Fear of Change: *Carpenter v. United States* and Third-Party Doctrine

Tricia A. Martino

Follow this and additional works at: https://dsc.duq.edu/dlr

Part of the Law Commons

Recommended Citation
Available at: https://dsc.duq.edu/dlr/vol58/iss2/6

This Student Article is brought to you for free and open access by Duquesne Scholarship Collection. It has been accepted for inclusion in Duquesne Law Review by an authorized editor of Duquesne Scholarship Collection.
Fear of Change: *Carpenter v. United States* and the Third-Party Doctrine

*Tricia A. Martino*

I. **INTRODUCTION** .................................................. 354

II. **HISTORY OF THE FOURTH AMENDMENT** ........ 355

III. **FACTS AND PROCEDURAL HISTORY OF CARPENTER** .......................................................... 360

IV. **THE MAJORITY OPINION** ...................................... 361

V. **THE DISSENTERS** ................................................ 363
   A. Justice Kennedy’s Dissent .................................... 364
   B. Justice Thomas’s Dissent ..................................... 365
   C. Justice Alito’s Dissent ....................................... 365
   D. Justice Gorsuch’s Dissent ................................... 366
      1. Maintain Smith and Miller ................................. 367
      2. Set Aside Miller and Smith and Retreat to Katz .......... 367
         3. Looking Elsewhere for Answers ....................... 368

VI. **THE PROBLEM WITH THE THIRD-PARTY DOCTRINE** .... 369
   A. Third-Party Support ........................................ 370
   B. Why the Third-Party Doctrine Should Be Curtailed or Overruled ....................... 371
   C. Considerations for Change ................................ 373

VII. **CONCLUSION** .................................................. 375

---

* J.D. Candidate, Duquesne School of Law, 2020; B.S. Criminology, B.A. Political Science, The Pennsylvania State University, 2014. The author dedicates this article to her father, Christopher J. Martino, who unexpectedly became sick and passed away during production.
I. INTRODUCTION

Today’s society is in an Information Age, which is “immeasurably enriched” and “seriously imperiled” by rapidly advancing technology. While individuals enjoy the benefit of having access to e-mail, global positioning system technology (GPS), social media, the internet, and a plethora of other applications on their phones, this same technology “endanger[s] the liberties at the core of our constitutional system.” Unknowingly, individuals are providing the government with ever-easier ways to access and record every action they take. Law enforcement officials need not expend their own resources to do this because the privacy scheme developed through the Fourth Amendment and relevant statutes allows law enforcement to simply ask third parties for the information. Unconsciously, each individual is giving law enforcement information on a grand scale that the government historically lacked the resources to collect. Whether it is the telephone company, the grocery store offering a rewards card, the internet service provider (ISP), Google, or even companies of which the individual is unaware, these companies are creating “digital dossiers” on anyone with a service account. Without due vigilance, this could be disastrous for the fundamental protections and liberties that define American society through the Fourth Amendment.

1. The Information Age is an era where technology allows individuals to “communicate, transfer and share information, access data, and analyze a profound array of facts and ideas.” Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. CAL. L. REV. 1083, 1089 (2002). However, individuals must “plug in” or enter into relationships with entities that then generate records of the individual’s personal information. Id.
3. Id. at 321-22.
4. Solove, supra note 1, at 1089 (“We are becoming a society of records, and these records are not held by us, but by third parties.”).
5. See id. at 1148-50.
6. Zachary Gold & Mark Latonero, Robots Welcome? Ethical and Legal Considerations for Web Crawling and Scraping, 13 WASH. J.L. TECH. & ARTS 275, 290 (2018). The type of tracking the government has access to now was “either impossible or prohibitively expensive in the past.” Id.
7. See Solove, supra note 1, at 1092 (describing companies that buy and aggregate people’s data from other entities).
8. Id. at 1084. These records are “becoming digital biographies, a horde of aggregated bits of information combined to reveal a portrait of who we are.” Id. at 1095.
9. Tomkovicz, supra note 2, at 322. This trajectory tolerates totalitarian features that allow the government to increase social control over citizens’ private lives. Solove, supra note 1, at 1102.
The United States Supreme Court’s recent decision in Carpenter v. United States takes a small step toward reigning in this technological encroachment. While imperfect, the decision began a judicial analysis about the impact of the Information Age on constitutional protections, specifically in the context of historical cell-site location information (CSLI). This article analyzes the Carpenter decision and posits whether the third-party doctrine should be re-evaluated or overruled in the technology-influenced era. Section II describes the history of the Fourth Amendment, and Section III addresses the facts of Carpenter. Sections IV and V discuss the majority and dissenting opinions, respectively. Lastly, Section VI examines the problems attendant to the third-party doctrine and suggests reform to the third-party doctrine.

II. HISTORY OF THE FOURTH AMENDMENT

In framing a government which is to be administered by men over men, the great difficulty lies in this: You must first enable the government to control the governed; and in the next place, oblige it to control itself.

The Fourth Amendment was a direct reaction to the colonists’ abhorrence for British use of the Writs of Assistance. In colonial times, England gave law enforcement officials general and unrestricted powers for the better part of four centuries. The American colonists resented the use of this unlimited power in the Writs of Assistance that enabled British soldiers to invade homes and businesses. These general warrants were random, unannounced, un-

11. Id. at 2211.
12. “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 Warrant shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. CONST. amend. IV.
14. Writs of Assistance were general warrants used by the British against the colonists which had no expiration. Nelson B. Lasson, The History and Development of the Fourth Amendment to the United States Constitution 26, 53-54 (1937). These arbitrary warrants needed no probable cause and were widely abused because they gave officials absolute and unlimited discretion subject only to the limits of (1) no arresting powers and (2) only daytime execution. Id.
15. Id. at 23.
16. Id. at 51.
supervised, and enacted without any suspicion of criminal activity.\textsuperscript{17} Eventually, the colonists brought the issue to court.\textsuperscript{18} James Otis, Jr.'s 1761 oration at court against the Writs of Assistance “breathed into this nation the breath of life” and “was the first scene of opposition to the arbitrary claims of Great Britain. Then and there the child of Independence was born.”\textsuperscript{19} Though the original draft of the Bill of Rights made no mention of it, the Founders at the Constitutional Conventions placed high importance on the inclusion of what became the Fourth Amendment.\textsuperscript{20}

The Fourth Amendment protects the security of “persons, houses, papers, and effects.”\textsuperscript{21} The Founders designed the Fourth Amendment to take decision-making out of the executing officer’s hands\textsuperscript{22} and into the “more trustworthy and sober judgment” of a judicial officer.\textsuperscript{23} The Fourth Amendment strikes a balance between liberty and social order—two concepts which stand on opposite sides of an ideological teeter-totter.\textsuperscript{24} The objective was “to guarantee the maximum amount of individual freedom that would be possible in a nation that also aspired to be safe, secure, and enduring.”\textsuperscript{25} Therefore, the Fourth Amendment allows government investigation so long as

