UIC
REVIEW OF INTELLECTUAL PROPERTY LAW


# *CARPENTER V. UNITED STATES*: STEP FORWARD FOR SMARTPHONES AND THEIR DATA, BUT MAYBE NOT FOR OTHER TECHNOLOGIES

STEPHEN BARTHOLOMEW

ABSTRACT

This article explores the landmark decision *Carpenter v. United States*, which represents a significant shift in how courts should evaluate the privacy implications of new disruptive technologies, like cell-site location information, and what they can offer to law enforcement. The Supreme Court evaluated the nature of the information collected in the context of a search, which is a stark departure from its conventional Fourth Amendment analysis that generally focuses on the manner or location in which a search transpires. This article parallels the Court's reasoning to facial recognition technologies and argues that *Carpenter* is a major inflection point in the Court's privacy jurisprudence concerning new pervasive technologies in our data-drive society.

UIC JOHN MARSHALL LAW SCHOOL

*Cite as* Stephen Bartholomew, *Carpenter v. United States: Step Forward for Smartphones and Their Data, But Maybe Not for Other Technologies*, 20 UIC REV. INTELL. PROP. L. 308 (2021).

# *CARPENTER V. UNITED STATES*: STEP FORWARD FOR SMARTPHONES AND THEIR DATA, BUT MAYBE NOT FOR OTHER TECHNOLOGIES

STEPHEN BARTHOLOMEW

# *CARPENTER V. UNITED STATES*: STEP FORWARD FOR SMARTPHONES AND THEIR DATA, BUT MAYBE NOT FOR OTHER TECHNOLOGIES

STEPHEN BARTHOLOMEW*

## I. INTRODUCTION

The United States is a nation of 326 million people, yet there are 396 million registered cell phone service accounts.[1] Additionally, the world creates over 2.5 quintillion bytes of data each day, and over 90% of the world's data is less than two years old.[2] Unsurprisingly, most of this new data consists of Cell-Site Location Information (CSLI). CSLI is created whenever a phone connects to a nearby cellular tower.[3] Whenever a user sends a text, makes a call, or receives a news update, a time-stamped record is created.[4]

Historically, the Supreme Court has held that one does not have a property interest in data or information conveyed to another party under the third-party doctrine.[5] The Supreme Court applied this principle to data and records created or held by a third-party on the grounds of voluntary disclosure.[6] The Court in *Smith v. Maryland* and *United States v. Miller* reasoned that one "assumes the risk" of any potential disclosure to a third-party.[7] But as Justice Gorsuch in his dissenting opinion in *Carpenter* so eloquently asserted, "no one believes that, if they ever did."[8]

The case of *Carpenter* represents a stark departure from the bright-line rule that one's Fourth Amendment privacy interest in information is extinguished when it is disclosed to another.[9] This case finally reconciles issues regarding data that is not truly

---

* © Stephen Bartholomew 2021. Juris Doctor Candidate, May 2022, at UIC John Marshall Law School, BA in Economics & Political Science, Certificate in Informatics, Indiana University Bloomington (2019). Thank you to the RIPL editing staff for all your help and input to assist me in finishing this article. And to Professor Robinson for exposing me to the field of data privacy; your valuable instruction and passion certainly impacted me in authoring this article.

[1] Carpenter v. U.S., 138 S. Ct. 2206, 2211 (2019).

[2] Bernard Marr, *How Much Data Do We Create Every Day?: The Mind-Blowing Stats Everyone Should Read*, FORBES (May 21, 2018), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/.

[3] Eric Lode, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment*, 92 A.L.R. FED. 2d 1, 2 (2015).

[4] *Cellphone Location Tracking: A Guide for Criminal Defense Attorneys*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/files/2017/10/30/cell_phone_location_information_one_pager_0.pdf (last visited Sept. 27, 2020).

[5] U.S. v. Miller, 425 U.S. 435, 444 (1976); Smith v. Maryland, 442 U.S. 735, 744 (1979).

[6] *Smith*, 442 U.S. at 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business.").

[7] *Id.* ("In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.").

[8] *Carpenter*, 138 U.S. at 2262.

[9] *Id.* at 2219.

"given," but automatically created.[10] Chief Justice Roberts, writing for the majority, held that historical CSLI is protected by the Fourth Amendment because of the "deeply revealing" nature of the data and the pervasiveness of smartphones in modern society.[11]

The Court in *Carpenter* arrived at the correct outcome but made the analysis more discretionary.[12] However, its decision may signal that the Court is willing to take a more flexible approach in its privacy jurisprudence concerning other disruptive technologies. Though the Court finally reconciled technology's pervasiveness in its evaluation, this will likely come at the expense of uniformity in its future application.

Part II will discuss CSLI, its functions, and the Supreme Court's Fourth Amendment jurisprudence prior to the decision in *Carpenter*. Part III will discuss the case itself and the perspectives that each opinion asserts with respect to CSLI. Part IV will evaluate the decision's shortcomings, future implications, its application amongst the lower courts, and its potential application to comprehensive facial recognition technologies. And finally, Part V will conclude that while *Carpenter* is a landmark decision for privacy rights, its future applicability for courts remains unclear. That being said, its flexibility is necessary to include more disruptive technologies in the future.

## II. BACKGROUND & EXISTING LAW

### A. *Overview of Cell-Site Location Information*

Each cell tower has multiple antennas pointing in each direction, covering a circular geographic area.[13] A CSLI record is created when a phone receives a call,

---

[10] *Id.* at 2220 ("Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other connection that a phone automatically makes when checking for news, weather, or social media updates . . . in no meaningful senses does the user voluntarily 'assume the risk' of turning over a comprehensive dossier of his physical movements.").

[11] *Id.* at 2221 ("Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection. The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.").

[12] *Carpenter*, 138 S. Ct. at 2266. Gorsuch argues that Roberts' analysis adds two subjective prongs to determine whether there is a need to avoid "arbitrary power" and "too permeating of a police surveillance" without offering any guidance for lower courts on how to do that. This leaves judges room to operate at their own discretion. He additionally notes that the line drawn at seven days is arbitrary itself and not logically tied to any former precedent or principle.

[13] *Carpenter*, 138 S. Ct. at 2225:

> The cell-site and antenna data points, together with the date and time of connection, are known as cell-site location information, or cell-site records. By linking an individual's cell phone to a particular 120– or 60–degree sector of a cell site's coverage area at a particular time, cell-site records reveal the general location of the cell phone user. The location information revealed by cell-site records is

email, text, news update, or anything which causes it to function.[14] This occurs each time a user's phone connects to a nearby cell-tower.[15] With the assistance of other nearby towers, any smartphone owner's location can be triangulated and tracked using CSLI.[16] As you travel, your phone connects to the nearest cell-site to provide you with the strongest signal—creating a CSLI record.[17] This generates a comprehensive register of any smartphone user's precise movements for as long as the wireless carrier deems necessary.

The accuracy of the CSLI-data is contingent upon the concentration of cell-sites in an area.[18] The more sites, the greater the tracking precision.[19] Last year, the Cellular Telecommunications and Internet Association recorded an 82.2% increase in the amount of data traffic in the United States.[20] The increase in the number of cell-sites mirrors the amount of CSLI generated. Also, because carriers sell aggregated location records to data brokers, your location is now one of your wireless carrier's most profitable commodities.[21]

In the digital age, smartphones have transformed from a privilege enjoyed by the affluent few to a necessity to accomplish mundane daily tasks. When the Court originally fashioned its Fourth Amendment jurisprudence, it could not have fathomed the technologies at the common man's disposal today. The rapid pace of innovation is a reason why the Court must adopt a flexible privacy framework. The conditions that Justice Brandeis feared in *Olmstead v. United States* are now a reality and judges should seek to protect citizens' liberties from the encroachments of technological innovation.[22]

---

> imprecise, because an individual cell-site sector usually covers a large geographic area.

