Richmond Journal of Law & Technology

Volume 26 | Issue 1 Article 2

2-21-2020

Too Big to Surveil: The Fourth Amendment Illuminated by 'Modern Lights' & Shadowed by Obsta Principiis in a Post Carpenter World Concerned with Privacy

Scott Keffer
Texas Tech Univeresity School of Law

Richmond Journal of Law & Technology Volume XXVI, Issue 1

TOO BIG TO SURVEIL: THE FOURTH AMENDMENT ILLUMINATED BY 'MODERN LIGHTS' & SHADOWED BY *OBSTA PRINCIPIIS* IN A POST-*CARPENTER* WORLD CONCERNED WITH PRIVACY

Scott Keffer*

Cite as: Scott Keffer, *Too Big to Surveil: The Fourth Amendment Illuminated by 'Modern Lights' & Shadowed by* Obsta Principiis *in a Post-*Carpenter *World Concerned with Privacy,* 26 RICH. J.L. & TECH., no. 1, 2020.

* Candidate for Doctor of Jurisprudence, Texas Tech University School of Law. Scott Keffer earned a B.A. in English and History at the University of Missouri and will graduate with a J.D. from Texas Tech University in May 2020. He wishes to thank the Texas Tech University School of Law, specifically Dean Jack Wade Nowlin, and Professors Brie Sherwin, John Watts, Jamie Baker, Alyson Drake, and Bill Keffer, as well as the members of the Texas Tech Law Review and the Richmond Journal of Law & Technology, and friends and family for all their support.

PREFACE

[1] The Fourth Amendment to the U.S. Constitution functions as a shield against excess governmental or police power by prohibiting unreasonable searches and seizures. Since its ratification, legal challenges have tempered this shield by frequently disputing the application of investigative processes and tools, including those that bypass the traditional—and simpler—analysis that focused on physical trespass. But recent technological advancements have prompted novel challenges and have forced the U.S. Supreme Court to adopt a parallel inquiry that evaluates society's expectations of privacy as an alternate path to invoke the Fourth Amendment's protections apart from any physical trespass.

[2] As revolutionary technology continues to present unique issues, this 200-year-old shield manifests a reflective luster, as if polished by years of legal discourse, that reveals the priorities of those who would interpret its text. Viewing the Fourth Amendment's shield as a mirror illustrates not only the thoughts of the drafters that revolved primarily around protecting property interests but also the expectations of modern society with its insistence on promoting privacy. Where the drafters channeled their outrage against the loathsome writs of assistance in colonial times, later Americans continued to denounce the similarly invasive general warrants and attempts by investigators to expand the tools in their arsenal beyond constitutional bounds, especially in the surveillance context. Yet, the problems posed by new technology upon privacy concerns are best resolved by relying on the core principles supporting the Fourth Amendment, previous U.S. Supreme Court precedent, and current societal perspectives regarding privacy as a top priority proven by recently enacted legislation both foreign and domestic.

[3] By applying a similar method to address advancing communication technology and its use as a surveillance tool in *Carpenter v. United States*, the Court turned this shield-become-mirror upon society to conclude that cell phone location information deserves Fourth Amendment protection because of its untiring comprehensiveness and its uniquely detailed nature.

Moreover, nearly every American adult carries a cell phone almost all the time, making it possible to create a time-stamped map of any cell-phone-carrying-individual's movements reaching back years and years. Unfortunately, the *Carpenter* Court did not extend this crucial protection far enough to protect *all* cell phone location data, and the unmistakable gap in its holding leaves a potential privacy vulnerability, the exploitation of which could cause greater harm than all previously disputed surveillance technology combined because of cell phone usage's general—near universal—applicability.

[4] Allowing cell phone location information to be obtained without probable cause and a proper search warrant not only fails to meet the spirit of the Fourth Amendment, but it also begins to tarnish that shield such that it no longer reflects historical or current societal values, reducing its goal of protecting Americans to a hollow incantation of words left to languish as time, and technology, marches on.