\textsuperscript{18} \textit{LASSON}, supra note 14, at 57.
\textsuperscript{19} \textit{Id.} at 59 (internal citations omitted).
\textsuperscript{20} \textit{Id.} at 79-80.
\textsuperscript{21} \textit{U.S. CONST.} amend. IV.
\textsuperscript{22} Organized police forces did not exist at the Founding; modern police forces began organizing in the nineteenth century and did not achieve modern sophistication until the mid-twentieth century. \textit{Solove, supra} note 1, at 1105. It is inherently difficult for law enforcement officials to balance order and liberty when under social pressure to control and prevent crime and violence. \textit{Id.} at 1106. This leads to the official taking short cuts, excessive force, or unwarranted exercises of discretion and insensitivity or brutality toward constitutionally protected rights of the citizen. \textit{Id.}
\textsuperscript{23} \textit{LASSON, supra} note 14, at 120.
\textsuperscript{24} \textit{Tomkovicz, supra} note 2, at 324-25. Full social order is possible only in repressive regimes, while full liberty would result in an unsustainable governmental scheme. \textit{Id.}
\textsuperscript{25} \textit{Id.} at 325.
searches\textsuperscript{26} and seizures\textsuperscript{27} are reasonable. Such reasonableness requires a warrant,\textsuperscript{28} supported by probable cause,\textsuperscript{29} which must particularize\textsuperscript{30} "the places to be searched and the persons or things to be seized."\textsuperscript{31} In this way, the Fourth Amendment prevented the "fishing expeditions" and "dragnet investigations" that the Founders resented.\textsuperscript{32}

Originally, the Court analyzed the Fourth Amendment under a common law trespass doctrine requiring a physical intrusion on a constitutionally-protected area by the government before Fourth Amendment protections were triggered.\textsuperscript{33} This property-based or trespass-based analysis dominated Fourth Amendment jurisprudence for centuries\textsuperscript{34} until \textit{Katz v. United States} recognized that "the Fourth Amendment protects people, not places."\textsuperscript{35} The Court in \textit{Katz} found that the trespass was doctrine no longer controlling\textsuperscript{36} and thereafter adopted an analysis focusing on reasonable expectations of privacy.\textsuperscript{37} Specifically, the physical trespass doctrine could no longer safeguard the privacy interests that so motivated the Founders, and a new threshold for the Fourth Amendment had to recognize and encompass the substance of that privacy protection.\textsuperscript{38}

As the Court later explained through the \textit{Katz} test:

\begin{quote}
[w]hen an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to
\end{quote}

\textsuperscript{26} An unreasonable search occurs whenever the intrusiveness of the investigation outweighs the gravity of the crime being investigated. Solove, \textit{supra} note 1, at 1119 n.201.

\textsuperscript{27} The test for unreasonable seizures examines whether there was "some meaningful interference with an individual's possessory interests in [the] property." United States v. Jacobsen, 466 U.S. 109, 113 (1984).

\textsuperscript{28} See U.S. Const. amend IV; Solove, \textit{supra} note 1, at 1118 ("Generally, searches and seizures without a warrant are per se unreasonable.").

\textsuperscript{29} Probable cause exists where the "facts and circumstances within [the police's] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed." Solove, \textit{supra} note 1, at 1119 (quoting Brinegar v. United States, 338 U.S. 160, 175-76 (1949)).

\textsuperscript{30} Particularized suspicion is a factual basis to believe a particular person is engaged in illegal conduct. \textit{Id.} at 1109.

\textsuperscript{31} U.S. Const. amend. IV.

\textsuperscript{32} Solove, \textit{supra} note 1, at 1125, 1151.


\textsuperscript{34} Andrew MacKie-Mason, The Private Search Doctrine After Jones, 126 Yale L.J.F. 326, 327 (2017).

\textsuperscript{35} 389 U.S. 347, 351 (1967).


\textsuperscript{37} The reasonable expectation of privacy test comes from Justice Harlan's concurrence in \textit{Katz}. See 389 U.S. at 361 (Harlan, J., concurring).

\textsuperscript{38} Tomkovicz, \textit{supra} note 2, at 339.
recognize as reasonable, we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause.\footnote{Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (internal quotations omitted).}

Judicial interpretation post-\textit{Katz} demonstrated privacy as a concept of total secrecy.\footnote{Solove, \textit{supra} note 1, at 1131.} Total secrecy is a theory wherein the Fourth Amendment protects only the information that an individual specifically acts to keep hidden.\footnote{\textit{Id}. Professor Solove contends this conception is not adaptable to advances in technology; thus, it limits Fourth Amendment protection. \textit{Id}; see also Tomkovicz, \textit{supra} note 2, at 341.} The total secrecy conception is detailed best in the third-party doctrine developed by the Court in \textit{Miller v. United States}\footnote{425 U.S. 435, 437 (1976) (ruling that the government obtainment of bank records was not a Fourth Amendment search).} and \textit{Smith v. Maryland}.\footnote{442 U.S. 735, 745-46 (1979) (ruling that the government’s use of a pen register at a telephone company was not a Fourth Amendment search).} The third-party doctrine, as its name implies, governs the collection of information about one individual from a third party.\footnote{Orin S. Kerr, \textit{The Case for the Third-Party Doctrine}, 107 MICH. L. REV. 561, 563 (2009).} Simply put, “[b]y disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed.”\footnote{\textit{Id}.} The \textit{Katz} test, together with the third-party doctrine, became the sole analysis for almost five decades.\footnote{MacKie-Mason, \textit{supra} note 34, at 328 n.14; see also United States v. Jones, 565 U.S. 400, 405 (2012).} In 2012, however, the Court strongly reminded that “the \textit{Katz} reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.”\footnote{\textit{Jones}, 565 U.S. at 409.} The Court in \textit{United States v. Jones} declared that a Fourth Amendment search occurs when the government trespasses on a constitutionally protected area conjoined with an attempt to find something or obtain information.\footnote{MacKie-Mason, \textit{supra} note 34, at 329. Thus, a GPS monitoring system applied without a valid search warrant to a suspect’s car was an unreasonable search in violation of the Fourth Amendment. \textit{Jones}, 565 U.S. at 404.} In \textit{Jones’s} aftermath, appellate courts have analyzed searches under either a \textit{Katz} privacy test or a \textit{Jones} property test, or both.\footnote{Totten & Purdon, \textit{supra} note 36, at 234.}
The Court now stands at a precipice where the third-party doctrine and total secrecy face the challenges of technological advancements of the Information Age.\textsuperscript{50} Most personal information now exists in records kept by a variety of third parties.\textsuperscript{51} Furthermore, advancements in technology allow increasingly intrusive means of investigating target individuals.\textsuperscript{52} Justice Sotomayor explained her concern with the sole reliance on either a trespass or third-party doctrine regime in the Information Age where surveillance need not physically trespass into the records of the target individual.\textsuperscript{53} As \textit{Jones} described, GPS monitoring precision continues to improve.\textsuperscript{54} While \textit{Jones} was decided on a trespass theory, various Justices hinted that a longer duration of government tracking could implicate other Fourth Amendment concerns.\textsuperscript{55} Similarly, in \textit{Riley v. California}, the Court recognized that cell phones are such a “pervasive and insistent part of daily life” that they seem to be a “feature of human anatomy.”\textsuperscript{56} Thus, a warrant is required to search the information stored in a cell phone, even during a search incident to arrest\textsuperscript{57} because “[t]he fact that technology now allows an individual to carry [private information] in his hand does not make the information any less worthy” of Fourth Amendment protection.\textsuperscript{58}

