and Meaning*, AVAST (Oct. 10, 2022), https://www.avast.com/c-what-is-metadata [https://perma.cc/QH7T-U2U5].

[8] MULLIGAN, WILSON & LINEBAUGH, *supra* note 1, at n. 224.

[9] *Id.* at 2.

entities without a warrant or probable cause.[10] This means instead of obtaining a court subpoena and forcing companies to hand over their collected data troves, the government writes a check instead. For just a relatively trivial price, the government plays the part of the consumer and enters the private sphere to advance its agencies' purposes.[11] People are concerned because law enforcement is exploiting a loophole in existing privacy laws—peering into their private affairs unimpeded by either judicial or legislative checks.[12]

With the cesspool of marketable location data continuously circulated, readily and easily accessible, the government's overstep needs to be addressed. Traditionally, people's privacy rights were protected from governmental intrusions under the Fourth Amendment and a body of case law developed over the course of the 20th century.[13] This constitutional right, however, does little to shield people's private information from being traded on the private market,[14] the source of governmental data purchases, which is where the root of the issue lies.

This Article discusses how to resolve location data privacy concerns in three core parts: Part I discusses the problem with using the Fourth Amendment to limit technological acquisition of data purchases; Part II discusses the proposal for Congress to promulgate a comprehensive location data regulation at the federal level, the need for the legislature to regulate location data privacy in both a directly and indirectly private capacity, and the specific methods to effectuate criminal enforceability of these regulations; and Part III discusses the relevant Fourth Amendment privacy principles and limitations, an in-depth analysis of the *Carpenter* decision and its applicability to modern electronic surveillance techniques, and the preferability of the legislative solution set forth in Part III.

---

[10] Orin S. Kerr, *Buying Data and the Fourth Amendment*, HOOVER INST. 1 (Nov. 17, 2021) https://www.hoover.org/sites/default/files/research/docs/kerr_webreadypdf.pdf [https://perma.cc/49T4-KZEA].

[11] *Id.*

[12] *Id.*

[13] MULLIGAN, WILSON & LINEBAUGH, *supra* note 1, at 36.

[14] *Id.* at 1.

I. A CONUNDRUM LARGER THAN THE CONSTITUTION

> *"From these, and many other selections which might be made, it is apparent, that the framers of the [C]onstitution contemplated that instrument, as a rule for the government of courts, as well as of the legislature."*[15]
>
> – Justice John Marshall

If a person entrusts another with a secret, and that secret is later exposed, one will normally blame the informer not the informed. In the same sense, when the government purchases someone's information from a third-party source, is it the fault of the government or the company which willfully extended the information? Perhaps a better question would be, who should be regulated, the consumer or the source?

Some scholars have suggested that governmental data purchases of sensitive location information should be regulated under the Fourth Amendment.[16] This is partially right—people's privacy rights do need to be protected—but the amendment is ill-suited for this type of limitation because it is too narrow. The Fourth Amendment restricts the government, but it generally does not impede third parties from independently helping law enforcement, a limitation collectively referred to as the third-party doctrine.[17] This iron-clad rule has been established precedent for decades and specifically states people do not possess rights in records owned and controlled by businesses.[18] There is, however, a narrow exception: *Carpenter v. United States*.[19]

In 2018, the *Carpenter* Court held that compelling wireless carriers to turn over cell-site location information (CSLI) that tracks users' movements for a period of seven plus days constitutes a search and requires a warrant, absent exigent circumstances.[20] *Carpenter* is the backbone of the argument that Fourth Amendment privacy protections should extend and restrict the government's purchase of cellphone location data from data brokers on the

---

[15] Marbury v. Madison, 5 U.S. 137, 179-80 (1803).

[16] *See* Rahbar, *supra* note 6.

[17] *See* United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).

[18] *See Smith*, 442 U.S. at 744-45.

[19] *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).

[20] *Id.*

private market.[21] However, this is imprudent for three main reasons: (1) the Supreme Court decision was narrow; (2) data purchases are distinguishable from the records protected in *Carpenter*; (3) the third-party doctrine limits a Fourth Amendment extension. This Article will discuss this argument in further detail in Part III.

Even if the government is constitutionally limited, data privacy concerns will continue to percolate. Though it is true several enforcement and intelligence agencies have undergone investigation for purchasing citizens' location data, Uncle Sam is not the only consumer of the public's personal information, nor is it even a major player.[22] In fact, various buyers purchase people's data including banks, health insurance companies, prospective employers, and predatory lenders.[23] Big business in particular likes to collect and analyze consumer data to improve product advertisement and internal processes.[24]

People's location data is a commodity in the private sector.[25] When a consumer uses their phone, installed applications subsequently acquire that person's data.[26] Fortune 500 companies including Facebook, Google, Apple, Amazon, Microsoft, and Twitter are just a few companies that regularly and continuously track user locations.[27]

In addition, the data is generally obtained through the user's affirmative action, but consumers are unaware of the true meaning

---

[21] *See* Rahbar, *supra* note 7.

[22] *See* Justin Sherman, *Data brokers and data breaches*, DUKE UNIV. (Sept. 27, 2022), https://techpolicy.sanford.duke.edu/blogroll/data-brokers-and-data-breaches/ [https://perma.cc/HTS8-43F3]. Agencies such as Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), the Drug Enforcement Administration (DEA), and the Federal Bureau of Investigation (FBI) are just a few who have all purchased surveillance products that ultimately rely on the harvesting, transfer, and sale of location data from smartphones. *Id.*

[23] *Id.*

[24] Sudipto Ghosh, *Data Privacy Day: Selected Quotes and Insights from the Industry Leaders- Part 1*, MARTECHSERIES (Jan. 29, 2020), https://martechseries.com/analytics/data-management-platforms/privacy-and-regulations/data-privacy-day-quotes-part-1./ [https://perma.cc/67KH-VVE8].

[25] Paige M. Boshell, *The Power of Place: Geolocation Tracking and Privacy*, AM. BAR ASS'N (Mar. 25, 2019), https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/ [https://perma.cc/787D-MTX9].

[26] *Id.*

[27] *Id.*

of such consent.[28] Smartphone users often consent to applications using their location data for specific location-related purposes like getting directions or tracking miles traveled, or for non-related ones like checking the weather and playing games.[29] What some may not realize is this consent is not limited to the transaction at hand.[30] When a person consents to one application using their location, they are often consenting to an entire industry obtaining access to their private location data. As data trades hands,[31] suddenly hundreds of businesses will come to know where a consenting user has been—even if they have never done business with that company.

Data broker firms exacerbate the problem. This is because their primary purpose is to collect high volumes of a person's data from different sources, aggregate the data, then ship it off to the highest bidder.[32] If the process were a puzzle, then each piece would be a source containing a person's location information, with the broker putting them together. In that sense, the broker may take some person's location information from a location app, some from a social media app, another from a game app, and pretty soon the broker has completed the puzzle and can see every place a person has been over the course of a week. This is concerning because a person's location habits reveal a lot. Just a week's worth of information can reveal a person's "lifestyle, priorities, professional and personal endeavors . . ."; "[it] can all be inferred from continuous location tracking."[33] Brokers like to advertise their practices are safe because they anonymize people's packaged

---

[28] Boshell, *supra* note 25 (noting there is evidence which suggests otherwise, which is also problematic).

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *See id.* ("The purpose of the initial collection of location data is to enable the data collector to provide a service to the individual; the secondary market purpose is to use that same location data to make conclusions and predictions about the tracked individual. The secondary location data market is used to monetize location data for unrelated purposes, such as enabling a subsequent buyer to compile a profile of the individual and sell access to the individual (whether the individual is identified by name or as part of a data category, like 'engaged female retail shopper').").