TABLE OF CONTENTS

I. INTRODUCTION

[5] From December 2010 until March 2011, Timothy Carpenter did something that most of us may never do, but he also did something that most of us do every single day.[1] Carpenter committed six counts of robbery while carrying a firearm, yet he was also carrying a cell phone that independently logged cell site location information (CSLI) detailing his movements, which ultimately led to his conviction and sentencing to over 100 years in prison.[2]

[6] This new species of evidence, CSLI data, used to convict Carpenter is significant because the Government obtained Carpenter's CSLI data without a warrant supported by probable cause.[3] In fact, CSLI is recorded automatically whenever *any* cell phone connects with cell sites that log the time and location of that connection, making such time-stamped, location records very helpful to retrace the trail left behind by *anyone* carrying a cell phone.[4] The prosecution then used that incriminating data, which is usually retained by cell carriers on *all* of its customers as routine business records for several years, as compelling circumstantial evidence to suggest that Carpenter was in the approximate location during the time of the alleged robberies because he was committing those crimes.[5]

---

[1] *See* Carpenter v. United States, 138 S. Ct. 2206, 2225–26 (2018) (Kennedy, J., dissenting).

[2] *See id.* at 2212–13 (majority opinion).

[3] *See id.* at 2212 ("That statute, as amended in 1994, permits the Government to compel the disclosure of certain telecommunications records when it 'offers specific and articulable facts showing that there are reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.' [Stored Communications Act, 18 U.S.C. § 2703(d) 2018].").

[4] *See id.* 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 [policies] of the wireless carriers, which currently maintain records for up to five years.").

[5] *See id.* at 2213; *see also* Steven M. Harkins, Note, *CSLI Disclosure: Why Probable Cause is Necessary to Protect What's Left of the Fourth Amendment*, 68 WASH. & LEE L.

[7] On appeal, the U.S. Supreme Court reviewed Carpenter's claim that the Fourth Amendment's prohibitions against unreasonable searches and seizures were violated, while also noting the staggering statistic that in the United States, a nation of 326 million people, there are 396 million cell phone service accounts.[6] Due, in large part, to this ubiquitous cell phone usage, the majority of the Court came to "recognize that CSLI is an entirely different species of business record . . . ."[7]

[8] Accordingly, the Court declared that "the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, [and despite] the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[8] Further, the Court determined that the acquisition of Carpenter's CSLI data constituted a search; but the majority, in the dissent's view, established an arbitrary and inconclusive threshold that considered the Government's procurement of seven days of CSLI records as sufficient to trigger the Fourth Amendment's protections.[9]

[9] This Article is the first to argue that this inexplicit time-threshold, in which acquisition of seven or more days' worth of CSLI data constitutes a search while records representing less than seven days of CSLI data are omitted from *Carpenter*'s pro-privacy insistence on a warrant in its holding, should be replaced by an all-inclusive rule. Such a rule must establish that

---

REV. 1875, 1882 (2011) ("A network may use a Time Distance of Arrival (TDOA) system, which determines location by measuring and comparing the time it takes the signal to arrive at each tower. Similarly, an Angle of Arrival (AOA) system measures the angle from which the signal reaches multiple towers, and uses that information to triangulate the cell phone's location.").

[6] *See Carpenter*, 138 S. Ct. at 2211.

[7] *Id.* at 2222.

[8] *Id.* at 2223.

[9] *See id.* at 2230 (Kennedy, J., dissenting).

acquisition of even a single day's CSLI records constitutes a search and requires *all* CSLI disclosures to first satisfy the warrant requirement imposed by the Fourth Amendment's protections to prevent unreasonable searches.[10] By focusing on the original purpose of the Fourth Amendment, closely analogous U.S. Supreme Court precedent, and current societal expectations of privacy, the solution will become clear: that *all* CSLI data, even a solitary day's worth, should be protected by the Fourth Amendment to require a search warrant founded on probable cause before disclosure by cell carriers, excepting, of course, exigent circumstances where time is of the essence such as rescue operations or active emergencies.[11] Part II of this Article surveys the history of the Fourth Amendment and particularly relevant Supreme Court opinions. Part III argues to extend *Carpenter*'s reasoning by highlighting advancing technology and societal expectations of privacy evidenced by recently enacted foreign and domestic legislation. Part III continues by reconciling the dissenting opinions in *Carpenter* with recommendations to Congress, and to the Supreme Court, to create marginal property interests in CSLI data to align with the traditional trespass analysis under the Fourth Amendment or to require search warrants before disclosure of *any* CSLI data to investigators as an expansion of *Carpenter*'s holding.

[10] Overall, this Article seeks to establish that the totality of cell phone users, as a group that encompasses almost every American, is *too big to surveil*. Additionally, CSLI data, as a new species of business record, is too sensitive, encyclopedic, and generally applicable to allow its usage by law enforcement without significant need or proof of probable cause resulting

[10] *Id.* at 2217, n.3 (majority opinion) ("[W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be.").