The Court has been trending toward a Fourth Amendment threshold based on the amount of information collected: when the government collects a certain amount of data, regardless if it is public or not, the nature of the inquiry changes and the collection becomes a search possibly subject to the Fourth Amendment.\textsuperscript{59} A similar inquiry presented itself in \textit{Carpenter v. United States}, where the Court was asked to address Fourth Amendment protection implications of the historical location information stored by cell phone providers.\textsuperscript{60}

\begin{footnotesize}
\item[50] See Solove, \textit{supra} note 1, at 1084.
\item[51] Id. at 1087.
\item[52] For example, CSLI can now locate a person within fifty meters. Carpenter \textit{v. United States}, 138 S. Ct. 2206, 2219 (2018).
\item[53] \textit{Jones}, 565 U.S. at 413-18; Gold & Latonero, \textit{supra} note 6, at 288-90.
\item[54] \textit{Jones}, 565 U.S. at 428 (Alito, J., concurring).
\item[55] See id. at 415 (Sotomayor, J., concurring); id. at 430 (Alito, J., concurring).
\item[56] 573 U.S. 373, 385 (2014). Interestingly, Chief Justice Roberts authored both \textit{Riley} and \textit{Carpenter}, which suggests he is “the architect of these new privacy principles.” Davis Wright Tremaine LLP, \textit{Cracking Open a Can of Worms: Why Carpenter v. United States May Not Be the Privacy Decision that Was Needed or Wanted}, JD SUPRA (July 11, 2018), https://www.jdsupra.com/legalnews/insight-cracking-open-a-can-of-worms-20667/.
\item[57] \textit{Riley}, 573 U.S. at 403.
\item[58] Id.
\item[59] Gold & Latonero, \textit{supra} note 6, at 291 (analyzing \textit{Jones} and \textit{Riley}).
\item[60] 138 S. Ct. 2206; 2211 (2018).
\end{footnotesize}
III. FACTS AND PROCEDURAL HISTORY OF CARPENTER

In 2011, police arrested several suspects in connection with multiple armed robberies.\(^{61}\) One of the suspects confessed, identified fifteen accomplices in nine robberies, and gave the FBI several phone numbers of these accomplices, including that of Timothy Carpenter.\(^{62}\) Pursuant to the Stored Communications Act (SCA),\(^{63}\) the government obtained court orders\(^{64}\) for two cell phone providers, MetroPCS and Sprint, in order to obtain Carpenter’s CSLI.\(^{65}\) CSLI is the time-stamped and location-recorded data collected and stored when cell phones connect to cell sites to perform ordinary functions, often several times per minute.\(^{66}\) The government requested 159 days of CSLI records from the two providers.\(^{67}\) Collectively, the providers produced 12,898 location points spanning 129 days.\(^{68}\)

Subsequently, Carpenter was charged with six counts of robbery and six firearms counts.\(^{69}\) Carpenter filed a pretrial motion to suppress the CSLI data alleging that the warrantless seizure violated the Fourth Amendment.\(^{70}\) The United States District Court for the Eastern District of Michigan denied the motion.\(^{71}\) Carpenter was convicted on all but one firearm count and sentenced to over one hundred years in prison.\(^{72}\) The United States Court of Appeals for the Sixth Circuit affirmed the conviction by adhering to the third-

\(^{61}\) Id. at 2212.
\(^{62}\) Id.
\(^{64}\) According to the SCA, the government needs a search warrant for records that are less than 180-days old but only requires a court order for records that are older than 180 days. Gold & Latonero, supra note 6, at 288. This distinction is significant where court orders do not require particularized suspicion and, in some instances, judges merely act as a rubber stamp due to statutory requirements mandating their approval if certain steps are followed. Solove, supra note 1, at 1150.
\(^{65}\) Carpenter, 138 S. Ct. at 2211-12.
\(^{66}\) Id. For example, imagine a girl, Jane, waking in the morning to her friend calling. The friend asks her what time Jane would be picking her up for work. Jane hangs up and texts this friend that she is going to leave the house after she takes a shower. In the shower, Jane listens to music using her cell phone. As she brushes her teeth, Jane checks her emails on her phone. Her mom calls while she is making breakfast. During this conversation, Jane’s phone pings some notifications about deals through store applications. Then, Jane texts her friend when she leaves her house. On the way, she uses Google Maps for directions. Upon arrival, Jane texts the friend. While waiting for the friend to come to the car, Jane has a text exchange with her husband about dinner that night. Jane also receives multiple notifications while on her way to work. In this simple example, Jane’s phone collected dozens of CSLI data points.
\(^{67}\) Id. at 2212.
\(^{68}\) Id.
\(^{69}\) Id.
\(^{70}\) Id.
\(^{71}\) Id.
\(^{72}\) Id. at 2213.
party doctrine.\textsuperscript{73} Because Carpenter shared the location information with his wireless carriers, the third-party doctrine dictated he did not have a reasonable expectation of privacy in that information; thus, there were no Fourth Amendment implications.\textsuperscript{74} The United States Supreme Court granted certiorari.\textsuperscript{75}

IV. THE MAJORITY OPINION

Chief Justice Roberts wrote the majority opinion, concluding that the government’s use of CSLI against Carpenter was a search under the Fourth Amendment.\textsuperscript{76} The Court determined that the government invaded Carpenter’s reasonable expectation of privacy in the whole of his physical movements when it accessed CSLI from wireless carriers for long durations of time.\textsuperscript{77} Historically, it was only practical for the government to pursue suspects for limited durations; therefore, society did not expect the government’s ability to “monitor and catalogue every single movement . . . for a very long period [of time].”\textsuperscript{78} Using GPS tracking as a touchstone,\textsuperscript{79} the Court compared CSLI to GPS location information, stating that time-stamped data “provides an intimate window into a person’s life”\textsuperscript{80} because cell phone users have their phones on them almost constantly, giving the government “near perfect surveillance” of the targeted user.\textsuperscript{81} Furthermore, historical CSLI allows the government to go back in time and effectively tail any individual, subject only to the retention policies of wireless carriers.\textsuperscript{82} The Court described the case as a “detailed chronicle of a person’s physical presence compiled every day, every moment, over several years.”\textsuperscript{83} For this reason, “an individual maintains a legitimate expectation of