[14] *Cellphone Location Tracking*, supra note 4.

[15] *Carpenter*, 138 S. Ct. at 2225.

[16] *Cellphone Location Tracking*, supra note 4.

[17] *Id.*

[18] Christian Bennardo, *The Fourth Amendment, CSLI Tracking, and the Mosaic Theory*, 85 FORDHAM L. REV. 2385, 2391 (2017).

[19] *Carpenter*, 138 S. Ct. at 2211 ("The precision of this information depends on the size of the geographic area covered by the cell site . . . . As data usage from cell phones has increased, wireless carriers have installed more cell sites to handle the traffic. That has led to increasingly compact coverage areas, especially in urban areas.").

[20] *2019 Annual Survey Highlights*, CTIA (June 20, 2019), https://www.ctia.org/news/2019-annual-survey-highlights.

[21] *Carpenter*, 138 S. Ct. at 2212 (Wireless carriers "collect and store CSLI for their own business purposes, including finding weak spots in their network and applying 'roaming' charges when another carrier routes data through their cell sites . . . carriers often sell aggregated location records to data brokers, without individual identifying information of the sort at issue here.").

[22] Olmstead v. U.S., 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting):

> Moreover, 'in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be.' . . . Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

### B. *Property Based Approach Centered on Trespass*

Initially, the Court based its privacy jurisprudence on the express language of the Fourth Amendment, which outlines protections for one's "person, house, papers, and effects" from unreasonable searches and seizures.[23] The case of *Olmstead v. United States* created the trespass-based approach to one's right to privacy.[24] There, law enforcement installed wiretaps, which did not physically encroach upon the defendant's property, in order to collect information to arrest Olmstead.[25] The Court held that employing a wiretap was not a "search" within the scope of the Fourth Amendment.[26] Chief Justice Taft asserted that a search under the Fourth Amendment must relate to one's physical person, a seizure of his papers, or tangible material effects.[27] Material seizure and physical intrusion were paramount for a search to occur under the Fourth Amendment.[28]

Nineteen years later, however, in *Silverman v. United States*, the Court defined its approach further in a case where agents used a "spike mike" to listen to the suspect's private conversation.[29] The evidence leading to Silverman's arrest was collected using the device, which was placed several inches into an adjoining wall.[30] The physical intrusion of the microphone into the heating duct of the defendant's property was enough for the Court to determine that a search occurred under the Fourth Amendment.[31]

---

[23] U.S. CONST. amend. IV:

> 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.

[24] *Olmstead*, 277 U.S. at 456. There, the defendant was convicted of violating the National Prohibition Act through a conspiracy to sell liquor illegally.

[25] *Id.* at 457 ("Small wires were inserted along the ordinary telephone wires from the residences of four of the petitioners and those leading from the chief office . . . . They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses.").

[26] *Id.* at 466.

[27] *Id.*

[28] Goldman v. U.S., 316 U.S. 129, 135 (1942). Similarly, in *Goldman*, the Court expanded on its trespass-centric jurisprudence. Goldman was convicted by using a detectaphone on an adjoining wall, next to the office where he was talking on the phone. The majority emphasized the absence of a physical trespass in its holding, refusing to overrule Olmstead because there was no "reasonable or logical distinction."

[29] Silverman v. U.S., 365 U.S. 505, 506 (1961) ("The petitioners were tried and found guilty . . . upon three counts of an indictment charging gambling offenses . . . police officers were permitted to describe incriminating conversations . . . at their alleged gambling establishment, conversations which the officers had overheard by means of an electronic listening device.").

[30] *Id.* at 507.

[31] *Id.* at 511 ("officers overheard the petitioners' conversations only by usurping part of the petitioners' house or office—a heating system which was an integral part of the premises occupied by the petitioners . . . In these circumstances we need not pause to consider whether or not there was a technical trespass.").

### C. *Katz and One's Reasonable Expectation of Privacy*

In the Sixties, the Court added another element to its privacy analysis based on one's reasonable expectations of privacy in the case of *Katz v. United States*.[32] There, agents attached a recording device to the top of a public phone booth from which Katz would make his calls.[33] The phone-tap recordings were used to support the state's indictment.[34]

The Court ruled that placing the recording device was impermissible, but the majority failed to fashion any concrete rule.[35] The majority asserted that the Fourth Amendment "protects people and not places," and held that the Amendment's language applied to the recording of oral statements regardless of any trespass.[36] The opinion emphasized that the State operated without a warrant in the case, which is why it ruled in Katz' favor.[37]

Justice Harlan's concurrence in *Katz*, however, offered a distinct perspective for courts to evaluate privacy rights. First, Justice Harlan considered whether a person has a reasonable expectation of privacy in an article of information, and then he considered whether society accepts it as "reasonable."[38] This framework is used in addition to the Court's trespass framework and is more discretionary in exchange for its additional flexibility.[39]

### D. *Smith and Miller: The Inception of the Third-Party Doctrine*

More than fifty years later, in the cases of *Smith* and *Miller*, the Court fashioned the third-party doctrine. The doctrine rests on the assumption that one has a "reduced expectation of privacy in information that is voluntarily shared with others."[40] In the case of *Miller*,[41] the Court held that Miller had no expectation of privacy in bank records because they cannot be considered Miller's "private papers," but rather business records that Miller voluntarily disclosed to the bank.[42] The Court reasoned

---

[32] Katz v. U.S., 389 U.S. 347, 348 (1967) ("The petitioner was convicted in the District Court for the Southern District of California under an eight-count indictment charging him with transmitting wagering information by telephone from Los Angeles to Miami and Boston in violation of a federal statute.").

[33] *Id.*

[34] *Id.*

[35] *Id.* at 352 ("But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen.").

[36] *Id.*

[37] *Katz*, 389 U.S. at 356.

[38] *Id.* at 360–61.

[39] U.S. v. Jones, 565 U.S. 400, 403 (2012). Justice Scalia asserts that the Court's trespass framework can be used for some cases, while Katz' reasonable expectation framework may be more proper for others.

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

[41] U.S. v. Miller, 425 U.S. 435, 436 (1976) ("Respondent 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.").

[42] *Id.* at 441.

that one takes a risk in disclosing information to another that the information will be conveyed to someone else, like the State.[43] Justice Powell additionally stated that it is immaterial if the information was only revealed for a "limited purpose."[44]

Likewise, in *Smith v. Maryland*, the Supreme Court employed the third-party doctrine for another technology—a pen register.[45] There, the Court rejected the notion that using a pen register amounted to a search.[46] The Court believed that Smith did not have an expectation of privacy in the numbers he dialed because he disclosed the information to the automatic connection service.[47] The Court reasoned that phone users "assumed the risk" of possible disclosure to the police.[48] Even if one has an expectation of privacy in these phone records, the expectation would not be legitimate because of the risk of such future disclosure.[49]

### E. *The Stored Communications Act, 18 U.S.C. § 2703*

In response to technological innovation, Congress enacted the Electronic Communications Privacy Act of 1986.[50] Article II of this legislation is the Stored Communications Act (SCA), which prohibits unauthorized compulsion or disclosure of stored communications like email and phone records.[51] Specifically, § 2703 prescribes procedures the State must comply with in order to compel the disclosure of consumer data.[52]

Access to stored records under the SCA is granted when a warrant is secured, or a court order is granted pursuant to subsection d.[53] Section 2703(d) requires a judge to issue an order if the State offers "specific and articulable facts, showing that there are reasonable grounds to believe the contents . . . are relevant and material."[54] This

---

[43] *Id.* 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.").