[11] *See* Olmstead v. United States, 277 U.S. 438, 478 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967) ("[E]very unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.").

in a warrant, as prescribed by the Fourth Amendment.[12] Further, *obsta principiis* (Latin for: resist the first approaches or encroachments), more than an antiquated motto, is an ineluctable and constant judicial duty to resist any serious encroachment on privacy or denigration of the Fourth Amendment as modern technology continues to create dangerous new possibilities for the exploitation of Americans.[13]

II. BACKGROUND

[11] The original source of inspiration supporting the Fourth Amendment could be found in many different instances in history from antiquity to the creation of the United States.[14] Looking to English history, as early as the year 1215, provides the greatest context due to the direct link from the common law of England to the founding principles adopted by the U.S. Constitution in 1788.[15] Building upon those embedded, core principles, eleven states voted to add the Bill of Rights, which includes the Fourth Amendment, to protect democratic goals by limiting the power of the newly established government in 1791.[16] Accordingly, the Fourth Amendment prohibits the federal government, and the individual states via the

[12] *See Carpenter*, 138 S. Ct. 2206, 2218 (2018) ("Only the few without cell phones could escape this tireless and absolute surveillance.").

[13] *See, e.g.*, Boyd v. U.S., 116 U.S. 616, 635 (1886) ("It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon. Their motto should be *obsta principiis*.") (emphasis in original).

[14] *See, e.g.*, Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1207–08 (2016).

[15] *See id.* at 1207 ("The law lords' rejection of general warrants in *Entick*, *Wilkes*, and *Leach* traced its origin, at least as argued in the seventeenth century, to the 1215 Magna Carta.").

[16] *See id.* at 1305.

Fourteenth Amendment, from searching or seizing property without a warrant based on probable cause.[17]

[12] Exactly one century later, Nikola Tesla developed the idea for wireless telegraphy (i.e., the radio) in 1891; or, perhaps, the radio wasn't created until 1909 when Guglielmo Marconi received the Nobel Prize in Physics for its invention.[18] In any case, the invention of radio transmissions evolved into the communication systems that smartphones utilize to send and receive data today.[19]

[13] This wide swath of history influencing the interpretation of the Fourth Amendment within the context of CSLI data, ranging from 1215[20] until 2018 when *Carpenter* was decided,[21] shows the inherent difficulty in defining a conclusive frame of reference to extrapolate the drafters' intent, especially when the radio would not be invented for at least 100 years after its ratification. For brevity's sake, only the most essential English common law opinions will be noted for their initial influence on the drafters of the

[17] *See* U.S. CONST. amend. IV; *see also* U.S. CONST. amend. XIV § 1. *See generally* Wolf v. Colorado, 338 U.S. 25, 27–28 (1949) ("The security of one's privacy against arbitrary intrusion by the police—which is at the core of the Fourth Amendment—is basic to a free society… and as such enforceable against the States through the Due Process Clause [of the Fourteenth Amendment]."), *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961) (holding that evidence obtained by unconstitutional search was inadmissible via exclusionary rule and abrogating that aspect of *Wolf*).

[18] *See* DAVID J. KENT, TESLA: THE WIZARD OF ELECTRICITY 121, 126–27 (Fall River Press, 2013) (noting also that the U.S. Supreme Court concluded that Marconi infringed on Tesla's patent No. 645576 after Tesla's death).

[19] *See* Carpenter v. United States, 138 S. Ct. 2206, 2225 (2018) (Kennedy, J., dissenting) ("When a cell phone user makes a call, sends a text message or e-mail, or gains access to the Internet, the cell phone establishes a radio connection to an antenna at a nearby cell site.").

[20] *See* Donahue, *supra* note 14, at 1207.

[21] *See Carpenter*, 138 S. Ct. 2206.

Fourth Amendment and continuing with the U.S. Supreme Court tasked with interpreting and applying the drafters' words as they reverberate throughout history.

A. The Original Intent of the Fourth Amendment: To Preempt Tyranny

[14] A primordial evil that the drafters of the Fourth Amendment sought to eliminate was the writ of assistance issued against American colonists, which granted English revenue officers the power to search any place they suspected to contain smuggled goods.[22] It was this intolerable intrusion without appreciable limits that the first draft of the Fourth Amendment, penned by James Madison, intended to prohibit.[23] Following some revision, the states ratified the Fourth Amendment, but "virtually no information appears to exist about ratification debates regarding the amendment in the individual states."[24]

[15] Yet, a seminal case, *Entick v. Carrington*, predicted the colonists' eventual angst towards such general writs in a similarly aggravating trespass suit for forceful entry of the plaintiff's house, breaking open his desk, and searching his private—and allegedly seditious—papers, which were then taken and made public.[25] Judging the legality of such general warrants,

[22] *See* Boyd v. United States, 116 U.S. 616, 624-25 (1886); *see also* Stanford v. Texas, 379 U.S. 476, 481 (1965) ("Vivid in the memory of the newly independent Americans were those general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists. The hated writs of assistance had given customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws.").