\begin{itemize}
\item \textsuperscript{73} Id.
\item \textsuperscript{74} United States v. Carpenter, 819 F.3d 880, 889-90 (6th Cir. 2016). Notably, Judge Stranch’s concurrence explained there were Fourth Amendment concerns but that a good faith exception applied. Id. at 893-94 (Stranch, J., concurring).
\item \textsuperscript{75} Carpenter, 138 S. Ct. at 2213.
\item \textsuperscript{76} Id. at 2220.
\item \textsuperscript{77} Id. at 2219. Notably, the Court refused to set time parameters for this decision, stating “[i]t is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.” Id. at 2217 n.3.
\item \textsuperscript{78} Id. at 2217 (quoting United States v. Jones, 565 U.S. 400, 430 (2012)). The majority opinion placed great weight on Justice Sotomayor’s Jones concurrence. Id.
\item \textsuperscript{79} See, e.g., id. at 2216 (“[T]racking partakes of many of the qualities of the GPS monitoring . . . .”); Id. at 2217-18 (like GPS monitoring, CSLI tracking is easy, cheap, and efficient); Id. at 2218 (historical cell-site records present “even greater privacy concerns than GPS monitoring”).
\item \textsuperscript{80} Id. at 2217 (citing Jones, 565 U.S. at 415).
\item \textsuperscript{81} Id. at 2218.
\item \textsuperscript{82} Id. Currently, cell phone providers retain records for five years. Id.
\item \textsuperscript{83} Id. at 2220.
\end{itemize}
privacy in the record of his physical movements as captured through CSLI."\textsuperscript{84} The Court declined to apply the third-party doctrine, created through \textit{Miller}\textsuperscript{85} and \textit{Smith}\textsuperscript{86} declaring that it would be a "significant extension" of the doctrine.\textsuperscript{87} It found that CSLI was categorically different information than telephone numbers and bank records.\textsuperscript{88} The Court opined, "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection,"\textsuperscript{89}—a determination which stands at odds with the original conception of the third-party doctrine.\textsuperscript{90} Distinguishing \textit{Miller} and \textit{Smith}, wherein the individuals assumed the risk of disclosure to the government by revealing information to a third party,\textsuperscript{91} the Court determined that CSLI is not "shared" as normally conceptualized; rather, it is logged automatically without any affirmative action by the user "beyond powering up."\textsuperscript{92}

Justice Roberts further determined the government's search of Carpenter's cell phone was unreasonable because it failed the probable cause standard.\textsuperscript{93} The government acquired a court order for the CSLI records pursuant to Section 2703(d) of the Stored Communications Act,\textsuperscript{94} which requires a standard of proof "well short" of probable cause.\textsuperscript{95} Therefore, Section 2703(d) utilized an unconstitutional mechanism for accessing historical CSLI due to its failure to meet the probable cause standard for a warrant.\textsuperscript{96} In rejecting

\begin{itemize}
  \item \textsuperscript{84} \textit{Id.} at 2217.
  \item \textsuperscript{85} United States v. Miller, 425 U.S. 435 (1976).
  \item \textsuperscript{86} Smith v. Maryland, 442 U.S. 735 (1979).
  \item \textsuperscript{87} \textit{Carpenter}, 138 S. Ct. at 2219.
  \item \textsuperscript{88} \textit{Id.} at 2216-17.
  \item \textsuperscript{89} \textit{Id.} at 2217.
  \item \textsuperscript{90} See \textit{id.} at 2262 (Gorsuch, J., dissenting) (the doctrine created a "categorical rule" whereby individuals surrender privacy expectations when disclosing information to third parties).
  \item \textsuperscript{91} \textit{Id.} at 2216 (majority opinion) (analyzing United States v. Miller, 425 U.S. 435, 443 (1976) and \textit{Smith}, 442 U.S. at 745).
  \item \textsuperscript{92} \textit{Id.} at 2220 (noting "there is no way to avoid leaving behind a trail of location data" unless the user turned it off, an action that renders the device unusable for its normal functions).
  \item \textsuperscript{93} \textit{Id.} at 2221; see also Solove, \textit{supra} note 1, at 1119 (explaining probable cause and what it requires).
  \item \textsuperscript{94} Stored Communications Act, 18 U.S.C. § 2703(d) (2012) (requiring the government to provide "specific and articulable facts" showing "reasonable grounds" that the records are "relevant and material to an ongoing criminal investigation").
  \item \textsuperscript{95} \textit{Carpenter}, 138 S. Ct. at 2221. Court orders, issued under a relevance standard, lie somewhere between subpoenas limited only by the burden placed on the producing party and warrants requiring probable cause and particularization. Solove, \textit{supra} note 1, at 1149-50.
  \item \textsuperscript{96} \textit{Carpenter}, 138 S. Ct. at 2221.
\end{itemize}
Justice Alito’s dissenting argument, the majority noted that subpoenas are subject to more relaxed scrutiny without regard to expectations of privacy in the records because: (1) the Court has never held the government could subpoena third-party records where the individual had a reasonable expectation of privacy in the information, (2) if subpoenas had no regard for Fourth Amendment implications, no record would be protected, and (3) there is an open argument whether warrant requirements apply to “modern-day equivalents” of people’s papers or effects, regardless of whether they are held by third parties. The Court emphasized its duty to step in to ensure Fourth Amendment protections are not swallowed by scientific progress and innovation.

In sum, Carpenter v. United States declared that, regardless of whether information may be held by a third party, a person has a reasonable expectation of privacy in location information via CSLI. Therefore, the government must obtain a warrant supported by probable cause to acquire this information. According to Justice Roberts:

[w]e decline to grant the state unrestricted access to a wireless carrier’s database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.101

Though a “narrow” decision, Carpenter provides greater protection to individuals in their technology and information given to third-party cell phone providers.102

V. THE DISSENTERS

Four Justices dissented, taking completely different views on the CSLI issue. Justice Kennedy focused on the third-party doctrine and argued the Court should have adhered to precedent and legislative judgment. Justice Thomas criticized the Katz doctrine completely, arguing it removes most of the Fourth Amendment

97. See generally id. at 2246-61 (Alito, J., dissenting).
98. Id. at 2221-22 (majority opinion).
99. Id. at 2223.
100. Id.
101. Id.
102. Id. at 2220.
103. See generally id. at 2223-35 (Kennedy, J., dissenting).
Justice Alito focused on the differences between subpoenas and warrants. And, Justice Gorsuch called for an entire re-evaluation of Fourth Amendment jurisprudence.

A. Justice Kennedy's Dissent

Justice Kennedy’s dissent characterized the new rule established by the majority as a needless departure from established precedent; he claimed it unhinged the property-based concepts of the Fourth Amendment. The third-party doctrine dictated the “commonsense principle” that property law analogues are dispositive in analysis of privacy expectations, and a defendant has no attenuated interest in property owned by another. Cell-site records are similar to the records involved in Smith and Miller because they are created, kept, classified, owned, controlled, and sold by the third party; thus, the new ruling creates an “unprincipled and unworkable” third-party doctrine for which the Court failed to establish guidelines. The majority, as Justice Kennedy pointed out, misread Miller and Smith as a balancing test rather than a dispositive threshold question; furthermore, even if it was a balancing test, the majority incorrectly protected location information more than bank records and phone calls.

Justice Kennedy ultimately cautioned the Court to defer to the legislature instead of imposing constitutional barriers that restrain further legislative debate. Here, the government received the information through a congressionally-authorized process which, Justice Kennedy highlighted, protected information more than a normal subpoena. By determining that CSLI was subject to the Fourth Amendment, the Court essentially reined in investigative tools and rendered the cell phone a “protected medium that dangerous persons will use to commit serious crimes.”