[44] *Id.*

[45] Smith v. Maryland, 442 U.S. 735, 737 (1979). After a robbery, McDonough began receiving strange calls from someone identifying themselves as the robber. The police requested the telephone company to place a pen register on the petitioner's house to record any incoming calls.

[46] *Id.* at 742.

[47] *Id.* ("All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.").

[48] *Id.* at 744.

[49] *Smith*, 442 U.S. at 746.

[50] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510–2703 (2021).

[51] Stored Communications Act, 18 U.S.C. § 2703 (2021).

[52] *Id.* Subsection (a) of the provision pertains to the contents of communications in electronic storage, (b) relates to remote computing services, and (c) pertains to the records of both categories.

[53] 18 U.S.C. §§ 2703(a)–2703(c) (2021). The requirements for disclosure prescribe a valid warrant be issued, unless a court order is granted under subsection (d).

[54] 18 U.S.C. § 2703(d) (2021):

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable

standard is lower than that prescribed by the Fourth Amendment. It is also frequently used by police to avoid having to collect more evidence to meet the Amendment's threshold of probable cause to obtain a warrant.[55]

### F. *The Court's Privacy Jurisprudence in Relation to Modern Technologies*

#### 1. *Modern Police Technologies, G.P.S., and Smartphones*

Like Congress, the Court also accounted for new disruptive technologies in its privacy jurisprudence. In the case of *Kyllo v. United States*, the Court evaluated the use of a thermal-imaging device.[56] Here, the Court appeared to fashion its rule to account more for new pervasive technologies, holding that the use of the device constituted a search under the Fourth Amendment.[57] Justice Scalia asserted that when law enforcement uses technology that is unavailable to the public to collect information, and which would otherwise be impossible without physical intrusion, it is "presumptively unreasonable absent a warrant."[58]

However, in the case of *Jones v. United States*, the Court reintroduced its traditional trespass approach when the State attached a G.P.S. device onto the defendant's car.[59] Justice Scalia, in his majority opinion, held that the State's installation of the G.P.S. device constituted a search within the scope of the Fourth Amendment.[60] In his analysis, Justice Scalia focused on the State's physical trespass when it installed the device on the undercarriage of the defendant's vehicle.[61] He

---

> grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

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

[56] Kyllo v. U.S., 533 U.S. 27, 29–30, (2001):

> In 1991 Agent William Elliott of the United States Department of the Interior came to suspect that marijuana was being grown in the home belonging to petitioner Danny Kyllo, part of a triplex on Rhododendron Drive in Florence, Oregon. Indoor marijuana growth typically requires high-intensity lamps. In order to determine whether an amount of heat was emanating from petitioner's home consistent with the use of such lamps, at 3:20 a.m. on January 16, 1992, Agent Elliott and Dan Haas used an Agema Thermovision 210 thermal imager to scan the triplex.

[57] *Id.* at 40.

[58] *Id.* ("when the state uses a device, not in general public use to explore the details of the home that would be impossible without physical intrusion, the surveillance is a search and presumptively unreasonable absent a warrant.").

[59] U.S. v. Jones, 565 U.S. 400, 403 (2012).

[60] *Id.* at 405–06 ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.").

[61] *Id.*

further noted that the *Katz* reasonable expectation framework simply supplements the common law trespass approach; it does not replace it.[62]

While joining in the opinion, Justice Sotomayor's concurrence argued that because of the nature of the information, "long term G.P.S. surveillance impinges on one's expectations of privacy."[63] Such a comprehensive record provides not just one's location, but details concerning one's "familial, political, professional, religious, and sexual associations."[64] Thus, supporting the notion that one possesses an expectation of privacy in whole of their physical movements.[65]

*Riley v. United States* was the first case to distinguish a smartphone from other traditional technologies.[66] Here, the Court held that an officer could not search a smartphone incident to arrest because the smartphone is fundamentally different from other articles on one's person.[67] Chief Justice Roberts noted that an individual's "entire private life can be reconstructed through a thousand pictures that have locations and descriptions."[68] The pervasiveness of a smartphone simply cannot be compared to that of physical records; and smartphone records are qualitatively different from any tangible record.[69]

### 2. *Facial Recognition Technologies*

Facial Recognition Technologies (FRT) present many of the same concerns as historical CSLI but with a sinister caveat. Just as Justice Sotomayor in *Jones* warned, FRT offers substantially more information than one's location; it offers the ultimate

---

[62] *Id.* at 409.

[63] *Id.* at 415 (Sotomayor, J., concurring).

[64] *Jones*, 565 U.S. at 415.

[65] *Id.* at 417. To end, she posited that the notion of the third-party doctrine should be reconsidered on the ground that disclosure of information to third parties is a necessity merely to carry on with their lives.

[66] Riley v. California, 573 U.S. 373, 379 (2014)

> An officer searched Riley incident to the arrest and found items associated with the "Bloods" street gang. He also seized a cell phone from Riley's pants pocket. According to Riley's uncontradicted assertion, the phone was a "smart phone," a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity.

[67] *Id.* at 383

> When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape . . . . In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction.

[68] *Id.* at 394.

[69] *Id.* at 393 ("The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

"privac[y] of life," your face.[70] Currently, China leads the world in the number of CCTV cameras it employs at 200 million, with the United States behind it at 50 million cameras.[71] However, the United States contains more CCTV cameras per capita than China, with both Chicago and New York boasting 35,000 and 11,000 cameras, respectively.[72]

Law enforcement may obtain anyone's photo through a number of government databases containing mugshots, civil service photos, and drivers' license photos.[73] Faces are also obtained through CCTV cameras, police body cameras, as well as privately owned security systems registered with the police for "centralized police monitoring."[74] According to a Georgetown study, half of all Americans have images stored in law enforcement facial recognition databases.[75] Generally, FRT first captures your face from a photo or video, then reads your face's geometry, which is then compared to a database of known faces.[76] It can be done retrospectively or contemporaneously as China has regarding protesters and its Uighur population.[77]

China's FRT system can locate a BBC reporter testing its capabilities amongst a city of 4.3 million citizens in a blistering seven minutes.[78] While the United States does not possess such capabilities yet, police departments across the country are adopting FRT from private companies like Clearview AI.[79] Clearview AI is currently used by around 2,400 law enforcement agencies around the country and offers police a repository of photos scraped from all across the web.[80] If this omnipotent tool can be created by a mere startup company, it can be perfected by a government absent proper limitations.

---

[70] *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

[71] Justinas Baltrusaitis, *Top 10 Countries and Cities by Number of CCTV Cameras*, PRECISE SECURITY (Dec. 12, 2020), https://www.precisesecurity.com/articles/Top-10-Countries-by-Number-of-CCTV-Cameras.

[72] *Id*.

[73] Jake Laperruque, *Facing the Future of Surveillance*, PROJECT ON GOV'T OVERSIGHT (Dec. 12, 2020), https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/.

[74] *Id*.

[75] Clare Garvie, Alvaro Bedoya & Jonathon Frankle, *The Perpetual Lineup: Unregulated Police Face Recognition in America*, GEORGETOWN CENTER ON PRIV. AND TECH. (Oct. 18, 2016), https://www.perpetuallineup.org.

[76] Steve Symanovich, *How Does Facial Recognition Work?*, NORTON, https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html (last visited Sept. 27, 2020).