[33] *Id.*

location data before they ship it off.[34] However, location data can be deanonymized easily, which is problematic.[35]

Ultimately, the root of the issue is the lack of federal regulation of the data trading industry.[36] Though federal and state data privacy laws do exist, most of them regulate entities with a direct relationship to consumers and only for certain subcategories of data. Because data brokers are in secondary possession of sensitive personal location information, they are relatively unimpeded from selling it, and trading the information to other entities like law enforcement is fair game.[37] Due to this, the government has been legally unhindered from buying and selling information from businesses that have amassed people's sensitive data.[38] In some instances, law enforcement agencies have brokered and sold or traded the data themselves.[39]

Governmental data purchases and data privacy are not just a civil concern—criminal enforceability should also be considered. Recently, the Department of Justice (DOJ) determined that if the location information is anonymized, the Fourth Amendment *Carpenter* case is not a basis for prosecuting companies under the Stored Communications Act (SCA).[40] Civil law itself allows this sort of transaction, so, without *Carpenter*, there is little basis for criminal liability for companies allowing warrantless data purchases. Since *Carpenter* is not a basis to impose either civil or criminal liability for selling to the government, this reinforces the overwhelming need to promulgate strong data privacy protection

---

[34] Boshell, *supra* note 25.

[35] *Id.* ("[T]he use of multiple systems to track location, and the use of data analytics to combine location data with other personal data, enables . . . both the identification of anonymous data and the compilation of comprehensive and precise profiles of tracked individuals.").

[36] MULLIGAN, WILSON & LINEBAUGH, *supra* note 2, at 1.

[37] *See* FED. TRADE COMM'N, *Data Brokers*: *A Call for Transparency and Accountability* (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/85FG-VJVS].

[38] Justin Sherman, *Data Brokers Are Advertising Data on U.S. Military Personnel*, LAWFARE (Aug. 23, 2021, 8:01 AM), https://www.lawfaremedia.org/article/data-brokers-are-advertising-data-us-military-personnel [https://perma.cc/8KLD-K4Z8].

[39] FED. TRADE COMM'N, *supra* note 37, at 11.

[40] *Sharing Cyberthreat Information Under 18 USC § 2702(a)(3)*, DEP'T OF JUST. (Mar. 26, 2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/03/26/guidance-for-ecpa-issue-5-9-2014.pdf [https://perma.cc/7DF5-RCJF].

laws for non-content data like location information. Broad data privacy concerns call for a comprehensive solution.[41]

II. COMPREHENSIVE LOCATION DATA REGULATION—A LEGISLATOR'S DUTY

Carpenter is a classic example of the judiciary's effort to fit a square peg in a round hole. Rather than continue to force a centuries-old search doctrine to conform to the modern investigative techniques, the problem would be better addressed on the legislative level.

This Article proposes the court forgo extending Fourth Amendment privacy protections over electronic surveillance. Instead, legislators should promulgate rules targeted toward limiting the selling of people's sensitive location information on the broker market. Directly policing the government's source of information will thereby indirectly regulate the government's intrusions, killing two birds with one stone.

Specifically, Congress should pass a federal law protecting location data.[42] Cellphone data is unique in that it does not have a confined border. With just the click of a button, information can cross from one state to another or even across the world. Because data is ubiquitous,[43] its regulation should also be broad-based. Recently, Senator Elizabeth Warren introduced the Health and Location Data Privacy Act of 2022 (the "Bill"), a Senate bill which limits data brokers from transferring and selling certain sensitive

---

[41] Note a comprehensive set of federal regulations broadly preventing data trading would be ideal, but it also requires Congress to consider several legal questions, including whether there should be a "conceptual framework of the law (i.e., whether it is prescriptive or outcome-based), the scope of the law and its definition of protected information . . . ." MULLIGAN ET AL., *supra* note 1. Federal regulations also raise the unique issue of potential federal preemption, whether and how it should be applied, which is outside the scope of this Comment. This Comment focuses on a specific subcategory of data privacy concern (location data) and addresses a few targeted improvements to be considered when drafting location data privacy law.

[42] Ultimately Congress needs to enact legislation protecting all types of data. "Points of consideration may include the conceptual framework of the law (i.e., whether it is prescriptive or outcome-based), the scope of the law and its definition of protected information, and the role of the FTC or other federal enforcement agency." MULLIGAN ET AL., *supra* note 1. However, this falls outside the scope of this paper.

[43] Boshell, *supra* note 25.

data, specifically health and location data.[44] This Bill sets up a solid framework for resolving the location data privacy issue, but there are some adjustments that could ensure an even more airtight regulatory seal.

This Article proposes the Bill be amended with three main provisions: (1) "data broker;" should be defined under the Federal Trade Commission's (FTC) definition; (2) data brokers must provide informed notice to consumers and clear instruction to the FTC on how they collect, process, and protect people's personal information in order to deepen the technological understanding behind data collection and help target problem areas in data privacy promulgation; and (3) along with civil enforceability, brokers should also be criminally liable for unlawfully buying, selling, trading, and licensing people's location data to ensure organizations remain compliant.

A. A Broad Definition

Data brokerage cannot be completely eradicated. Why? Well, for one, there is a lot of money in the industry—billions in fact.[45] In 2021, the market size of the industry was around 250 billion, with the United States part of the leading share of the data brokers market.[46] This includes data used for a wide range of purposes including retail & e-commerce, healthcare, IT and Telecom, media, government, etc.[47] And the industry is only expected to grow.[48] By 2031, the market is predicted to nearly double in size.[49]

In addition, data collection is not entirely bad. In fact, several entities have recognized the positive impact of data trading,

---

[44] *See* S. 4408, 117th Cong. (2022).

[45] *Data Brokers Market Estimated to Reach US$ 462.4 billion by 2031, TMR Report*, GLOBENEWSWIRE (Aug. 1, 2022, 10:30), https://www.globenewswire.com/news-release/2022/08/01/2489563/0/en/Data-Brokers-Market-Estimated-to-Reach-US-462-4-billion-by-2031-TMR-Report.html [https://perma.cc/Q343-9NPD] [hereinafter *TMR Report*].

[46] *Id.*

[47] *Id.*

[48] *Id.* ("TMR estimates the data broker market to expand at a CAGR of 6.8% during the forecast period from 2022 to 2031. Rapid adoption of business intelligence (BI) solutions from a range of industries including finance and healthcare to analyze large data sets and obtain actionable insights for competitive advantage fuels the growth of data brokers market.").

[49] *Id.*

especially location data.[50] For example, this information can "help urban planners alleviate traffic problems, health officials identify patterns of epidemics, and governmental agencies monitor air quality."[51] In the same vein, the data is also beneficial in the commercial sector for service availability and demand, offering insights on internal improvements.[52]

Regulatory data laws do exist, though they are imperfect. There are a number of state and federal privacy laws regulating data practices.[53] Federal statutes that generally protect people's data include the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, Children's Online Privacy Protection Act, and others.[54] Several agencies such as the Federal Trade Commission, the Consumer Finance Protection Bureau (CFPB), and the Department of Health and Human Services (HHS), ensure the laws are being enforced.[55] But these laws are limited because they are sector specific and only regulate certain categories of data and cannot be applied to others.[56] Therefore, despite the existence of so many privacy laws, personal location data generally falls through the cracks of statutory protection and can be sold unimpeded to virtually anyone, whether for nefarious or legitimate reasons.[57]

To ensure people's location information is protected, the definition of data brokers should be broad. The legal definition of data brokers is important because it has resulted in a disproportionate number of entities falling outside the scope of state and federal privacy laws.[58] In other words, there is a

---

[50] Boshell, *supra* note 25.