104. See generally id. at 2235-46 (Thomas, J., dissenting).
105. See generally id. at 2246-61 (Alito, J., dissenting).
106. See generally id. at 2261-72 (Gorsuch, J., dissenting).
107. Id. at 2224 (Kennedy, J., dissenting).
108. Id. at 2228. Justice Kennedy argued that Katz v. United States, 389 U.S. 347 (1967) provided property-based analogies in expectations of privacy rather than abandoning the doctrine completely. Id.
109. Id. at 2227.
110. Id. at 2224, 2230.
111. Id. at 2224, 2231-32.
112. Id. at 2224, 2233.
113. Id. at 2224, 2234.
114. Id. at 2224, 2235.
115. Id. at 2223.
also criticized the majority’s failure to address threshold questions for applying this new inquiry.116

B. Justice Thomas’s Dissent

Justice Thomas’s dissent called for the dissolution of the *Katz* reasonable expectation of privacy test.117 He declared that the test “has no basis in the text or history of the Fourth Amendment” and leads courts to make policy decisions rather than law.118 He also contended that it removed many words from the Amendment itself119 by defining a search under the *Katz* test in ways that defy common understanding120 and by focusing on privacy in ways contrary to the text of the Fourth Amendment.121 He explained the Founders enacted the Fourth Amendment as a protection from the Writs of Assistance that allowed broad searches of one’s home.122 In Justice Thomas’s view, there is a hierarchy to Fourth Amendment protections, namely property and privacy protections.123 The ancillary protection accorded privacy should not be the “sine qua non of the Amendment” according to Justice Thomas.124 Justice Thomas advocated overruling the *Katz* test, stating the case should involve whose property was searched, an analysis which returns to the text of the Fourth Amendment.125

C. Justice Alito’s Dissent

Justice Alito’s dissent expounded the distinction between subpoenas *duces tecum* and actual searches.126 Where actual searches allow law enforcement officials to enter homes and root through private papers and effects, subpoenas require parties to search

---

116. *Id.* at 2234. Justice Kennedy questioned what makes records a distinct category of information, how much information can be requested without a warrant, whether a time limitation depends on the type of information at issue, the scope of Congress’s power to authorize the government’s collection of information, and how to apply the Fourth Amendment’s reasonableness to compulsory processes. *Id.*

117. See generally *id.* at 2236 (Thomas, J., dissenting).

118. *Id.*

119. *Id.* at 2241. Justice Thomas argued that *Katz* rendered the phrase “persons, houses, papers, and effects” “entirely ‘superfluous’” and read out the word “their.” *Id.* (quoting United States v. Jones, 565 U.S. 400, 405 (2012)).

120. *Id.* at 2238.

121. *Id.* at 2239.

122. *Id.* at 2240.

123. *Id.*

124. *Id.*

125. *Id.* at 2235.

126. *Id.* at 2247 (Alito, J., dissenting). Subpoenas *duces tecum* are tools used to compel the production of tangible evidence like books, papers, and other physical evidence. *Id.* at 2248.
through and produce their own records.\textsuperscript{127} The Founders, in creating the Fourth Amendment, revolted against the means of acquiring information, not the acquisition itself.\textsuperscript{128} Justice Alito critically stated the Founders knew of subpoenas \textit{duces tecum}, yet chose not to include them in the Fourth Amendment text.\textsuperscript{129} Notwithstanding, Justice Alito admitted Fourth Amendment jurisprudence evolved to include subpoenas \textit{duces tecum} under a less strict standard.\textsuperscript{130} Justice Alito conceded that the government satisfied this burden in \textit{Carpenter}.\textsuperscript{131}

Justice Alito also condemned the departure in \textit{Katz} from property-based rights, stating it led people to claim privacy rights in others' items.\textsuperscript{132} He qualified this by stating that the majority misunderstood \textit{Miller} and \textit{Smith} as a new doctrine rather than a rejection of "an argument that would have disregarded the clear text of the Fourth Amendment."\textsuperscript{133} Reminding the Court that Fourth Amendment rights are personal, Justice Alito admonished the majority for creating a new line of Fourth Amendment doctrine by allowing individuals to object to the search of another individual or entity.\textsuperscript{134} Additionally, Justice Alito questioned why the Court now afforded an individual greater Fourth Amendment protection than a party actually subject to the subpoena.\textsuperscript{135}

\textbf{D. Justice Gorsuch's Dissent}

Justice Gorsuch agreed with the majority's judgment but departed from its reasoning.\textsuperscript{136} He began his dissent with two powerful questions: "[w]hat's left of the Fourth Amendment" and "[w]hat to do [about it]?"\textsuperscript{137} Justice Gorsuch explained that everything today is on the internet and held by third-party servers, including documents that were historically kept locked away.\textsuperscript{138} According to

\begin{itemize}
\item[\textsuperscript{127}] \textit{Id.} at 2247.
\item[\textsuperscript{128}] \textit{Id.} at 2251.
\item[\textsuperscript{129}] \textit{Id.} at 2252. Justice Alito points out subpoenas were not even discussed during the writing of the Fourth Amendment. \textit{Id.}
\item[\textsuperscript{130}] \textit{Id.} at 2254 (citing Okla. Press Publ'g Co. v. Walling, 327 U.S. 186 (1946)). The standard foregoes probable cause and instead requires the material production to be particularly described, authorized by law, and relevant. \textit{Id.}
\item[\textsuperscript{131}] \textit{Id.} at 2255 (describing the standard for a court order to be "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome") (citations omitted).
\item[\textsuperscript{132}] \textit{Id.} at 2259-60. Justice Alito hailed \textit{Miller} for rejecting this notion. \textit{Id.} at 2260.
\item[\textsuperscript{133}] \textit{Id.}
\item[\textsuperscript{134}] \textit{Id.} at 2257.
\item[\textsuperscript{135}] \textit{Id.} at 2256.
\item[\textsuperscript{136}] See generally \textit{Id.} at 2261-72 (Gorsuch, J., dissenting).
\item[\textsuperscript{137}] \textit{Id.} at 2262.
\item[\textsuperscript{138}] \textit{Id.}
\end{itemize}
Miller and Smith, the police could review all of it because individuals have no reasonable expectation of privacy in material held by third parties.\textsuperscript{139} This presents a problem to which Justice Gorsuch found three possible responses: (1) ignore the problem and continue application of Smith and Miller, (2) set aside the third-party doctrine and go back to Katz analysis, or (3) look elsewhere.\textsuperscript{140}

1. Maintain Smith and Miller

Unlike the majority’s use of a balancing test, Justice Gorsuch said Miller and Smith create a categorical rule where individuals who disclose information to third parties forfeit their Fourth Amendment reasonable expectation of privacy.\textsuperscript{141} From Justice Gorsuch’s standpoint, the doctrine is unworkable in today’s technological society precisely because people will inevitably relinquish personal information while wanting to maintain privacy.\textsuperscript{142} Justice Gorsuch noted the Court has never given persuasive justification for the third-party doctrine.\textsuperscript{143}