[77] Abdullah Hasan, *2019 Proved We Can Stop Face Recognition Surveillance*, ACLU (Jan. 17, 2020), https://www.aclu.org/news/privacy-technology/2019-was-the-year-we-proved-face-recognition-surveillance-isnt-inevitable/.

[78] Jon Russell, *China's CCTV surveillance network took just 7 minutes to capture BBC reporter*, TECHCRUNCH (Dec. 12, 2020), https://techcrunch.com/2017/12/13/china-cctv-bbc-reporter/.

[79] Connie Fossi & Phil Prazen, *Miami Police Used Facial Recognition Technology in Protester's Arrest*, NBC 6 SOUTH FLORIDA (Dec. 11, 2020), https://www.nbcmiami.com/investigations/miami-police-used-facial-recognition-technology-in-protesters-arrest/.

[80] Heather Somerville, *Facial-Recognition Startup Clearview Moves to Limit Risk of Police Abuse*, WALL ST. J. (Dec. 10, 2020), https://www.wsj.com/articles/facial-recognition-startup-clearview-moves-to-prevent-possible-police-abuse-11603217327.

## III. *CARPENTER V. UNITED STATES* (2018)

### A. *Facts of Carpenter*

The case of *Carpenter* stemmed from a string of Radio Shack and T-Mobile store robberies that occurred in Michigan and Ohio.[81] Based on a confession, the FBI requested two court orders under § 2703(d) of the S.C.A. to obtain the CSLI of Timothy Carpenter from his wireless carriers.[82] Both orders were granted, which disclosed almost 13,000 location points to the FBI—an average of 101 points per day.[83] This information ultimately implicated Carpenter's involvement as it showed his phone "roaming" in Ohio at the time the robberies occurred.[84]

### B. *Procedural Posture*

At trial, Carpenter moved to suppress the evidence arguing that the seizure of cell-site information violated his Fourth Amendment right against unreasonable seizures absent a warrant supported by probable cause.[85] Ultimately, the District Court denied his motion to suppress.[86] The District Court found in favor of the State and convicted Carpenter.[87] Carpenter appealed to the Sixth Circuit and it upheld his conviction using the third-party doctrine.[88] This CSLI data, in the Sixth Circuit's view, was "voluntarily conveyed" by phone users for connection and was not within the purview of the Fourth Amendment.[89]

### C. *Chief Justice Roberts' Majority Opinion*

Chief Justice Roberts began his opinion by emphasizing that the purpose of the Fourth Amendment "is to safeguard privacy and security of individuals against

---

[81] Carpenter v. U.S., 138 S. Ct. 2206, 2212 (2018). Officers arrested four men connected with the robberies and obtained, through a confession, the phone numbers of his co-conspirators.

[82] *Id.* ("The first order sought 152 days of cell-site records from MetroPCS, which produced records spanning 127 days. The second order requested seven days of CSLI from Sprint, which produced two days of records covering the period when Carpenter's phone was "roaming" in northeastern Ohio.").

[83] *Carpenter*, 138 S. Ct. at 2122.

[84] *Id.* The United States subsequently filed suit alleging Carpenter's involvement, charging him with six counts of robbery and six counts of carrying a firearm during a federal crime of violence.

[85] *Id.*

[86] *Id.* at 2213. This conclusion rested on seven accomplices denoting Carpenter as the operation's leader and an FBI agent's expert testimony interpreting the CSLI to show Carpenter at the scene of four robberies.

[87] *Id.* Carpenter was convicted on all six counts of robbery and all but one of the six firearm counts. He was sentenced to more than 100 years in prison.

[88] U.S. v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016) ("Given that cell phone users voluntarily convey cell-site data to their carriers as "a means of establishing communication," the court concluded that the resulting business records are not entitled to Fourth Amendment protection.").

[89] *Id.*

arbitrary invasions."[90] He then summarized the Court's privacy jurisprudence and noted how there is no single test under the Fourth Amendment.[91] In Roberts' opinion, the Amendment "seeks to secure the 'privacies of life' against 'arbitrary power'. . . and 'to place obstacles in the way of too permeating police surveillance'"[92]

Roberts ended his summary of the Court's Fourth Amendment jurisprudence by discussing the Court's modern cases, which began to emphasize the technology's pervasiveness.[93] With that, he turned to the present dispute and concluded that requests for historical CSLI intersect two precedential lines.[94] The first addresses one's "expectations of privacy in their physical location and movements."[95] The second concerns the third-party doctrine and one's expectation of privacy regarding information voluntarily divulged to others.[96]

Beginning with the first line of cases, Roberts mentioned that "a person does not surrender all Fourth Amendment protection by venturing into the public sphere."[97] Additionally, he noted a majority of the Court already recognizes a privacy expectation in the "aggregate of one's physical movements."[98] While this reasoning directly pertained to G.P.S. technology, he contended that cell-site records are even more intrusive, thus warranting protection.[99]

CSLI, according to Roberts, achieves near perfect surveillance, "as if there were an ankle monitor on a user's phone."[100] It grants the government a comprehensive record of anyone's historical location and therefore should be subject to an expectation of privacy.[101] Using this reasoning, Roberts rejected the State's argument that the

---

[90] *Carpenter*, 138 S. Ct. at 2213. The founders crafted this provision as a response to the General Warrants and Writs of Assistance, permitting British officers to go through homes unrestrained searching for evidence of criminal activities. *See* Camara v. Municipal Ct. of San Francisco, 387 U.S. 523, 528 (1967).

[91] *Carpenter*, 138 S. Ct. at 2213–14.

[92] *Id.* at 2214; U.S. v. Di Re, 332 U.S. 581, 595 (1948); Boyd v. U.S., 116 U.S. 616, 630 (1886).

[93] *Carpenter*, 138 S. Ct. at 2214.

> As technology has enhanced the Government's capacity to encroach . . . this Court has sought to "assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34. "Likewise in Riley, the Court recognized the "immense storage capacity" of modern cell phones in holding that police officers must generally obtain a warrant before searching the contents of a phone." Riley, 573 U.S. at 380.

[94] *Carpenter*, 138 S. Ct. at 2215.

[95] *Id.*; U.S. v. Knotts, 460 U.S. 276, 281 (1983).

[96] *Carpenter*, 138 S. Ct. at 2216; *Miller*, 425 U.S. at 444; *Smith*, 442 U.S. at 744.

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

[98] *Id.* ("A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements.").

[99] *Id.* ("Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations") (quoting *Jones*, 565 U.S. at 415).

[100] *Id.* at 2218.

[101] *Id.*

third-party doctrine should apply because CSLI is a "business record."[102] Given the nature and pervasiveness of CSLI, the doctrine cannot apply because this information is not voluntarily shared; it is created automatically anytime your phone functions.[103]

Roberts ultimately held that the government's acquisition of CSLI constituted a search, and because it was conducted absent a valid warrant, was impermissible.[104] Moreover, § 2703(d) of the S.C.A. was an invalid avenue to obtain Carpenter's historical location data because a warrant supported by probable cause was required.[105] Simply offering facts to show why information was "relevant and material" to the state's investigation under § 2703(d), was insufficient.[106] A more stringent standard is required to uphold citizen privacy rights. Finally, Roberts stated that the opinion is narrow and applies only in circumstances of historical CSLI collection, before remanding the case for further proceedings consistent with the majority's opinion.[107]

### D. *Justice Kennedy's Dissenting Opinion*

Conversely, in his dissent, Justice Kennedy argued that a search did not occur because CSLI is a typical business record.[108] Kennedy stated that customers have no expectation of privacy because they do not "own, possess, control, or use" the records.[109] Unlike Roberts, Kennedy disputed the records' accuracy because of the design of cell-site dishes, which cover such a vast geographical area.[110]

Justice Kennedy classified the third-party doctrine from *Smith* and *Miller* as a categorical rule, and argued the majority misapplied the rule when it distinguished CSLI from other business records.[111] If it's a business record, there is no expectation of

---

> the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices 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.