[51] *Id.*

[52] *Id.* ("Commercial uses of aggregated location data include inventory and fleet control, retail location planning, and geofencing. Specified data points may be aggregated over a defined time period and then presented as an overlay to a geographic map. For example, a trucking company can view in real time the locations of its trucks and the demand for trucking services to more efficiently assign routes. Alternatively, the trucking company can geofence its trucks, which means that if a truck goes out of a designated geographical zone, the company will be alerted in real time. Location data is critical to certain types of commercial and public data analytics.").

[53] *See* MULLIGAN ET AL., *supra* note 1, at 7.

[54] *Id.* at 8-10.

[55] *Id.*

[56] *Id.*

[57] *See Id.*

[58] *See* MULLIGAN ET AL., *supra* note 1, at 8-10.

significant amount of data trading by entities whose sole purpose is not brokering data.

Of course, brokers are difficult to fit under a single legal definition.[59] Data brokers are difficult to define because, depending on the type of data acquired, the procurement methods at their disposal, and the purposes for obtaining the data, brokers operate differently. For example, some companies are formed entirely for brokerage purposes; others collect and sell the data as a secondary interest.[60] Likewise, brokers sell data to a wide variety of consumers in the public and private sector—even foreign entities.[61]

Consider the legal definition of data brokers in Vermont.[62] The state defines data brokers as firms which have the primary purpose of selling, trading, or licensing data.[63] Effectively, this definition is too narrow because it excludes all other companies that broker as a secondary interest, and therefore may bypass the state brokerage requirements and regulations.[64]

The 2022 Bill provides a similar, nearly verbatim, definition of data brokers to the Vermont definition: "The term 'data broker' means a person that collects, buys, licenses, or infers data about individuals and then sells, licenses, or trades that data."[65] To remedy this constricted interpretation, the Bill should adopt the FTC's definition of data brokers. In 2014, the FTC released a report on the industry defining data brokers as "companies that collect consumers' personal information and resell or share that information with others . . . ."[66]

The FTC definition is more suitable than the Vermont and 2022 Bill definitions because it does not distinguish between a company whose primary goal is to broker data and companies that broker as a secondary interest.[67] It also does not exclude companies

---

[59] *See* FED. TRADE COMM'N, *supra* note 37, at i.

[60] *Id.* at 40.

[61] Sherman, *supra* note 38.

[62] VT. STAT. ANN. tit. 9, § 2430 (West 2020).

[63] Justin Sherman, *Federal Privacy Rules Must Get "Data Broker" Definitions Right*, LAWFARE INST. (Apr. 8, 2021, 11:00 AM), https://www.lawfaremedia.org/article/federal-privacy-rules-must-get-data-broker-definitions-right [https://perma.cc/A4AM-CCP8].

[64] *Id.*

[65] S. 4408, 117th Cong. § 4 (2022).

[66] FED. TRADE COMM'N, *supra* note 37.

[67] Sherman, *supra* note 63.

that sell data to their direct consumers.[68] In this sense, the big tech powerhouse Google would be considered a broker if it sold location information to a third-party, whether the government or other entity.[69] Furthermore, this extends to a company selling data collected by a subsidiary, such as Amazon and its e-commerce platforms.[70]

In addition, the definition is promising because it limits companies that "resell" data.[71] This is important because it encompasses entities that obtain already pre-packaged data.[72] This means if a broker or other entity collects and aggregates the data then sells it to a business, that business would legally qualify as a broker if it resold the data to another.[73] Moreover, the FTC's use of "share," and not just selling is important.[74] This is because many entities share data through agreements extending beyond just buying and selling.[75]

The effect of data brokerage can be pictured as a drop of water suspended over a chain of multi-colored links. The drop is the packaged data, the chain the private market, with each link representing a different entity within the market depending upon the color. When the drop falls and flows freely down the chain and between links, each link that touches the water is a broker.

Ultimately, the FTCs definition is broader because it considers the entire network of data sharing rather than narrowed market practices included in the Bill's definition. To ensure an all-encompassing, direct and indirect, regulation, it is important to maintain a broad definition of brokers.

B. Transparent Practices

Acxiom Corporation, Equifax Inc., Oracle Corporation, Moody's Corporation, FICO, LexisNexis, Experian Plc, CoreLogic, Epsilon, eBureau, Intellius — do these companies sound familiar?[76]

---

[68] Sherman, *supra* note 63.
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] Sherman, *supra* note 63.
[75] *Id.*
[76] *TMR Report*, *supra* note 45.

In fact, they are at the top of the broker industry—key players which aggregate and anonymize people's data and sell for profit or other purposes. Ironically, one of the players, LexisNexis, generally advertises itself as a legal research database.

Lexis is a prime example of how most location data trading mechanics and its actors are a mystery to the general public. Data privacy concerns are high because people tend to fear what they do not know. Only recently have a few come forth and explained how they obtain people's cellphone information, and their data collection methods are alarming.[77] The sheer volume of data collected, the way its processed, and the purposes for collection are complex and thereby make it extremely difficult to promulgate a legal plan.[78]

The data broker industry is intricate. Perhaps because they fundamentally operate beyond the private eyes, collecting people's personal information behind tech "advertising," their methods are similarly unknown.[79] In its simplest form, the chain of location data may generally flow as follows: (1) from a person's cellphone or mobile device to (2) a third-party company servicing the phone to (3) a secondary entity, such as brokers, to analyze and sell to other brokers, businesses, or the government.[80] As far as their role in the public market, licensed data brokers (entities whose *primary* interest is to collect data and sell for profit) function as a middle-man in the supply chain of location data.[81]

To exemplify this process with Step (1) to (2) alone, consider an interaction with Google Maps on a cellphone.[82] A person inputs an address into the application and a dialog box appears on the device's screen requesting consent for the user's location.[83] The person has two choices: (a) decline consent and manually input a start and end address for the application to route or (b) consent and allow the map to tracks their initial real-time location.[84] For

---

[77] Boshell, *supra* note 25.

[78] *Id*.

[79] *Id*.

[80] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), http://ftc.gov/os/2012/03/120326privacyreport.pdf [https://perma.cc/G7BU-5MHU].

[81] *Id*.

[82] Boshell, *supra* note 25.

[83] *Id*.

[84] *Id*.

convenience, people tend choose option (b) and consent to the application using their location.[85] When that happens, the application will use either Global Positioning System (GPS) or its equivalent to determine the person's starting location.[86]

Subject to a non-disclosure agreement, the service provider for the phone often transmits the location to a third-party entity, which then transmits the data to the application, Google Maps.[87] Strangely enough, this third party is akin to a service provider for one's service provider. Its services are to provide location information to a service provider like AT&T, but it may also send information to the application upon request. The purpose is to send directions to the person and, therefore, efficiently complete the transaction, effectively ending the two's (third-party and application) interactions.[88] With the non-disclosure agreement, the flow of the person's location information should stop there.[89] However, sometimes, it is not that simple.