2. Set Aside Miller and Smith and Retreat to Katz

Returning to a Katz regime would inevitably end in the same analytical problems confronted today, according to Justice Gorsuch.\textsuperscript{144} He found that history did not support Katz because existing jurisprudence did not resemble it.\textsuperscript{145} Furthermore, Fourth Amendment protections historically depended neither on expectations of privacy nor on what a judge believed to be reasonable, but rather protected the person, house, papers, and effects whenever they were unreasonably searched or seized.\textsuperscript{146} Justice Gorsuch explained multiple ways that the Katz test conflated Fourth Amendment jurisprudence into an unpredictable and unbelievable mess guided by no single rubric.\textsuperscript{147} The question of whether the reasonable expectation of

\begin{flushright}
\textsuperscript{139} Id.
\textsuperscript{140} Id.
\textsuperscript{141} Id.
\textsuperscript{142} See id. (providing examples including emails from Google and DNA from 23andMe).
\textsuperscript{143} Id. at 2263; see also Kerr, supra note 44, at 564. In ruling out justifications, Justice Gorsuch described (1) the Restatement’s definition of assumption of the risk—expressly agreeing to or manifesting willingness to accept risks—has no context in the Fourth Amendment, (2) that voluntary consent to disclose information is the same as assumption of the risk, and (3) that clarity is no excuse where it would be just as easy to categorically say Fourth Amendment protections are not per se diminished in information shared with third parties. Carpenter, 138 S. Ct. at 2263 (Gorsuch, J., dissenting).
\textsuperscript{144} Id. at 2264 (noting it was Katz that produced Miller and Smith).
\textsuperscript{145} Id.
\textsuperscript{146} Id.
\textsuperscript{147} See id. at 2266-67.
\end{flushright}
privacy test is empirical or normative remains unsettled; nevertheless, this question should be resolved by the legislative, rather than the judicial, branch.\textsuperscript{148}

Justice Gorsuch believed the majority needlessly complicated Fourth Amendment analysis.\textsuperscript{149} He described two principles that the majority melded into the \textit{Katz} test, namely arbitrary power and permeating police surveillance.\textsuperscript{150} The Court, however, refused to provide guidelines on these principles.\textsuperscript{151} The Court directed lower courts to first perform a \textit{Katz} analysis and then evaluate whether disclosure to a third party outweighed privacy interests in the category of information.\textsuperscript{152} This pyramid of balancing inquiries, in Justice Gorsuch’s opinion, puts lower courts on a path “where \textit{Katz} inevitably leads.”\textsuperscript{153}

3. \textit{Looking Elsewhere for Answers}

Justice Gorsuch believed the answer to the problem lay elsewhere.\textsuperscript{154} The two prevalent ideas he suggested were resorting to traditional property-based approaches or relying on positive law.\textsuperscript{155} First, Justice Gorsuch advocated returning to a property-based approach to the Fourth Amendment, albeit with a slightly different focus.\textsuperscript{156} By applying a property-based analysis, Fourth Amendment protections and privacy interests would not automatically dissipate when information is shared with third parties.\textsuperscript{157} Rather, third parties obtaining information such as CSLI was similar to a bailment in which the original owner retains interests in the property that is possessed by the third party; this approach is counter-intuitive to \textit{Miller} and \textit{Smith} because it provides greater Fourth Amendment protection.\textsuperscript{158} In this way, complete or exclusive control over property was not required for Fourth Amendment rights.\textsuperscript{159}

\begin{itemize}
\item \textsuperscript{148} \textit{Id.} at 2265.
\item \textsuperscript{149} \textit{Id.} at 2267.
\item \textsuperscript{150} \textit{Id.} at 2266.
\item \textsuperscript{151} \textit{Id.}
\item \textsuperscript{152} \textit{Id.} at 2267.
\item \textsuperscript{153} \textit{Id.}
\item \textsuperscript{154} \textit{Id.}
\item \textsuperscript{155} \textit{Id.} at 2268.
\item \textsuperscript{156} \textit{Id.}
\item \textsuperscript{157} \textit{Id.} (providing examples where giving one’s car keys to a valet or asking a neighbor to watch one’s dog does not eliminate the owner’s interest in the car or dog).
\item \textsuperscript{158} \textit{Id.}
\item \textsuperscript{159} \textit{Id.} at 2269-70 (for example, individuals have a Fourth Amendment interest in their houses without holding fee simple title).
\end{itemize}
Second, Justice Gorsuch balanced positive law and constitutional protections. He explained that positive law guides evolving technologies while constitutional evaluation establishes a floor which no legislation may subvert. Finally, Justice Gorsuch admonished the majority for “keep[ing] Smith and Miller on life support” and Carpenter for not invoking any property right which would have been “his most promising line of argument.”

VI. THE PROBLEM WITH THE THIRD-PARTY DOCTRINE

Rather than side-step the third-party doctrine, the doctrine should be overruled as a per se categorical limitation on Fourth Amendment protection. The majority alluded to but refrained from doing so. Justice Gorsuch called for reevaluation. The doctrine continues to have value in situations involving informants and traditional tracking practices. Especially in today’s ever-growing technological world, the antiquated third-party doctrine stands for principles no longer applicable to the enormity of stored and shared data. As technological advancements unfold, its implications on the Fourth Amendment grow. Increasingly, a constitutionally appropriate distinction must be struck as to which technological “enhancements of human capabilities” should be regulated by the Fourth Amendment and which should “be able to promote societal safety unfettered by Fourth Amendment demands.” Not surprisingly, half of law enforcement agencies have no formal policies or processes in using technology or the internet in investigations.

Indeed, algorithms and artificial intelligence have allowed computers and computer programs to collect, analyze, and store vast amounts of information beyond that of human capability. Computers now store what used to be kept within the home—documents, photographs, records, and other private matters. Moreover, facial recognition technology infringes upon intimate privacy interests. Such technology identifies persons, not only through

160. Id. at 2270.
161. Id. at 2270-71.
162. Id. at 2272.
163. See generally id. at 2211-23 (majority opinion).
164. Id. at 2272 (Gorsuch, J., dissenting).
165. Solove, supra note 1, at 1136.
166. Id. at 1087.
167. See supra Introduction.
168. Tomkovicz, supra note 2, at 323.
169. Gold & Latonero, supra note 6, at 285. This lack of oversight and thus self-regulating nature resembles that of the Writs of Assistance abhorred by the Founders. Id.
170. Id. at 277.
171. Id. at 290.
their own pictures, but also in images posted by strangers.\textsuperscript{172} Consequently, the current scheme does not account for the increasing invasiveness of technology.

A. Third-Party Support

Professor Orin Kerr may fairly be described as the chief proponent of the third-party doctrine.\textsuperscript{173} He defends that use of the third-party doctrine outweigh its criticism for various reasons, not the least of which is a dearth of any reasonable alternatives.\textsuperscript{174} He asserted that the doctrine: (1) creates reasonable divides between less invasive investigatory procedures and more intrusive procedures requiring probable cause,\textsuperscript{175} (2) maintains technological neutrality of the Fourth Amendment by prohibiting a substitution of public for private transactions,\textsuperscript{176} and (3) provides \textit{ex ante} clarity by eliminating the need to track information’s history.\textsuperscript{177} Kerr explained that the third-party doctrine is best understood as a “consent doctrine” rather than an application of the reasonable expectation of privacy approach.\textsuperscript{178} Further, it is a shared-space doctrine where the individual consents to a third party having control over the information.\textsuperscript{179} Lastly, he criticizes opposing arguments for treating the Fourth Amendment as a be-all-end-all, rather than one of many

\textsuperscript{172} Id. at 284. Besides this recognition, metadata is also collected from these photos, including the times and locations, as well as the people at the same location or in the same picture. \textit{Id.}

\textsuperscript{173} See generally Orin Kerr, \textit{BERKELEY LAW}, https://www.law.berkeley.edu/our-faculty/faculty-profiles/orin-kerr/ (last visited Mar. 15, 2020). Professor Kerr has written over sixty articles, the majority of which have been cited by judicial opinions. \textit{Id.}

\textsuperscript{174} Kerr, \textit{supra} note 44, at 581.