[102] *Carpenter*, 138 S. Ct. at 2219.

[103] *Id.* at 2220.

[104] *Id.*

[105] *Id.* at 2221 ("Under the standard in the Stored Communications Act, however, law enforcement need only show that the cell-site evidence might be pertinent to an ongoing investigation—a "gigantic" departure from the probable cause rule, as the Government explained below.").

[106] 18 U.S.C. § 2703(d) (2021).

[107] *Id.*

[108] *Carpenter*, 138 S. Ct. at 2224.

[109] *Id.* ("Cell-site records, however, are no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process. Customers . . . have no reasonable expectation that they cannot be disclosed pursuant to lawful compulsory process.").

[110] *Id.* at 2225 ("The typical cell site covers a more-or-less circular geographic area around the site. It has three (or sometimes six) separate antennas pointing in different directions . . . . So a cell phone activated on the north side of a cell site will connect to a different antenna than a cell phone on the south side.").

[111] *Id.* at 2230, 2232. Additionally, he argues that the records at issue in *Smith* and *Miller* also paint a comprehensive picture of one's life.

privacy in the information.[112] Accordingly, the case should have been resolved by using traditional property principles since the government searched nothing which Carpenter owned.[113]

Justice Kennedy argued that requiring a warrant to obtain CSLI encroaches on Congress' powers to denote a compulsory process as an alternative way to collect information to aid investigations.[114] Given that Carpenter did not possess a legitimate expectation of privacy in anything the government searched, the search was permissible because it was authorized according to § 2703(d) of the S.C.A.[115]

### E. *Justice Gorsuch's Dissenting Opinion*

Justice Gorsuch began his dissent by discussing the pervasiveness of smart phone technologies. He noted how many of people's most private documents, which would have been locked away, now reside on third-party servers.[116] He then proceeded to criticize the logic of the third-party doctrine, arguing no one ever believed it, "if they ever did."[117] Justice Gorsuch chose to frame his opinion with three potential avenues forward for the Court's privacy jurisprudence.

The first is to ignore the problems with the third-party doctrine and "live with the consequences."[118] The second avenue disregards the doctrine and returns to the *Katz* framework, which he fears will return us to where we are now.[119] The final option is to re-couple the Court's privacy framework with positive law.[120] Gorsuch believed the third avenue was best, through his criticism of the majority's approach, arguing it effectively creates two balancing tests that will be problematic for lower courts to apply.[121]

First, he framed the analysis through a Fourth Amendment lens but noted that unless the Court is evaluating tangible items, the application of "papers and effects" to a digital world fails.[122] He next hypothesized whether the archaic concept of bailments can provide an effective solution.[123] Gorsuch seemed to support the parallel of entrusting your data to another party to one's "modern papers and effects," but understood the approach's limitations. [124]

---

[112] *Id.*

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

[114] *Id.* Without the compulsory process under § 2703(d), he argues, police would have a daunting job, and their efforts would be stymied for no reason. It also unnecessarily calls into question the subpoena mechanisms the legislature decided to implement.

[115] *Id.* at 2235.

[116] *Id.* at 2262.

[117] *Id.*

[118] *Carpenter*, 138 S. Ct. at 2262.

[119] *Id.*

[120] *Id.*

[121] *Id.* at 2267.

[122] *Id.* at 2268.

[123] *Carpenter*, 138 S. Ct. at 2268 ("a bailment is a delivery of a thing in trust for some special object or purpose, and upon a contract, expressed or implied, to conform to the object or purpose of the trust. A bailee normally owes a legal duty to keep the item safe.").

[124] *Id.* at 2269.

Justice Gorsuch also postulated that statutory law may provide guidance on how a property interest can be identified in one's data.[125] To conclude, Gorsuch explicitly recognized that customers have substantial legal interests in digital information, which could even rise to a property right.[126] However, he asserts that he dissented on this matter because the majority's framework was overly arbitrary.[127]

## IV. ANALYSIS

### A. *Technological Exceptionalism to Create a New Flexible Approach*

In many respects, *Carpenter* was a revolutionary decision. Not because of the test it promulgates, but because of the general principles present in the case concerning new technologies. Chief Justice Roberts, writing for the majority, emphasized the nature of the information collected because it created an "all-encompassing record" of Carpenter's location.[128] This is a significant departure from the Court's prior Fourth Amendment cases, which typically focused on the manner or location in which a search transpires.[129] Although *Katz* stated that the Fourth Amendment "protects people and not places," *Carpenter* is one of the first Supreme Court cases to employ this principle in the context of a search.[130]

Much of Roberts' reasoning appears to adopt an approach based on a theory of technological exceptionalism through his refusal to analogize CSLI with any former technology.[131] Technology is exceptional "when its introduction . . . requires a

---

[125] *Id.* at 2272 ("The statute generally forbids a carrier to 'use, disclose, or permit access to individually identifiable' CPNI without the customer's consent, except as needed to provide the customer's telecommunications services . . . It also requires the carrier to disclose CPNI 'upon affirmative written request by the customer, to any person designated by the customer.'").

[126] *Id.*

[127] *Id.*

[128] *Carpenter*, 138 S. Ct. at 2217 ("Although such records are generated for commercial purposes, that distinction does not negate Carpenter's anticipation of privacy in his physical location. Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts.").

[129] *Olmstead*, 277 U.S. at 457 (Taft focused on the absence of a trespass. What was material was that the wires did not encroach on Olmstead's property.); Goldman v. U.S., 316 U.S. 129, 132 (1942) (The majority emphasized the absence of a trespass. The substance of the defendants' conversations was not important.); Silverman v. U.S., 365 U.S. 505, 506 (1961) (Court again focused on the location and the manner in which the police used a spike mike to listen.); *Katz*, 389 U.S. at 348 (Majority focused on the police operating without a warrant); *Kyllo*, 533 U.S. at 30 (The Court emphasized the thermal imaging device used to look into Kyllo's residence.); *Jones*, 565 U.S. at 403 (Scalia, writing for the majority, focused on the police placing a GPS device on Jones' car.).

[130] *Katz*, 389 U.S. at 315. *See Riley*, 573 U.S. at 393. In the case of *Riley*, Chief Justice Roberts did not focus on the location in which the suspect was searched, nor did he focus on the information that stemmed from the search. There, what was material was the fact that a smartphone is entirely distinct from any traditional article that would be searched incident to an arrest. Where the suspect was searched did not matter, however, what was searched did.

[131] *Carpenter*, 138 S. Ct. at 2219:

systematic change to the law or legal institutions in order to reproduce an existing balance of values."[132] Roberts kept this in mind when the Court looked forward rather than retrospectively when evaluating CSLI. To Roberts, "the rule the Court adopts must take account of more sophisticated systems that are already in use or development."[133]

The pervasiveness of smartphones and CSLI, how the information is automatically created and not voluntarily disclosed, and the efficiencies CSLI offers law enforcement persuaded Roberts to extend protections to citizens and their information when these modern technologies are involved.[134] This technology fundamentally changed the way police can conduct investigations—a reason why Fourth Amendment protection is necessary. Roberts stressed that "with just the click of a button, the government can access each carriers' deep repository of information at practically no expense."[135] For Roberts, it seemed there was simply no analogy that would capture the pervasiveness and issues CSLI poses for privacy. CSLI is an exceptional technology that requires more protection than other forms of information under the Fourth Amendment.