This example was only one of many ways in which data passes between entities. The third-party company which sends the location information to the application may have agreements with other companies to pass the information along and vice versa.[90] Essentially, information can be passed directly from an application service on a person's phone, from a third party that furnishes the phone's service such as in the example, from unauthorized third parties which may steal the information through data breaches or purchase from consented carriers.[91]

The data broker industry—where brokers secondarily acquire the location information from other companies to analyze and sell to other brokers, businesses, or the government—is where the practices get shaky, and lawless trading may arise.[92] As mentioned, data is money, and the location data market is relatively unregulated. Businesses are willing to sell because it is legal, and the inherent purpose of a business is to make money. Take the third

---

[85] Boshell, *supra* note 25.
[86] *Id.*
[87] *Id.*
[88] *Id.*
[89] *Id.*
[90] Boshell, *supra* note 25.
[91] *Id.*
[92] *Id.*

party from the Google Maps example. There is evidence that it and other similar entities "routinely sell location data to a series of parties that are not intermediaries to the initial data transaction, leading to dissemination of location data beyond its intended purpose, and resulting in unrelated third-party access to the individual's location data."[93] What this means is, when a person consents to one application using their location, they are often consenting to an entire industry obtaining access to their private location data.[94]

LocationSmart is an example of this type of third-party entity that, without a direct relationship to the consumer, nonetheless maintains authority over consumers' location information through consent from a phone's service provider.[95] LocationSmart provides various location services for several devices, including cellphones, to some pretty big names, such as AT&T, Verizon Wireless, T-Mobile US, and Sprint Corporation.[96] Essentially, they help the companies more accurately pinpoint people's locations for better service efficiency.[97] LocationSmart was sued for selling people's location records it had compiled for the Big-Name service providers to the government.[98] This meant everyone with AT&T servicing their phone may have unwittingly had their location information sold to the government.[99] No consent was required, and there was no way to opt-out.[100]

Many businesses like LocationSmart may advertise that their practices are safe because they aggregate and anonymize people's location data. Aggregate means the brokers take each piece of data collected from different sources—some of which only provide a few data points about a consumer's activities—and assemble them into a detailed and composite record of a phone's location routes.[101] Anonymized means the information is made "impractical or even

---

93 Boshell, *supra* note 25.
94 *Id.*
95 *Id.*
96 *Id.*
97 *Id.*
98 Boshell, *supra* note 25.
99 *Id.*
100 *Id.*
101 *Id.*

impossible . . . to reidentify."[102] However, investigation into these practices has revealed that this it is a little more complicated than that.[103]

Deanonymization is not very difficult. Essentially, if one obtains a chronicled, time-stamped record where an unidentifiable person has traveled throughout the day, it may not tell much. However, if the records contained their whereabouts over the course of a few days, it would probably tell a lot—their morning work commute, when they eat, where they live, etc. With several more days' worth, it would not be hard to develop a working profile over this person's entire lifestyle. This is why location information is so sensitive. People want to ensure their data does not fall into the wrong hands because, if that happens, their private lives will be essentially laid bare for the purchaser to see.

As mentioned, data trading is profitable and can be beneficial.[104] But, at the end of the day, data is private and needs to be protected. Therefore, to ensure brokers are maintaining ethical and compliant practices, licensed brokers should be transparent with their methods and submit clear instruction to users on how they collect, process, and protect people's personal location information.[105] This will also have the added benefit of increasing the tech literature and help in the promulgation of more data privacy laws because it is more effective to regulate entities if one knows how they operate.

C. Criminalizing Unlawful Data Use

Along with the provisions to the Bill discussed in Sections A and B of Part II of this Article, Congress should legislate the bill to criminalize brokers which unlawfully use people's data, particularly entities that sell data to a governmental agency that has neither a warrant nor probable cause.

The Bill explicitly reserves authority to the FTC for enforceability: "[T]he Commission shall enforce section 2 [enforceability] in the same manner, by the same means, and with

---

[102] Silvio Sampaio, et al., *Collecting, Processing and Secondary Using Personal and (Pseudo)Anonymized Data in Smart Cities*, 13 APPLIED SCI. 3830, 3834 (2023).

[103] Boshell, *supra* note 25.

[104] *Id.*

[105] *Id.*

the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act."[106] Provisionally, the Senate should amend the Bill with a simple clause permitting the FTC as the federal agency in charge of enforcement to discretionarily refer matters the DOJ. This would thereby allow the DOJ to then criminalize unfair broker conduct through the SCA.[107]

The SCA is a relevant source of authority because it directly overlaps and penalizes misuse of the subject matter at issue here: cellphone data.[108] Under 18 U.S.C. § 2510, the SCA defines electronic communication as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part . . . that affects interstate or foreign commerce . . . ."[109] Location data qualifies as an electronic communication under the Act.[110]

18 U.S.C. § 2702(a) imposes criminal liability upon service providers for voluntarily disclosing location records to third parties.[111] Specifically, § 2702(a) says the following:

---

[106] S. 4408, 117th Cong. § 3 (2022).

[107] DEP'T OF JUST., *supra* note 40. *See also* Stored Communications Act, 18 U.S.C. 2701 et seq. (2018).

[108] DEP'T OF JUST., *supra* note 40.

[109] 18 U.S.C. § 2510.

[110] DEP'T OF JUST., *supra* note 40.

[111] 18 U.S.C. § 2702 (2018).

> (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
>
> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—
>
> > (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
> >
> > (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and
>
> (3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.[112]

Section 2702 is limited to cellphone service providers. Specifically, the section prohibits any service which helps phones send and receive signals.[113] This means the SCA only imposes criminal liability upon companies that have a direct relationship with the consumer, thereby excluding data brokers and other third-party companies that may obtain unauthorized access to people's information.[114] This is problematic because the broker industry pipeline is where most of the lawless location data trading takes place, and where criminal liability also needs to be imposed.

---

[112] § 2702 (2018).
[113] *Id.*
[114] *Id.*

There is a possible improvement, at least for preventing governmental purchases of location data. Note that under § 2702, the requisite mens rea is that the criminal *knowingly* shares information.[115] Some scholars have suggested the mens rea element for § 2702(3) should be amended to include knowingly, either directly or indirectly.[116] This seems right because it imposes a duty upon service providers not to give people's location information to entities they reasonably believe would pass the information on to the government, thereby preventing indirect transfer of data. Though it does not specifically impose liability upon brokers, it does deter consumer companies from giving people's sensitive information to brokers which sell to the government, thereby indirectly regulating them. The service provider would shoulder criminal enforcement for the actions of others. Brokers would still be allowed to continue their practices, directly undeterred. However, their source would more tightly regulate their location information. Ultimately, with the sheer size of the broker industry, this would be a "band-aid" fix.[117] Brokers have a number of sources to compile data from, and a broader reformation of the SCA is desirable.

Furthermore, criminal enforceability for unsavory broker behavior is appealing for its deterrent effect. Most of the companies trading in the broker industry are profiting up to billions of dollars, so civil penalties seem to be a moot point unless they are significant. Generally, incarceration is enough to make anyone, especially white-collar entities, stop in their tracks. Incarceration is a sensitive topic and is not a tool for abuse, and the punishment for a crime should be justified and proportionate to the crime committed, but criminalizing data brokerage is justified.

There are incarceration penalties for voluntary disclosure, and the DOJ should amend § 2702 to include similar penalties granted in § 2701. Penalties for violating § 2701 can be dealt in three ways. First-time violations committed for purposes other than commercial or criminal furtherance include a maximum of one year imprisonment and a $100,00 fine.[118] In the event there is a repeat

---

[115] § 2702 (2018).

[116] Rahbar, *supra* note 6, at 751-52.

[117] *Id.* at 752.

[118] *See* 18 U.S.C. § 2701(b)(2)(A); *see also* 18 U.S.C. § 3571(b)(5).

violation for the same purpose, then the maximum penalty is five years and a $250,000 fine.[119] Finally, for repeat violations "for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act," the maximum penalty is ten years and $250,000 fine.[120]

In this case, the penalties for exposing people's sensitive information is justified for deterrence as well as for retributive purposes. The internet is forever. Once a person's information is circulating on the market, it is nearly impossible to completely erase it. Particularly in cases where someone's location information was deanonymized and their identity exposed, there can be adverse effects. Brokers tend to aggregate the location data with others in order to build a complete profile of a person and their lifestyle.[121] This can include all types of sensitive information such as their marital status, income, and social security number.[122] When that information, along with their comings and goings, become available, predators then have the perfect roadmap on when, where, and how to take advantage of vulnerable targets to advance their criminal purposes. An entity that knowingly gives others this access in exchange for money should be punished accordingly.