\textsuperscript{175} Id. at 574.

\textsuperscript{176} Historically, crimes had a public and a private element. \textit{Id.} at 573. The public component was critical to police investigation; however, the use of technology and third parties have substituted “a hidden transaction for the previously open event.” \textit{Id.} at 575. The third-party doctrine, then, maintains the status quo. \textit{Id.} at 581.

\textsuperscript{177} \textit{Id.} at 565. This analysis posits that the history of an individual’s information is unknowable at the time law enforcement officials seek it; therefore, it is easier to determine the information’s privacy interests based on its location. The third-party doctrine guarantees that all information at a particular location is treated the same. \textit{Id.} at 582. Difficulty lies in creating a doctrine to replace the third-party doctrine’s clarity in the face of the possible exclusion of evidence if improperly judged. \textit{Id.}

\textsuperscript{178} \textit{Id.} at 588-89. Professor Kerr explained that the United States Supreme Court’s applications of the third-party doctrine have been “awkward and unconvincing” because in his opinion, the Court incorrectly focused on the application of Katz’s privacy test rather than consent principles. \textit{Id.} at 588. Professor Kerr contends that as long as it is a knowing disclosure, a person’s choice to give the information to law enforcement is a valid and voluntary consent that extinguishes Fourth Amendment protection. \textit{Id.}

\textsuperscript{179} \textit{Id.} at 589.
tools to prevent governmental abuses.\textsuperscript{180} All of these justifications are short-sighted and only rationalize the use of third parties in obtaining information in real time. The justifications do not hold up in the analysis of third-party records such as CSLI.\textsuperscript{181}

B. Why the Third-Party Doctrine Should Be Curtailed or Overruled

In this Information Age, Americans have no choice but to establish relationships with numerous third parties to fully enjoy what society has to offer.\textsuperscript{182} With every connection, third parties collect records that are increasingly useful to law enforcement officials.\textsuperscript{183} Rather than a rigid view of privacy, modern society requires sharing of information with others.\textsuperscript{184} Instead, privacy should be seen as contextual and built through relationships with other individuals and entities.\textsuperscript{185} For example, it seems intuitive that medical information may be shared from patient to doctor, and the doctor in turn may share that relevant information with pharmacists or medical insurance companies.\textsuperscript{186} It would be appalling, however, to think that doctors would be able to share sensitive medical information to newscasters or marketers.\textsuperscript{187} In a similar sense, individuals share location information in applications like Uber or Google Maps.\textsuperscript{188} They also share personal and intimate information in dating applications like Tinder specifically to be matched with a compatible partner.\textsuperscript{189} While it is expected that this information be shared with that partner, individuals do not expect the stored information to then be supplied to other entities such as the government or employers.\textsuperscript{190} Privacy is an enduring right in American life and the Fourth Amendment protections need to embrace the changing attitudes toward those interests to fully embrace the Amendment’s original purpose. Therefore, the third-party doctrine is an

\textsuperscript{180} Id. at 591 (explaining that other amendments, statutes, privileges, the entrapment doctrine, the Massiah doctrine, and internal agency regulations all similarly regulate government uses of third parties).
\textsuperscript{182} See Solove, supra note 1, at 1084.
\textsuperscript{183} Id.
\textsuperscript{184} Gold & Latonero, supra note 6, at 288-89.
\textsuperscript{185} Id. at 289.
\textsuperscript{186} Id.
\textsuperscript{187} Id.
\textsuperscript{188} Davis Wright Tremaine LLP, supra note 56.
\textsuperscript{189} Id.
\textsuperscript{190} Id. Furthermore, there are some technological developments that, by necessity, are relayed to the government such as autonomous driving technology systems that utilize private government networks for navigation and analysis of public roads. Id.
antiquated doctrine unsuited for the Information Age. It gives the government too much power. This is so, especially when considering the retainability dynamic between fallible human memory and infallible technological recording of information. The third-party doctrine, therefore, is “not responsive to life in the modern Informational Age.”

Statutory attempts to bridge the gap between privacy interests and technological advancements left in the wake of the third-party doctrine are weak and “uneven, overly complex, filled with gaps and loopholes, and containing numerous weak spots.” Another problem with the current privacy scheme is whether the threshold should relate to actual societal expectations or to the original values underlying the Fourth Amendment. For example, what place should actual public use hold in the evaluation of governmental exploitation of technology? Therefore, the third-party doctrine must be re-evaluated, if not completely overruled.

Additionally, multiple state supreme courts have rejected the third-party doctrine as applied to their jurisprudence. The Indiana Supreme Court declared “the third-party doctrine plays no part in our State’s search-and-seizure jurisprudence” before applying its state constitutional analysis instead. The Indiana Supreme Court also noted that the highest courts in California, Colorado, Florida, Hawaii, Idaho, Illinois, New Jersey, Utah, and Washington have rejected the third-party doctrine.

Individuals may become targets of investigations based on third-party disclosures for information that may not be related to them at all. Even where individuals attempt to remain anonymous on

191. Solove, supra note 1, at 1087.
192. Kerr, supra note 44, at 572 (explaining the third-party doctrine “gives the government more power than is consistent with a free and open society”).
193. Id.
194. Solove, supra note 1, at 1087.
195. Id. at 1088.
196. Tomkovicz, supra note 2, at 415 (“The protection afforded by a living Constitution might expand or contract due to changes in the fabric of the society for which it was designed.”).
197. Professor Tomkovicz suggests that public use requires more than the possibility that the public could use the technology; it also considers whether society has accepted and actually made use of such technology. Id. at 417.
198. Kerr, supra note 44, at 564.
200. Id.
201. All individuals who log onto an unsecured network, such as free Wi-Fi at Starbucks, receive the same internet protocol (IP) address. Erin Larson, Tracking Criminals with Internet Protocol Addresses: Is Law Enforcement Correctly Identifying Perpetrators?, 18 N.C.
the internet, the law recognizes only that the user "must still ini-
tially 'disclos[e] his identifying information to complete
strangers.'" Therefore, the third-party doctrine excepts the activ-
ity from constitutional protection.\textsuperscript{203} While the Carpenter Court did
not address tower dumps, the magnitude of information about in-
ocent people received through tower dumps cautions against the
continuation of the third-party doctrine in the Information Age.\textsuperscript{204}
Government surveillance in this way is subject only to self-regu-
lation by the specific law enforcement department.\textsuperscript{205}