### B. *Riley and Jones' Pivotal Role in this Shift of Judicial Thinking*

Moreover, Roberts arrived at his conclusion through *Riley's* reasoning and the *Jones* concurrences to justify his distinction for historical CSLI.[136] He began with Justice Sotomayor and Alito's concurrences in *Jones*, recognizing an expectation of privacy in the whole of one's movements.[137] The concurrences signify that the aggregation of enough locational data points, absent probable cause, impinges on

> There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.

[132] Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J. L. & TECH. 357, 403 (2019) (quoting Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 550–51 (2015)).

[133] *Carpenter*, 138 S. Ct. at 2218.

[134] *Id.*:

> Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may . . . call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.

[135] *Id.* at 2219 (citing Brief for Electronic Frontier Foundation et al. as Amici Curiae 12). The majority additionally noted that the number of cell-sites has increased, therefore the sector covered by each has shrunk. Given this, the precision of CSLI information is approaching GPS level precision. Further, the majority noted that "wireless carriers already have the capability to pinpoint a phone's location within 50 meters."

[136] *Riley*, 573 U.S. at 393 (2014); *Jones*, 565 U.S. at 415.

[137] *Jones*, 565 U.S. at 430 (Alito, J., concurring); *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

individual privacy rights.[138] To Roberts, CSLI records revealing some of peoples' most private associations, crosses the line of permissibility.[139] Given that smartphones are so universal to societal participation, CSLI grants the State a comprehensive catalogue of its citizens' location and personal associations. This is precisely what Justices Sotomayor and Alito alluded to in *Jones*.[140]

Roberts next relied upon *Riley*, where the Court refused to compare smartphone records to other physical effects. Smartphones hold a breadth of information for users, and the devices are practically a "feature of the human anatomy" that catalogue their owner's every movement.[141] Building upon this notion, he framed the capabilities of historical cell-site location tracking in virtually a dystopian manner. Each citizen can be effortlessly tracked absent being a suspect to a crime merely because of the smartphone in their pockets.[142] The case of *Riley* was the first case to evaluate a smartphone's capabilities incident to one's arrest.[143] Roberts in *Carpenter* extended this logic to the surveillance capabilities of smartphone data because of the sheer amount of information it offers to law enforcement at a whim.[144] CSLI is distinct from other forms of surveillance technology and warrants a separate analysis because of its investigative capabilities.

### C. *Flexibility Comes with a Price of Subjectivity, and No Definite Framework*

The Court departed from its historical privacy jurisprudence in distinguishing CSLI data from other third-party records. This is where the opinion receives much criticism for its subjectivity. Roberts distinguished CSLI from other records to justify not extending the third-party doctrine to a "distinct category of information."[145] This distinction, according to Kennedy, will "inhibit law enforcement and keep defendants and judges guessing for years to come."[146] To Kennedy, the case was simple: CSLI is a third-party record and the doctrine is a categorical rule, rather than the balancing test the majority sets forth.[147] The decision cannot be reconciled with *Smith* and *Miller*.[148]

Notwithstanding Justice Kennedy's concerns, the *Carpenter* decision makes the evaluation more discretionary; and this subjectivity accounts for a technology's omnipresence at the expense of a bright-line rule. Cases reconciling privacy issues with disruptive technologies are not conducive to a bright-line rule because innovation moves rapidly, and all cases possess varying issues and considerations. In the case of *Riley*, Roberts noted that when the suit was filed, flip phones were used, while when

---

[138] *Id*.

[139] *Carpenter*, 138 S. Ct. at 2218.

[140] *Jones*, 565 U.S. at 430; *Carpenter,* 138 S. Ct. at 415.

[141] *Carpenter*, 138 S. Ct. at 2218 (citing *Riley*, 573 U.S. at 385) ("a cell phone – almost a 'feature of human anatomy,'- tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time.").

[142] *Id.* ("Unlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when.").

[143] *Riley*, 573 U.S. at 393.

[144] *Carpenter*, 138 S. Ct. at 2218.

[145] *Id*. at 2219.

[146] *Id.* at 2234 (Kennedy, J., dissenting).

[147] *Id*. at 2226–27.

[148] *Id.*

the case was heard at the Supreme Court, they were obsolete.[149] Roberts certainly, and correctly, accounted for this speed in the approach he chose to adopt in *Carpenter*.

Moreover, Kennedy argued that traditional property principles govern the case. The State searched nothing that Carpenter owned but instead information his wireless carrier created and possessed, therefore implicating the third-party doctrine.[150] But as Justice Brandeis asserted in his *Olmstead* dissent, judges must protect citizens' liberties from technological innovation.[151] Justice Kennedy's approach failed to account for the applicability and flexibility property law principles lack towards contemporary cases evaluating modern technologies, which Justice Gorsuch also noted in his dissent.[152] Kennedy's approach would undermine one's privacy whenever a disruptive invention is created and does not comport with modern technological realities.

The third-party doctrine has become antiquated with the expansion of digitalized data and big data aggregation. It over-generalizes current data collection processes.[153] This doctrine should be left in the pre-*Carpenter* era and not be applied to new technologies. Technologies such as smartphones and CSLI cannot be adequately analogized to anything preceding them.

The dissenting justices opined that Roberts failed to assert a workable framework to extend this reasoning to other areas and technologies. Justices Kennedy and Gorsuch also argued that the opinion is arbitrary and leaves a host of questions unanswered.[154] Justice Gorsuch characterized the majority's approach as an "amorphous balancing test" that is too discretionary and based on a judge's policy views.[155] He added that the opinion fails to denote a duration for which it is permissible for the government to collect CSLI.[156] Both Justices focused on the apparent arbitrariness of footnote 3, which states that more than seven days of data collection

---

[149] *Riley*, 573 U.S. at 394. Roberts recognizes the difference between a traditional phone and a smartphone which is essentially a miniature computer capable of storing mass amounts of data tailored on its user.

[150] *Carpenter*, 138 S. Ct. at 2230.

[151] Olmstead v. U.S., 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting):

> Moreover, 'in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be' . . . Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

[152] *Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting).

[153] Jordan M. Blanke, *Carpenter v. United States Begs for Action*, 2018 U. ILL. L. REV. ONLINE 260, 260 (2018). *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 573 (2009).

[154] *Carpenter*, 138 S. Ct. at 2266–67 (Gorsuch, J., dissenting); *id*. at 2234 (Kennedy, J., dissenting in judgment).

[155] *Id*. at 2267 ("But how are lower courts supposed to weigh these radically different interests? Or assign values to different categories of information? All we know is that historical cell-site location information (for seven days, anyway) escapes *Smith* and *Miller's* shorn grasp, while a lifetime of bank or phone records does not.").

[156] *Id*.

constitutes a search, yet fails to explain how the majority drew this line.[157] To the dissenters, Roberts came to the outcome he wanted on baseless reasoning.

### D. *Workable Carpenter Tests Created by Legal Scholars*

As the dissenters appropriately argued, it is uncertain what the test promulgated by *Carpenter* truly is. However, legal scholars have attempted to condense the case's principles into a workable framework to be used by the lower courts. In his book, Orin Kerr reduces *Carpenter* to three elements: the information is collected via modern technology; the information is not disclosed voluntarily; and the information must reveal an intimate depiction of one's life irrelevant to any investigation.[158] The three elements parallel much of what Roberts' noted at the end of his majority opinion.[159]

Similarly, other scholars have also emphasized the factors the Chief Justice believed critical to highlight for *Carpenter* to apply.[160] While the frameworks theorized by scholars vary slightly, one principle is central. *Carpenter* shifted the analysis from an emphasis on collection and location to the nature and scope of the collected information. This is what *Carpenter* (and *Riley*) should be read to symbolize: a fundamental shift in the Court's opinion on how technology can dramatically affect society. Depending on the technology, a more stringent analysis is sometimes required.