Moreover, imposing criminal liability would align with some of Congress's intended purposes for the law.[123] Congress drafted § 2702 drafted with the motivation to safeguard people's information from being misused and abused.[124] Businesses should handle private information as if it was their own trade secrets. It is not unreasonable to request that companies protect information because to do so is in the interest of the general public. People should live without fear of unwanted and inexhaustive scrutiny. Citizens may have the option to forgo technological use, but this is an unrealistic choice. Phones are an integral part of life in modern society, heavily integrated into one's work and personal livelihood—to live is to generate data. As such, companies which

---

[119] *See* 18 U.S.C. § 2701(b); *see also* 18 U.S.C. § 3571(b)(3).
[120] *See* 18 U.S.C. § 2701(b); *see also* 18 U.S.C. § 3571(b)(3).
[121] Boshell, *supra* note 25.
[122] *Id.*
[123] DEP'T OF JUST., *supra* note 40.
[124] *Id.*

handle their sensitive data information should be deterred from treating others' information with anything but the utmost care.

Realistically, imposing criminal liability in a broad capacity would take significant reform on the DOJ's side, amendments which are also in some tension with Congress's original purpose for the law.[125] Originally, the SCA was intended to be strict on content such as email communications but less stringent on non-content like location data.[126] But the Stored Communications Act has not been meaningfully amended since its enactment in 1986.[127] Technology has changed significantly since then, and it would be wise for the DOJ to consider some legislative alterations.

Ultimately, promulgating comprehensive data privacy legislation is a necessary prerequisite to incentivize some much-needed amendment to the SCA and impose criminal liability. Recently, the DOJ determined if the location information is anonymized, the Fourth Amendment *Carpenter* case is not a basis for prosecuting companies under the SCA.[128] There are some holes in this argument because, as discussed in Part II.B, it is very easy to deanonymize data. Regardless, as discussed in Part IV, the DOJ is right that *Carpenter* does not protect location data purchases. Civil law itself allows this sort of transaction, so without *Carpenter*, there is little basis for criminal liability for companies allowing warrantless data purchases. This reinforces the overwhelming need to promulgate strong data privacy protection laws for non-content data like location information.

III. DATA PURCHASES ARE NOT A FOURTH AMENDMENT CONCERN

In light of public concern and the DOJ's determination, this Part discusses the relevant Fourth Amendment privacy principles and limitations, an in-depth analysis of the *Carpenter* decision and its applicability to modern electronic surveillance techniques, the

---

[125] DEP'T OF JUST., *supra* note 40.

[126] *Id.*

[127] Elizabeth Goitein, *The government can't seize your digital data. Except by buying it.*, WASH. POST (Apr. 26, 2021, 6:00 AM), https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/ [https://perma.cc/4VS3-AQ8F].

[128] *Id.*

distinction between *Carpenter* protected records and data purchases, and reinforces the preferability of the legislature to regulate data privacy in both a directly private and indirectly public capacity and to incentivize improvement in criminal law. It argues that warrantless data purchases on the public market are not searches under Fourth Amendment principles, underlines technology changes so rapidly that courts should decline using the Fourth Amendment against governmental digital intrusions and leave the *Carpenter* holding as it was intended to be—narrow. Ultimately, it emphasizes the Fourth Amendment should not be extended and reinforces the idea that it is Congress's duty to enact proper regulations regarding public cybersecurity and privacy laws limiting the use of people's sensitive location data.

A. Relevant Fourth Amendment Principles

Under the Fourth Amendment, U.S. citizens are protected from the government's unreasonable searches and seizures of their "persons, houses, papers, and effects . . . ."[129] Essentially, the Amendment is intended to protect citizens "against arbitrary invasions by governmental officials."[130]

For the government's data purchases to be considered under Fourth Amendment privacy protections, the acquisition would have to constitute a search; the most complicated and contextually relevant point of Fourth Amendment law.[131] Simply put, if data purchases do constitute a search, then the government needs a warrant or probable cause to obtain people's location data.[132] Traditionally, the court's main concern with the search doctrine involved whether law enforcement physically, with subjective intent to obtain information, intruded upon a constitutionally protected area.[133] In other words, did the government trespass upon property?

---

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

[130] Carpenter v. United States, 585 U.S. 296, 302-03 (2018) (quoting Camara v. Mun. Ct. of City & Cnty. of San Francisco, 387 U.S. 523, 528 (1967)).

[131] *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

[132] *Id.* at 336.

[133] *Carpenter*, 585 U.S. at 304 (citing United States v. Jones, 565 U.S. 400, 405, 406, n. 3 (2012)).

Ultimately, property interests have been put on the backburner in favor of privacy interests as far as Fourth Amendment search claims are concerned.[134] In *Katz v. United States*, the Supreme Court held that a search occurs if law enforcement examines a place or thing in which a person possesses a reasonable expectation of privacy.[135] The Court created the reasonable expectation of privacy test because "the Fourth Amendment protects people, not places."[136] Typically, the test is a two-part inquiry that asks (1) whether a suspect subjectively has an expectation of privacy and (2) whether that subjective expectation is also objectively reasonable to society.[137]

Of course, there have been several cases that establish where people have a reasonable expectation of privacy. For example, people generally have a reasonable expectation of privacy in their own person such as articles on or adjacent to their bodies—purses, wallets, backpacks, jackets, etc.—or everything not plainly visible such as one's internal organs.[138] In addition, people have a reasonable expectation of privacy in private, enclosed spaces such as their homes.[139] Typically, the court considers the home to be where a person has the greatest expectation of privacy and thus the strongest constitutional protection.[140] It is the governmental intrusion upon private areas and similar spaces that result in searches under the Fourth Amendment.

---

[134] *Carpenter*, 585 U.S. at 304.

[135] Katz v. United States, 389 U.S. 347, 353 (1967); *See also Carpenter,* 585 U.S. at 304.

[136] *Katz*, 389 U.S. at 351-52; *see also Carpenter*, 585 U.S. at 304.

[137] *Katz*, 389 U.S. at 347 (Harlan, J., concurring); *see also Carpenter*, 585 U.S. at 345 (Thomas, J., dissenting).

[138] *See* New Jersey v. T.L.O., 469 U.S. 325 (1985) (holding that a student has a reasonable expectation of privacy in regard to their purse); United States v. Dionisio, 410 U.S. 1, 4 (1973) (citing Davis v. Mississippi, 394 U. S. 721, 724-728 (1969)) ("The Fourth Amendment prohibition against unreasonable search and seizure applies only where identifying physical characteristics, such as fingerprints, are obtained as a result of unlawful detention of a suspect, or when an intrusion into the body, such as a blood test, is undertaken without a warrant, absent an emergency situation.").

[139] Silverman v. United States, 365 U.S. 505, 511 (1961) ("The Fourth Amendment, and the personal rights which it secures, have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.").

[140] *Id.*

However, when the test does fail, it will generally do so under the second prong. For instance, a person may subjectively believe that having a conversation on a crowded bus at rush hour is private, thereby satisfying the first element of the test. However, most would agree that expectation is unreasonable because the other people on the bus, the public, could overhear the conversation and are also arguably privy to that information. Thus, if a government actor eavesdropped on the conversation, the content would not be protected from the government's use under the search doctrine.