[23] *See* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 1044–45 (2011).

[24] *Id.* at 1051.

[25] *See* Entick v. Carrington, 95 E.R. 807, 812 (King's Bench 1765) ("A power to issue such a warrant as this, is contrary to the genius of the law of England, and even if they had found what they searched for, they could not have justified under it; but they did not

Charles Pratt, who would become Lord Camden, expressed many critical thoughts, including: "[W]e can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society; for papers are often the dearest property a man can have. . . [thus] we are all of opinion that this warrant is wholly illegal and void." [26]

[16] More than a century later, the U.S. Supreme Court in *Boyd v. United States*, quoting Lord Camden's remarks at length, used these statements to clarify the core principles supporting the Amendment, as they demonstrated that "every American statesman . . . was undoubtedly familiar with this monument of English freedom . . . [and] that its propositions were in the minds of those who framed the Fourth Amendment to the Constitution, and were considered as sufficiently explanatory of what was meant by unreasonable searches and seizures."[27] The *Boyd* Court continued by expressing its determination that the duty to resist encroachments upon constitutional rights from the beginning (i.e., *obsta principiis*) and to liberally construe constitutional protections militate against steady or even sporadic deviations from the specific protections granted by the Constitution.[28] Moreover, the Court conceded that even though the

find what they searched for, nor does it appear that the plaintiff was author of any of the supposed seditious papers mentioned in the warrant, so that it now appears that this enormous trespass and violent proceeding has been done upon mere surmise . . . . [and if allowed] this would be worse than the Spanish Inquisition . . . .").

[26] *Id.* at 817–18; *see* Donohue, *supra* note 14, at 1197–99, 1197 n.70; *see also Stanford*, 379 U.S. at 484 ("Thereafter, the House of Commons passed two resolutions condemning general warrants, the first limiting its condemnation to their use in cases of libel, and the second condemning their use generally.").

[27] *Boyd*, 116 U.S. at 626–27; *see* Donohue, *supra* note 14, at 1297 ("General warrants stood as the foremost example of the abridgement of individual liberty rights.").

[28] *See Boyd*, 116 U.S. at 633–35 ("It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. This can only be obviated by adhering to the rule that constitutional

Legislature may be similarly motivated to resist such encroachments, the vast amount of public business it conducts often prevents immediately reactive, or effectively proactive, legislation.[29] Add almost another century, and while similarly supportive of Lord Camden's disdain for general warrants, the Court in *Stanford v. Texas* noted:

> Two centuries have passed since the historic decision in *Entick v. Carrington*, almost to the very day. The world has greatly changed, . . . [b]ut the Fourth and Fourteenth Amendments guarantee to John Stanford that no official of the State shall ransack his home and seize his books and papers under the unbridled authority of a general warrant—no less than the law 200 years ago shielded John Entick from the messengers of the King.[30]

Thus, the *Stanford* Court relied on English legal history to reject the constitutionality of general warrants, requiring more specific objectives to limit the scope of a warrant.[31]

[17] Also appreciative of this history, the Court in *United States v. Verdugo-Urquidez* concluded that the "available historical data show . . . that the purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government . . . ."[32] This

provisions for the security of person and property should be liberally construed. . . . It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon. Their motto should be obsta principiis.").

[29] *See id.* at 635 ("We have no doubt that the legislative body is actuated by the same motives; but the vast accumulation of public business brought before it sometimes prevents it, on a first presentation, from noticing objections which become developed by time and the practical application of the objectionable law.").

[30] *See Stanford*, 379 U.S. at 486 (emphasis added).

[31] *See id.* at 485–86.