### E. *Applications to Comprehensive Facial Recognition Technologies*

The pillars of the *Carpenter* decision concerning total surveillance can be paralleled to other disruptive technologies like facial recognition.[161] Facial Recognition Technologies (FRT), when coupled with third-party databases and surveillance technologies, which supply the state "with access to millions of images, will enable large scale surveillance of the general populace."[162] Roberts believes the Fourth Amendment seeks to secure "the privacies of life against arbitrary power" and "places

---

[157] *Id*. at 2266 (Gorsuch, J., dissenting) ("The Court does not tell us, for example, how far to carry either principle or how to weigh them against the legitimate needs of law enforcement. At what point does access to electronic data amount to 'arbitrary' authority? When does police surveillance become 'too permeating'?"); Carpenter, 138 S. Ct. at 2234 (Kennedy, J., dissenting) ("The Court's decision also will have ramifications that extend beyond cell-site records to other kinds of information held by third parties, yet the Court fails 'to provide clear guidance to law enforcement' and courts on key issues raised by its reinterpretation of *Miller* and *Smith*.").

[158] ORIN KERR, THE DIGITAL FOURTH AMENDMENT 3 (Oxford University Press, 2018).

[159] *Carpenter*, 138 S. Ct. at 2223 (Chief Justice Roberts highlighted the "deeply revealing nature" of CSLI, its "depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection." These were the qualities that distinguished CSLI from other categories of information).

[160] Ohm, *supra* note 132, at 361. (citing *Carpenter*, 138 S. Ct. at 2223).

[161] KERR, *supra* note 158, at 3. The *Carpenter* case's logic applying Fourth Amendment protections to data providing a historical personal record of one's life irrelevant to any investigative purpose, which is not voluntarily disclosed and continuously collected may be applicable to other modern technologies that will be at issue in future cases. These principles are embodied in Orin Kerr's framework promulgated in his book and other publications, which will be used to evaluate *Carpenter's* applicability to facial recognition technologies.

[162] H.R. Rep. No. 46-541, at 5 (2020).

obstacles in the way of a too permeating police surveillance."[163] According to this reading of the Fourth Amendment, the parallels between CSLI and FRT systems become apparent.

Although FRT systems share many similarities with CSLI, FRT can possess more insidious tendencies with the records they produce. These records are not mere "business records" as Justice Kennedy characterized CSLI, but a digital faceprint of an individual.[164] The concerns of FRT systems can be seen in China, where the government uses them to track and contain ethnic minorities[165]—akin to what protestors experienced in Hong Kong.[166] While Roberts' dystopian examples in *Carpenter* about total surveillance may seem exaggerated, technologies permitting governments to do this are taking hold around the world—even in the United States.[167]

There is a real possibility that there is much Fourth Amendment litigation on the horizon with the emergence of FRT as such an omnipresent surveillance technology. It is important to evaluate this technology in context of the principles that *Carpenter* promulgates. The subsequent three sections will consist of an application of the three-part Kerr framework to FRT collected information. Despite there being no precise test that can be discerned from *Carpenter*, Kerr's framework is an effective vehicle for applying *Carpenter's* rationale to emerging technologies that potentially encroach upon citizens' Fourth Amendment rights.

### 1. *FRT Systems are Digital-Age Technologies*

Under the first element of Kerr's framework, the information at issue must be collected via modern technology "rather than traditional forms of surveillance."[168] Aligning with Roberts' technological exceptionalism approach, this element omits technologies pre-dating the digital age. FRT systems, regardless of form, would belong in this category of technology, particularly when paired with police body cameras or expansive third-party databases.

Roberts in *Carpenter* was conscious to distinguish between modern surveillance methods and traditional measures like security cameras.[169] However, privacy concerns

---

[163] *Carpenter*, 138 S. Ct. at. 2215 (citing *Boyd*, 116 U.S. at 630; *Di Re*, 332 U.S. at 595).
[164] *Id*. at 2234 (Kennedy, J., dissenting).
[165] Hasan, *supra* note 77.
[166] *Id*.
[167] *Id*.:

> Three California cities — San Francisco, Berkeley, and Oakland — as well as three Massachusetts municipalities — Somerville, Northhampton, and Brookline — banned the government's use of face recognition from their communities. Following another ACLU effort, the state of California blocked police body cam use of the technology — forcing San Diego's police department to shutter its massive face surveillance flop. And in New York City, tenants successfully fended off their landlord's efforts to install face surveillance.

[168] KERR, *supra* note 158, at 18 ("traditional forms of surveillance that predate the digital age are categorically exempt.").
[169] *Carpenter*, 138 S. Ct. at 2220 ("We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information.").

are heightened when police use FRT algorithms to automatically identify citizens and track people in real-time.[170] When Roberts drew this distinction, he likely did not account for a pole camera equipped with an FRT system. If such technology were at issue, it is less certain Roberts would categorize this technology as "traditional surveillance." This form of surveillance would be comprehensive enough to implicate *Carpenter's* concerns.

2. *Absence of Any Meaningful Choice by an Individual*

The second element of Kerr's framework concerns information that is not voluntarily divulged by the user.[171] This, by far, was the most crucial consideration Roberts accounted for in his decision not to extend the third-party doctrine to CSLI.[172] This element's application depends largely on how the FRT system is implemented. If police compare an image to a database of drivers' licenses and publicly posted photos—*Carpenter* likely will not apply.[173] Records of this nature would implicate the third-party doctrine and would not be automatically generated in the same sense as CSLI records.[174]

On the other hand, when law enforcement compares images with a database like the FBI's FACE database, a nationwide repository comprised of law-abiding citizens, new privacy issues arise.[175] This is what the majority in *Carpenter* was primarily concerned about: carriers collect this information regardless of whether you're a person of interest.[176] The same logic applies to comprehensive FRT systems. Though FRT systems' records are more intrusive than CSLI records, issues of absolute surveillance stemming from technological innovation remain present.

---

[170] Jonathan Manes, *Secrecy & Evasion in Police Surveillance Technology*, 34 BERKELEY TECH. L. J. 503, 505 (2019).

[171] KERR, *supra* note 158, at 20 ("This is plainly met when the government conducts the surveillance or orders a third-party provider to do it . . . . The requirement is also met when the government collects third-party records that are inescapably created through use of broadly-used services.").

[172] *Carpenter*, 138 S. Ct. at 2220. CSLI generation requires no affirmative act on the part of the user outside of merely powering the phone on.

[173] H.R. Rep. No. 46-541, at 9 (2020) ("In short, current Supreme Court jurisprudence holds that surveillance of activities arising in public typically does not raise Fourth Amendment concerns, but surveillance that is prolonged and continuous may implicate privacy interests protected under the Fourth Amendment."); *See* Garvie, Bedoya & Frankle, *supra* note 75, at 132 (discussing Maryland's Image Repository System); *see also* Kevin Rector & Alison Knezevich, *Maryland's Use of Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates*, BALT. SUN (Oct. 18, 2016), https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html.

[174] Under these circumstances, users will have voluntarily disclosed this information to the Bureau of Motor Vehicles, or the social media site in which they initially posted the photo. Here, an affirmative act on the part of the user will ultimately cause the record to be created in the first place. In a scenario such as this, it is likely that the third-party doctrine would apply in the same manner in which it would apply in the cases of *Smith* and *Miller*.