Likewise, there is no objectively reasonable expectation of privacy in places or items exposed to the public such as people's trash bags left on the curb,[141] abandoned items,[142] or spaces a person has consented to be searched.[143]

B. The Third-Party Armor & the Willing Seller Shield

Ultimately, data purchases are not traditional searches under the Fourth Amendment because of the third-party doctrine. One of the strongest limitations of the Fourth Amendment are the holdings from *Smith*[144] and *Miller*,[145] collectively known as the third-party doctrine. The third-party doctrine says a person does not have a reasonable expectation of privacy in information voluntarily given to a third party[146] or the business records created, owned, and controlled by a third party.[147] This is true even if the

---

[141] *See* California v. Greenwood, 486 U.S. 35 (1988) (holding that the police's warrantless search and seizure of the defendant's trash bags left for collection did not violate the Fourth Amendment).

[142] Abel v. United States, 362 U.S. 217, 241 (1960).

[143] *See* United States v. Matlock, 415 U.S. 164 (1974) (holding that a third party's consent can supplement that of the defendant's when the third party shares possession or common authority of the subject property).

[144] *See* United States v. Miller, 425 U.S. 435 (1976) (holding that defendant's bank records were not subject to Fourth Amendment protections).

[145] *See* Smith v. Maryland, 442 U.S. 735 (1979) (holding that defendant's phone records possessed by the telephone company were not subject to Fourth Amendment protections).

[145] *Id.*

[146] *Miller*, 425 U.S. at 443; *see also Smith*, 442 U.S. at 743-44.

[147] *Miller*, 425 U.S. at 445; *see also Smith*, 442 U.S. at 744.

records contain sensitive personal content such as bank, telephone, and certain credit information.[148]

The Court has noted, however, that the sole act of sharing the information is not the only factor to take into account.[149] The "nature of the particular documents sought," is also considered.[150] For example, in *Smith,* the Court determined information gleaned from pen registers have limited capabilities.[151] Their capabilities are limited because they do not reveal any particular identifying information about a person.[152] Acquiring someone's call log is considered *mildly* intrusive or not as personal. Therefore, with the diminished privacy protections under the third-party doctrine, they failed to trigger the Fourth Amendment.[153] The rationale for the third-party doctrine was if a person knowingly shares information with another, there is a reasonable expectation that information has reduced privacy protections.[154] People generally have little to no control over the autonomy and actions of others.[155] This idea is only fortified through the willing seller rule.[156]

The willing seller rule concerns companies and their right to voluntarily sell business records. Generally, people do not have any Fourth Amendment rights to business records, even if that information concerns themselves.[157] This is because companies created the records and control them and therefore have common authority over the business records.[158] Since the Fourth Amendment generally offers no relief for the actions of people other than governmental actors, people are out of luck if third parties

---

148 *Miller*, 425 U.S. at 443 ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."); *Smith*, 442 U.S. at 744.

149 *See* Carpenter v. United States, 585 U.S. 296, 308 (2018) (citing *Miller*, 425 U.S. 435 (1976)).

150 *Miller*, 425 U.S. at 442.

151 *Smith*, 442 U.S. at 742.

152 *Id.* at 741.

153 *Id.*

154 *Carpenter*, 585 U.S. at 314.

155 Kerr, *supra* note 10.

156 *Id.*

157 Kerr, *supra* note 10, at 3.

158 *Id.* at 4.

reveal their information to the government.[159] These implications in regard to data purchases will be discussed further in Sections D and E.

C. The Mosaic Theory: An Evolution of the Search Doctrine Approach

Ultimately, the search doctrine approach has become muddled concerning technologically compiled location data. In 2014, renowned Professor Orin Kerr wrote a famous Fourth Amendment journal article in response to the release of the *Jones v. United States* opinion which established protections against law enforcement's warrantless placement of a GPS tracking device on a person's vehicle.[160] In his article, he detailed the Fourth Amendment's imperfect application to digital investigatory methods.[161]

Dubbed the Mosaic Theory of the Fourth Amendment, Kerr discussed court's likelihood to shift the traditional Fourth Amendment "sequential" search approach to a "mosaic," type of approach in regard to technology.[162] Essentially, Kerr explained the sequential approach regarded traditional determinations of a Fourth Amendment search—looking at particular governmental acts at a specific point in time to determine whether a search occurred.[163] In contrast, the mosaic approach simply means that rather than a snapshot of government action, the Court will consider the entirety of information gleaned over a period of time.[164]

In other words, it is the pervasiveness of the government action—information obtained over a long period of time—that matters with the mosaic approach. To clarify, an individual's location at a particular place and time is analogized as a piece of

---

[159] *See* United States v. Karo, 468 U.S. 705, 732 (1984) (holding one who purchases property assumes the risk that the seller has permitted the police to install a tracking device on it. However, continuous and pervasive monitoring the tracking information such that the police learn the layout of private spaces constitutes a Fourth Amendment search).

[160] *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

[161] *Id.*

[162] *Id.*

[163] Kerr, *supra* note 160, at 316-17.

[164] *Id.* at 320.

mosaic.[165] By itself, one can glean nothing more than what that particular piece shows.[166] However, when there are multiple pieces, and the parts are fit together, the meaning becomes something else entirely.[167] Rather than focusing on the individual pieces that make up the mosaic, one focuses on the entirety of the picture.[168] Similarly, if the government's surveillance method allows it to see a picture or mosaic of a person's life, then that would constitute a search.

What the mosaic approach implicates is that a lot of actions considered non-searches under the sequential approach would suddenly become a search. And Kerr emphasized the impracticability of implementing this sort of approach because technology changes too rapidly for the court to keep up.[169] Yet, six years later, the court implemented a mosaic type analysis in *Carpenter v. United States*.[170]

D. Carpenter *Protections and* Riley *Rationale*

In the past ten years, there have been two major Supreme Court cases regarding Fourth Amendment privacy protections—*Riley v. California*[171] and *Carpenter v. United States*.[172] Arguably, the most important point of the *Riley* decision was the rationale that phones contain more information than our homes.[173] It is no secret how much reverence the Court defers to people's right to privacy in their own homes,[174] so to compare technology to such a place was indicative of the Court's recognition and desire to address Fourth Amendment limitations with technology. More notably, in 2018, the landmark *Carpenter* Court held that compelling wireless carriers to turn over cell-site location information (CSLI) that

---

165 Kerr, *supra* note 160, at 320.
166 *Id.*
167 *Id.*
168 *Id.*
169 *Id.* at 347.
170 Carpenter v. United States, 585 U.S. 296 (2018).
171 573 U.S. 373 (2014).
172 585 U.S. 296 (2018).
173 *Riley*, 573 U.S. at 373.
174 *See* Silverman v. United States, 365 U.S. 505, 511 (1961).

tracks users' movements for a period of seven plus days constitutes a search and requires a warrant, absent exigent circumstances.[175]

CSLI are records detailing the approximate location of phones at a particular time.[176] Wireless providers like AT&T often collect and store this information for business purposes.[177] The records are generated when a person performs any activity that generates data connections,[178] such as when a person calls or answers a phone call.[179] Each record is time-stamped and provides the physical location of the nearest servicing provider's cell tower at the time of the call.[180] Cell towers are responsible for sending and receiving signals to and from cellphones.[181] Therefore, to connect, a phone must link to a service provider's cell tower.[182]

Since the records only provide the location of cell towers, and not the exact positioning of the phone itself, the information may not seem very accurate.[183] This is partially right. The CSLI records are generated (1) when the phone originally connects, (2) throughout the duration of connection, and (3) at the termination of the connection.[184] Using the phone call example, what's important is the nearest tower location at the beginning of the call and the end of the call.[185] The individual's location can then be pinpointed between the towers. Though a single record does not show the exact location of the phone itself or how far it is from the tower, the information can be determined through "triangulation in which the angles of the various signals are calculated when two cell towers are involved."[186] This is typically done by third-party

---

[175] *Carpenter*, 585 U.S. at 310.