C. Considerations for Change

While supporters of the third-party doctrine cite to the clarity
created by the doctrine,\textsuperscript{206} this is not enough to justify the privacy
interests breached. The idea of the third-party doctrine's clarity is
that "[b]ecause the history of information is erased when it arrives,
the law can impose rules as to what the police can or cannot do
based on the known location of the search instead of the unknown
history of the information obtained."\textsuperscript{207} This line of reasoning does
not hold up when compared to other constitutional and statutory
tests. For example, just like the bona fide occupational qualifica-
tion defense in employment discrimination law, Fourth Amend-
ment privacy in third parties can be an inquiry into whether the
information is "reasonably necessary to the normal operation of
that particular business or enterprise."\textsuperscript{208} Consider, for example, a

\begin{itemize}
\item J.L. & Tech. 316, 327 (2017). Internet activity and IP addresses, as understood currently,
are not protected information under the Fourth Amendment. \textit{Id.} at 323.
\item \textsuperscript{202} \textit{Id.} at 326 (quoting United States v. Farrell, No. CR15-029RAJ, 2016 WL 705197, at
\item \textsuperscript{203} \textit{Id.}
\item \textsuperscript{204} For example, North Carolina law enforcement officials are obtaining "reverse
searches" to gather all information from Google accounts within a seventeen-acre area in-
cluding homes, businesses, bars, restaurants, and apartments to find suspects in crimes.
Tyler Dukes, \textit{To Find Suspects, Police Quietly Turn to Google}, WRAL NEWS (Mar. 15, 2018, 5:05
AM), https://www.wral.com/raleigh-police-search-google-location-history/17377435/. The
police obtain time, location, names, dates of birth, email, phone number, and types of devices
Accounts as Part of Downtown Fire Probe}, WRAL NEWS (Feb. 14, 2018),
https://wral.com/scene-of-a-crime-raleigh-police-search-google-accounts-as-part-of-down-
town-fire-probe/17340884/.
\item \textsuperscript{205} See Dukes, supra note 204 (tactics are "used in extraordinary circumstances because
the department is aware of the privacy issues [raised]") (internal quotations omitted).
\item \textsuperscript{206} Kerr, supra note 44, at 582.
\item \textsuperscript{207} \textit{Id.}
\item \textsuperscript{208} James O. Pearson, Jr., Annotation, \textit{What Constitutes "Business Necessity" Justifying
Employment Practice Prima Facie Discriminatory Under Title VII of Civil Rights Act of 1964
\end{itemize}
telephone provider's financial statements or even the numbers dialed from particular phone numbers. They are reasonably necessary to normal business operations; however, the location logging of where those numbers were dialed is not related to the purpose or operations of the business. Thus, government information gathering of this data should be subject to Fourth Amendment warrant requirements.

In formulating a new Fourth Amendment analysis, a modified property-based analysis could quickly distinguish Fourth Amendment protections. An emerging consensus among reported cases finds that a warrant is required for constitutionally-protected areas. In short, if a police officer walks into an individual’s house in search of evidence, he must have a warrant. This is the most basic type of situation requiring a warrant.

Additionally, Fourth Amendment analysis must focus on whose information is sought by the search and how the information was obtained by the original third party. Specifically, the evaluation must question whether the information was voluntarily, knowingly, and affirmatively conveyed. First, there is a distinct difference in situations where an individual freely explains criminal plans to a person who is an informant and where an individual who, just by owning a cell phone, is tracked every minute of the day without any affirmative actions on that individual’s behalf. While the third-party doctrine still benefits analysis in an informant context, it should be reconsidered in other areas of surveillance and investigation. Second, there even can be a difference seen in an individual voluntarily and knowingly dialing phone numbers into the cell phone to connect a call, and again, the individual being tracked


211. See Kerr, supra note 44, at 589. Professor Kerr describes the third-party doctrine as a "shared space doctrine," whereby an individual who discloses information to a third party consents to its control over that information. Id. While this is correct, this analysis points to an opposite outcome than that of the third-party doctrine: both parties have an interest in the information with the individual having a reasonable expectation of privacy in it.

212. The Court began demarking this categorically by stating CSLI is not “shared” as normally conceptualized. Carpenter, 138 S. Ct. at 2220.

213. Compare Hoffa v. United States, 385 U.S. 293, 297 n.3 (1966) (individual confided in a confidential informant), with Carpenter, 138 S. Ct. at 2220 (cell phone provider automatically tracked individual "by dint of its operation").
every minute of the day without the individual performing any affirmative actions to trigger recording. On one hand, the individual’s location, including aggregated data of movement inside his home, is information personal to the individual who has not knowingly or affirmatively conveyed such information nor has the ability to contest the collection thereof. On the other hand, an individual specifically contracts with a telephone provider to make telephone calls, and therefore the act of dialing telephone numbers is knowingly and affirmatively conveyed to the provider. The difference in these records is clear and distinguishes the records in which an individual would have an expectation of privacy from those in which he does not.

VII. CONCLUSION

Today’s Information Age both benefits and imperils society. Rapidly advancing technology enriches citizens’ lives, but it does so at the cost of relinquishing private information to third parties. The tension between privacy interests and society’s increasing use of technology creates problems when the government uses this information in criminal investigations. In Carpenter v. United States, the United States Supreme Court addressed this usage in the context of CSLI and Fourth Amendment protections.

Fourth Amendment interpretation has developed throughout history to include property protections as well as privacy protections. It began as a limitation against general warrants used by the British and is now a major right enjoyed by all citizens. The United States Supreme Court reminded lower courts that both interpretations, property and privacy, are valid analyses in United States v. Jones. The Court then analyzed Timothy Carpenter’s conviction using CSLI records.

The majority emphatically declared that the third-party doctrine does not extend to the historical CSLI stored by cell phone service providers. They declared CSLI is categorically different information and, if applied, it would significantly extend the third-party doctrine. This is so because CSLI is not shared as originally posited. Moving forward, the government must utilize warrants to obtain such information. The dissenters, however, criticized the deci-

214. Compare Smith v. Maryland, 442 U.S. 735, 744 (1979) (Smith’s affirmative action of dialing telephone numbers was recorded by a pen register), with Carpenter, 138 S. Ct. at 2220 (Carpenter made no affirmative steps other than having his cell phone turned on).

215. See, e.g., Carpenter, 138 S. Ct. at 2218 (cautioning that the government “achieves near perfect surveillance” in this manner).
sion and admonished it for departing from the established precedents and textual reading of the Fourth Amendment. They focused on the differences between subpoenas and warrants. Justice Gorsuch even called for a reevaluation of the Fourth Amendment jurisprudence.

Professor Kerr defends the third-party doctrine in saying it creates divides, maintains Fourth Amendment neutrality, and provides clarity. However, the doctrine leaves citizens susceptible to intrusion on the private information that, by necessity, individuals must share with third parties. Statutory attempts to address the issue are weak and state supreme courts have declined to adopt the third-party doctrine. Furthermore, individuals become targets of investigations unrelated to their conduct.

Moving forward, the third-party doctrine must be reevaluated and tailored to the technological Information Age. A modified property-based analysis conjoined with an analysis of whose information is at issue and how that information was obtained could distinguish where the doctrine would be relevant and where it should not apply to Fourth Amendment analysis.

*Carpenter* has paved the way for finally allowing Fourth Amendment analysis to concern itself with the technological advancements of the Information Age. While some attempt to support the continuation of the third-party doctrine, this antiquated regime cannot answer to the privacy interests implicated with the utilization of the internet and other technology in government searches and seizures. The doctrine must be replaced with a more workable privacy scheme.