[175] Garvie, Bedoya & Frankle, *supra* note 75, at 20.

[176] *Carpenter*, 138 S. Ct. at 2218. Chief Justice Roberts is chiefly concerned with the continuity and comprehensiveness that logs such as a historical CSLI record achieve almost perfect surveillance of an individual. This is universal throughout society and defies the logic in which the third-party doctrine rests on. There are no limits in which wireless carriers abide by outside of their own company policies.

3. *Information That is Deeply Revealing, Personal in Nature, and Irrelevant to Any Investigation*

The final element in Kerr's framework evaluates whether information is profoundly revealing, personal in nature, and irrelevant to any on-going investigation.[177] FRT that compares a single photo to a database of other images may not reveal enough information about one's life to implicate *Carpenter*. However, if used systematically, FRT systems are capable of enabling a government to "identify who attends protests, political rallies, church, or AA meetings on an unprecedented scale."[178] To capture enough of one's personal life, a FRT system must aggregate location data from multiple points that creates a comprehensive record.[179]

Looking to the future as Roberts did in *Carpenter*, if major cities implement FRT technologies on their camera networks, governments will be able to track citizens' movements retroactively or in real-time.[180] A scenario of this nature would undoubtedly satisfy this element requiring a detailed chronicle of a person's whereabouts over a significant period.[181] Given the ubiquitous technologies, like CSLI, currently at law enforcement's disposal, it truly is not difficult to imagine a surveillance technology such as this.

## V. CONCLUSION

The Court, as Justice Brandeis stated in *Olmstead*, has an obligation to protect citizens' liberties from the encroachments of technological innovation.[182] Justice Brandeis would have considered much of the technology at issue today in the courts to be mere science fiction. This is why a flexible framework, as Brandeis opined, is required. This idea was at the forefront of Roberts' mind as he chose to end his opinion with Brandeis' passage from *Olmstead*. Roberts focused on the over-arching principles

---

[177] KERR, *supra* note 158, at 18:

> The 'privacies of life' that Carpenter honors maintains the confidentiality of the "private interests and concerns" central to our identities. They are truths about us, such as our sexual preferences, our medical conditions, and our religious beliefs, that in most cases the state has no legitimate interest in learning. These truths do not reveal evidence of crime. They are just private facts about private people leading quiet lives free from criminal conduct.

[178] Hasan, *supra* note 77.

[179] *Carpenter*, 138 S. Ct. at 2218 ("With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years.").

[180] Garvie, Bedoya & Frankle, *supra* note 75, at 22.

[181] *Carpenter*, 138 S. Ct. at 2217–18. Chief Justice Roberts focused on the absolute surveillance aspect of CSLI in distinguishing it from other third-party information that is created contemporaneously, specifically, when the information creates a historical log of one's location that reveals not only one's movements but associations. With the various networks of cameras throughout modern cities in the United States, Europe, and Asia, such cameras equipped with FRT will be able to capture the breadth of information CSLI does.

[182] *Id*. at 2223 (quoting *Olmstead*, 277 U.S. at 473–37).

that the Fourth Amendment stands for rather than mechanically applying its text.[183] *Carpenter* should be read to symbolize this notion.

Roberts indeed made the inquiry more subjective; however, this discretion is well placed on the principles of technological exceptionalism that can also be seen in the Court's cases like *Riley*, *Jones*, and *Kyllo*.[184] CSLI and technology of such a pervasive nature cannot be compared to other traditional analogs. As technology becomes even more of a cornerstone to society, the concerns of absolute surveillance that yields a historical record contemporaneously absent any meaningful choice are evermore present.[185]

Comprehensive FRT implicates precisely these concerns if they are used in the manner authoritarian regimes around the world currently do.[186] When evaluating a single photo in comparison to a database, these concerns are not present. Though, when a network of cameras is used to track demonstrators like in Hong Kong, China, or Turkey, *Carpenter* should apply to such surveillance.

The subjectivity that stems from the *Carpenter* framework will come at the price of uniformity or a general rule resembling the third-party doctrine. However, this likely will make *Carpenter's* reasoning applicable to more pervasive technologies in the future, so long as concerns of total surveillance are present. Technologies are so unique and distinct that a bright-line rule which would suffice for traditional matters, is not workable in a realm that changes so frequently. Roberts, in choosing to adopt a flexible framework, accounted for this.[187]

It is difficult to discern where the case will ultimately nestle into the Court's privacy jurisprudence. *Carpenter*, which represents a stark departure from the categorical third-party doctrine, could be left to the side by courts on the grounds of the narrowness of the decision.[188] If CSLI is not at issue, then *Carpenter* may not be

---

[183] *Id*. at 2214 (To Roberts, the Fourth Amendment of the Constitution seeks to "'secure the privacies of life' against 'arbitrary power' and to him what was central to the framers was to "place obstacles in the way of a too permeating police surveillance") (internal citation omitted)).

[184] *Id*. ("As technology has enhanced the Government's capacity to encroach...this Court has sought to "assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted . . . . Likewise, in *Riley*, the Court recognized the "immense storage capacity" of modern cell phones in holding that police officers must generally obtain a warrant before searching the contents of a phone.").

[185] *Id*. at 2223. Roberts singled out the "deeply revealing nature" of CSLI as well as its "depth, breadth, and inescapable automatic nature of its collection." As modern technologies become ever more complex, more processes will be left to automation. In the future, as it is now, the only affirmative act one could undertake would be creating a user profile or downloading the application. Is this the proper place to draw the line for voluntary disclosure concerning digital age technologies, despite no true act leading to such disclosure?

[186] Hasan, *supra* note 77.

[187] *Carpenter*, 138 S. Ct. at 2218 ("At any rate, the rule the Court adopts 'must take into account of more sophisticated systems that are already in use of in development") (quoting *Kyllo*, 533 U.S. at 36).

[188] *Id*. at 2220. In *Carpenter*, the Chief Justice noted that the decision was narrow, and it did not opine on matters outside of historical CSLI aggregation. He stated that real-time CSLI collection nor "tower dumps" were covered by this opinion. Additionally, he stated that both *Smith* and *Miller* remain undisturbed, though it appears that the third-party doctrine's applicability has been stripped somewhat. *See also* U.S. v. Diggs, 385 F. Supp. 3d 648, 655 (N.D. Ill. 2019) ("the government's warrantless search of historical GPS data revealing Diggs's movements over the court of more than a

relevant for lower courts. Although, courts could take the decision for what it signifies: that an extension of principles used for analog technologies to the modern technologies of today fails to protect the liberties guaranteed by the Fourth Amendment.

Comparable to Justice Harlan in the case of *Katz*, Roberts understood that the analysis needed to change to abate the encroachment of citizens' liberties by new innovations.[189] Traditional analogies, much like the property principles Justice Gorsuch asserted, can only take us so far when modern technologies are at issue.[190] The assumptions relied on there are not present with innovations that dramatically alter the way the world works. *Carpenter* arrived at the correct outcome; however, it is impossible to state whether the case will be a step forward. That being said, the case should not be overruled. *Carpenter* represents the first step in constructing new assumptions to evaluate new disruptive technologies in the future.

month was a search"); U.S. v. Tuggle, 2018 WL 3631881, at *3 (C.D. Ill. 2018) ("The cameras only captured what would have been visible to any passerby in the neighborhood . . . while the Supreme Court has recently extended Fourth Amendment protections to address surveillance methods implicating new technologies, the surveillance here used ordinary video cameras that have been around for decades.").

[189] *Katz*, 380 U.S. at 360–61.

[190] *Carpenter*, 138 S. Ct. at. 2268.