[176] GINA STEVENS, CONG. RSCH. SERV. 7-5700, LEGAL STANDARD FOR DISCLOSURE OF CELL-SITE INFORMATION (CSI) AND GEOLOCATION INFO. (2010).

[177] *Id.* at 3.

[178] *Carpenter*, 585 U.S. at 315 ("Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.").

[179] STEVENS, *supra* note 176.

[180] *Id.* at 1.

[181] *Id.* at 3.

[182] *Id.*

[183] *Id.*

[184] STEVENS, *supra* note 176, at 2.

[185] *Id.* at 3.

[186] *Id.*

companies like the aforementioned LocationSmart. In summation, using the cell tower location at the beginning of a call and the end of a call, the phone's location can be determined within 100 meters.[187] And the technology has only grown more accurate and advanced with time.[188]

Prior to *Carpenter,* law enforcement would generally forego a probable cause warrant and subpoena the CSLI information from cellphone service providers using either the Stored Communications Act or the act in conjunction with the Pen Register and Trap and Trace Device Act.[189] Of course, these methods are technically still viable. The *Carpenter* Court held that seven days' worth of CSLI data records constitutes a search. Anything less seems to be fair game because the court did not address records obtained through these methods. Real-time location acquisition also was not addressed. It is notable, though, that some states have expanded the *Carpenter* holding and promulgated legislation specifically requiring law enforcement to obtain a warrant for access to CSLI data.[190]

---

[187] STEVENS, *supra* note 176, at 3 ("This [CSLI] information is stored by cellular telephone companies when the cellular telephone is operational through the phone's roaming antenna function, which allows the phone to link with the closest cell phone tower for the service provider. The information catalogs these changes in tower connection and also is cataloged in the context of individual telephone calls, showing the closest tower at the beginning of the telephone call and the closest tower at the end of the call. This information is limited, however, because towers can be up to 10 or more miles apart, and the location is not pinpointed since there is no GPS information involved. Records also do not indicate a phone's distance from the serving tower. The information can, however, provide a general indication of where a cell phone call was made, and the location can be pin-pointed more specifically through a process known as triangulation in which the angles of the various signals are calculated when two cell towers are involved. In 2005, the FCC mandated that cell phones be capable of being located within 100 meters for public safety purposes." (footnotes omitted)).

[188] Carpenter v. United States, 585 U.S. 296, 313 (2018).

[189] Stephanie Lacambra, *Cell Site Location Information*, ELEC. FRONTIER FOUND. (Mar. 28, 2019); *see also* 18 U.S.C. § 2703(d); 18 U.S.C. § 3121.

[190] Lacambra, *supra* note 189 ("Many states have enacted statutes requiring a warrant to get CSLI: California, Colorado, Maine, Minnesota, Montana, New Hampshire, New Mexico, and Utah. Other states like Illinois, Indiana, and Maryland, specifically protect real-time CSLI; while Iowa protects GPS location data. The standards for obtaining these types of warrants differs from state to state, along with what kind of CSLI is being sought. For example, California's CalECPA has specific particularity requirements for [search warrants] seeking electronic location information.").

Post-*Carpenter*, scholars hailed the case as likely to incite significant change in the legal world.[191] For the first time, people had a reasonable expectation of privacy in public company records they did not "own, possess, or control."[192] Suddenly, the third-party doctrine seemed to become a moot point. However, that was simply not the case. Essentially, the Court in *Carpenter* evaluated CSLI data constituted a search because (1) an individual has an expectation of privacy in CSLI records which produce a "near perfect surveillance" of a person's movements, and (2) the third-party doctrine could not be strictly applied to CSLI business records because historical CSLI provides a "chronicle" of people's movements and CSLI is not voluntarily obtained from consumers.[193]

To clarify, the first part of the Court's analysis focuses on whether an individual subjectively possesses an expectation of privacy in his CSLI records. The majority explained a person has an expectation of privacy because compiled CSLI data reveals more than just a person's whereabouts.[194] Articulating Sotomayor's concurrence in *Jones*, the Court determined the data showed an "intimate window into a person's life, revealing not only his particular movements, but through them his 'familial political, professional, religious, and sexual associations.'"[195] When examined chronically, the records reveal more than location, making the government's acquisition significantly more intrusive.[196]

But is this really true? Arguably, telephone logs and an individual's financial statements also reveal similarly intimate details about a person's life. Who someone talks to and how they

---

191 Rahbar, *supra* note 6, at, 729.

192 *Carpenter,* 585 U.S at 322 (Kennedy, J., dissenting).

193 *Id.* at 297-98

194 *Id.* at 310-11.

195 *Id.* at 310 (quoting United States v. Jones, 565 U.S. 400, 430 (Alito, J., concurring).

196 *Id.*

spend their money can very well indicate their "'familial, political, professional, religious, and sexual associations.'"[197]

Furthermore, the second part of the Court's analysis addressed whether the expectation of privacy was reasonable in society.[198] The Court ultimately distinguished the records in *Smith* and *Miller* from the type of records held by wireless carriers.[199] An exhaustive list of data records from cell phone providers is different from the limited personal information granted from telephone logs and bank records.[200] Though this distinction may be true, it is irrelevant to the third-party doctrine analysis. As Justice Gorsuch articulated in his dissent, is location information truly more intrusive and sensitive than who people talk to or their financial statements?[201]

Moreover, the Court determined CSLI information is not something that is voluntarily given to providers.[202] Echoing the *Riley* rationale, it is not voluntary because cellphones are an "insistent part of daily life" and are continuously generating CSLI without requiring an "affirmative act on the part of the user beyond powering up."[203] Nearly everyone in society has a smartphone which they carry which generates CSLI.[204] The only other way to avoid having their data information taken by their providers would be to forgo a cellphone at all. This would be an unreasonable and unrealistic standard today. However, the Court seemed to be overreaching here. Arguably, the personal information from *Smith* and *Miller*, telephone logs, are also records generated from phones. Also, simply powering on a device does not seem to be completely

---

[197] *Carpenter,* 585 U.S at 336-37 (Kennedy, J. dissenting) ("By contrast, financial records and telephone records do 'revea[l] . . . personal affairs, opinions, habits and associations.' *Miller*, 425 U.S., at 451 (Brennan, J., dissenting); see *Smith*, 442 U.S., at 751 (Marshall, J., dissenting). What persons purchase and to whom they talk might disclose how much money they make; the political and religious organizations to which they donate; whether they have visited a psychiatrist, plastic surgeon, abortion clinic, or AIDS treatment center; whether they go to gay bars or straight ones; and who are their closest friends and family members.").

[198] *Id.* at 304.

[199] *Id.* at 308-10.

[200] *Id.* at 313.

[201] *Carpenter,* 585 U.S. at 388 (Gorsuch, J., dissenting).

[202] *Id.* at 315.

[203] *Id.* at 298.

[204] *Id.*

right. Cell towers are responsible for sending and receiving signals.[205] This means a person affirmatively has to send a signal. Overall, the reasoning in *Carpenter* seems to be based more in personal concern with location data trading rather than constitutional overstep.

E. Carpenter *Protected Records Do Not Apply*

Carpenter protected records should not be extended to warrantless data purchases for three reasons: (1) the purchase method is not a Fourth Amendment search under the third-party doctrine and willing-seller rule; (2) data purchases are distinguishable from *Carpenter* protected records; and (3) there are too many unanswered questions.

Before *Carpenter,* the third-party doctrine and its protection over company business records was a straightforward, iron-clad rule. People do not have Fourth Amendment privacy rights in records companies autonomously own and control, even if those records contain sensitive information pertaining to them.[206] And this rule should still hold post-*Carpenter,* especially in application to data purchases. In fact, in the opinion itself, the majority explicitly distinguished CSLI acquired data from the aggregated and anonymized data sold to data brokers.[207]

Data purchases are distinguishable from *Carpenter* protected records because of the willing seller rule.[208] Under the rule, a company may produce records about how its consumers used the company's service, and it may use those records for business purposes, including voluntary sale. [209] A seller may voluntarily "transfer[] any possessory interest he may have had . . . to the purchaser . . . ."[210] Essentially, if a seller willingly wants to offer its consumers' business records to the government, the Fourth

---

[205] STEVENS, *supra* note 176.

[206] *See* United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).

[207] *See* Carpenter v. United States, 585 U.S. 296, 301 (2018) ("In addition, wireless carriers often sell aggregated location records to data brokers, without individual identifying information of the sort at issue here.").

[208] Kerr, *supra* note 10.

[209] *Id.*

[210] Maryland v. Macon, 472 U.S. 463 (1985).

Amendment cannot stop them.[211] Likewise, location data constitute these types of records. Many companies compile people's location records to help provide better services, ensure widespread service usage qualities across all consumer products, and develop ideas for internal improvements.[212] And, more importantly, consumers consent to companies using their information.[213] Because users consent, they have no legitimate claims to the data records—the service providers possess and own them.[214] Therefore, companies in possession of those records may sell location data to the government.

Furthermore, a mosaic type approach as in *Carpenter* is undesirable because judges cannot independently research complex technology during a proceeding.[215] Essentially, they must rely on the information presented by the parties.[216] Though they can consult with legal experts, these communications cannot be face to face.[217] This makes it particularly difficult in regard to digital surveillance methods. The way technology works and gathers information is arguably important to a Fourth Amendment proceeding because the more accurate and comprehensive an investigative technique is, the more sensitive the information may be inferred.

In *Carpenter,* CSLI became a concern because its location tracking capabilities had become refined and accurate enough to chronicle an individual's location in such a way that it exceeded society's reasonable expectation of privacy.[218] There is no person who could similarly provide such accurate records without technology's assistance.[219] As technology, continues to grow, there will be alternative digital techniques, potentially unimaginable ones, that will also need to be addressed. The Court will have to learn, understand, and weigh whether the Fourth Amendment prohibits governmental use of these techniques. This seems

---

[211] Kerr, *supra* note 10.
[212] Boshell, *supra* note 25.
[213] *Id.*
[214] *Id.*
[215] MODEL CODE OF JUD. CONDUCT R. 2.9 (2020).
[216] *Id.*
[217] *Id.*
[218] Carpenter v. United States, 585 U.S. 296, 296-298 (2018).
[219] *Id.* at 311-13.

difficult to maintain as technology transforms and becomes more sophisticated by the day.

And the government should not be entirely limited from investigating private citizens using digital techniques like data purchases, nor is that the Fourth Amendment's intention. When considering Fourth Amendment claims, there is a balance of interests at play: the state's interest to protect the public safety and the people's interest in privacy.[220] In other words, the Fourth Amendment is meant to prevent governmental overstep. Digital investigations have helped the government become more efficient at protecting the public safety. Unless the government has some "seismic shift," in power that grants them uninhibited access and egregious intrusion into people's privacy lives, and tips the balance of interests, there should be no extension. Data purchases have not become so relied on and widespread by the government that the balance cannot still be maintained.[221]

The court's analysis in *Carpenter* followed the traditional search doctrine two-pronged test on its face—whether the suspect had both a subjective and objective reasonable expectation of privacy. However, the Court departed from its traditional outlook that people do not have a reasonable expectation of privacy in their public movements, finding instead that they do not have one to a certain *extent*.[222] Because of this departure, there are now too many unanswered questions. The Court failed to clarify what length of time of chronicled location records tips the scale. At what point in time does the governmental acquisition constitute a search? When does the third-party doctrine become inapplicable? Perhaps, this is why the Court itself emphasized the opinion was a *narrow* holding.[223]

Carpenter was only the tip of the iceberg in determining Fourth Amendment privacy protections as applied to technology. In

---

[220] *Carpenter*, 585 U.S. at 337-338.

[221] Kerr, *supra* note 10.

[222] Carpenter v. United States, 585 U.S. 296, 298 (2018) (emphasis added).

[223] *Carpenter*, 585 U.S. at 298 ("This decision is narrow. It does not express a view on matters not before the Court; does not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras; does not address other business records that might incidentally reveal location information; and does not consider other collection techniques involving foreign affairs or national security.").

fact, the conundrum is the Court specifically noted in *Carpenter* that the holding was a narrow one, yet there has been significant dissension and, in some cases, improper application of the *Carpenter* decision to non-CSLI data related cases among the district courts of the United States.[224] Just how broadly does *Carpenter* extend? The short answer is not very far. Nor does it need to.

The unsuitability of the Fourth Amendment protections to digital intrusion reinforces the idea that there should be better data privacy laws in place regulating the private market. Rather than continue to force a centuries-old search doctrine to conform to the modern investigative techniques, the problem would be better addressed on the legislative level. Location data is a commodity that is lawlessly being collected, aggregated, and sold in troves, relatively uninhibited by legal repercussions. Congress has the capabilities to remedy this. In fact, there is a working, successful example already in place. The European Union recently enacted a comprehensive set of data privacy rules,[225] a model Congress could consider as a framework for its own enactment.

CONCLUSION

Ultimately, Congress should decline to extend the Fourth Amendment over the government's data purchases of people's location data because warrantless data purchases on the private market are not searches, technology changes too swiftly for the court to match, and the *Carpenter* holding should be left as it was intended to be—narrow. Instead, it is Congress's duty to enact proper regulations regarding public cybersecurity and privacy laws limiting the use of people's sensitive location data. Specifically, legislators should pass, with some minor adjustments, Elizabeth Warren's Health and Location Data Privacy Act of 2022, a Senate bill which limits data brokers from transferring and selling certain sensitive data, specifically health and location data. This Bill sets up a good framework for resolving the location data privacy issue,

---

[224] *Id. See In re* Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 733, 737 (N.D. Ill. 2020); United States v. Santos-Matos, No. CR 17-61-LPS, 2018 WL 5294509, at *2 (D. Del. Oct. 25, 2018); United States v. Kidd, 394 F. Supp. 3d 357, 362 (S.D.N.Y. 2019).

[225] Boshell, *supra* note 25.

but there are some tweaks that could ensure an even more airtight regulatory seal.

In particular, the Bill should be amended with three main provisions: (1) "data broker;" should be defined under the FTC's definition (2) licensed brokers must submit clear instruction to the FTC on how they collect, store, and process the people's personal information and (3) along with civil enforceability, brokers may also be held criminally liable for unlawfully buying, selling, trading, and licensing people's location data in order to ensure organizations remain compliant.

As for future considerations, data privacy will continue to be a concern so long as technology grows. At one point in time, cell phones were an unimaginable technological phenomenon—no one could have predicted their impact on the privacy crisis that looms today. Going forward, Congress must maintain and broaden the current protections, engage with legal and tech experts in the field to predict growing areas of privacy concerns, and tackle each issue one step at a time. Moreover, legal expert Professor Orin Kerr has pointed to several rising Fourth Amendment issues including police's use of long-term pole camera surveillance, the warrantless border searches of computers, the private search reconstruction doctrine's application to internet providers (where law enforcement acquires warrantless online searches from private parties), and the limits of computer warrants.