[32] United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990) (noting also that "[t]he Framers originally decided not to include a provision like the Fourth Amendment,

protection against government overreach was so crucial in the minds of the Founders "[t]hat initially the Fourth Amendment was to be placed in Article I, § 9 [which] underscores the Founders' intent to restrict Congress from being able to abridge the people's right to be secure in their homes from unwanted government intrusion."[33] Moreover, as the influential model of English jurisprudence relates, "[b]y 1768, the Court of Common Pleas, the Court of the King's Bench, members of Parliament, and the public had come to reject the granting of general warrants as an exercise of tyrannical power."[34]

[18] By acknowledging the legacy of pivotal English cases and its effect on the drafters, courts have concluded that the Fourth Amendment specifically targeted general warrants as a threat to our democracy due to its history of corruption.[35] Additionally, the drafters intended to limit the Government's ability to search and seize a citizen's property without sufficient cause and specific scope determined by the judiciary as a barrier to prevent tyranny.[36] Thus, the Fourth Amendment embodies the early outrage against boundless writs of assistance, and similarly unbridled general warrants, due to fears of oppressive use as a remnant of past political discord.

---

because they believed the National Government lacked power to conduct searches and seizures.").

[33] Donohue, *supra* note 14, at 1321 ("When the First Congress moved the clause that now forms the Fourth Amendment to an appendix, it was because it did not make sense to insert it into the main body, to which the members of the Convention had previously affixed their signatures.").

[34] *Id.* at 1325.

[35] *See id.*

[36] *See id.*

B. The Great *Katz*-by: Building Expectations of Privacy

[19] Moving along to 1967, the Court departed from the traditional trespass analysis when it declared that "the Fourth Amendment protects people, not places."[37] In *Katz v. United States*, where novel eavesdropping technology attached to the outside of a public telephone booth was used to record Katz's allegedly illegal telephone communications, the Court noted that the FBI had not presented any facts demonstrating probable cause to a neutral judge who could then authorize a search warrant pursuant to the Fourth Amendment's directives.[38] Lacking such judicial oversight, the Court refused to exempt what the Government argued was a non-trespassory search from the restrictions of the Fourth Amendment.[39] On the contrary, the Court concluded: "Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[40] Accordingly, the Court reversed Katz's conviction and held that a showing of probable cause resulting in a judicially authorized search warrant "to be a constitutional precondition of the kind of electronic surveillance involved in this case."[41]

---

[37] Katz v. United States, 389 U.S. 347, 351, 353 (1967) ("Once this much is acknowledged, and once it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.").

[38] *See id.* at 356–57. ("'Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes,' . . . and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment ….") (quoting United States v. Jeffers, 342 U.S. 48, 51 (1951) (footnote omitted)).

[39] *See id.* at 357–59.

[40] *Id.* at 359.

[41] *Id.*

[20] Additionally, Justice Harlan's concurrence in *Katz* emphasized the analysis of reasonable expectations of privacy and its relation to Fourth Amendment protections.[42] He posited that "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[43] Encouraging this departure from the rigid, physical trespass requirement to invoke the Fourth Amendment, Justice Harlan concluded that such limits "in the present day, [are] bad physics as well as bad law . . . ."[44]

[21] Even now, *Katz*'s reasoning and conclusions, along with Justice Harlan's concurrence, remain informative not only because the *Carpenter* Court viewed *Katz* as the genesis of the reasonable expectation of privacy inquiry but also for its treatment of new surveillance technology that allowed investigators to avoid the traditionally dispositive element of trespass.[45] No one should fault the FBI for attempting to enforce the law with all the tools at their disposal; but, more significantly, the Court's holding should be recognized for its determination to prevent the use of such invasive surveillance technology without judicial involvement—the

[42] *See id.* at 360–62 (Harlan, J., concurring); *see also* Peter Winn, *Katz and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 7 (2009) ("Within a year, the Supreme Court started to use Harlan's 'reasonable expectation of privacy' test as the standard in its Fourth Amendment jurisprudence. Within a decade, Harlan's test became so familiar that the Court officially recognized it as the essence of the *Katz* decision—a rare instance where a concurrence effectively replaced a majority opinion.") (footnotes omitted).

[43] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[44] *Id.* at 362.

[45] *See* Carpenter v. United States, 138 S. Ct. 2206, 2227 (2018) (Kennedy, J., dissenting).

prerequisite developed by the drafters of the Fourth Amendment to restrain investigatory power.[46]

C. Party of Three: Third-Party Doctrine in *Miller* & *Smith* to Limit *Katz*

[22] In his dissent in *Carpenter*, Justice Kennedy credited *United States v. Miller* and *Smith v. Maryland* as important limitations on *Katz*'s holding to protect people over places.[47] The Court in *Miller* held that financial records maintained by a bank pursuant to the Bank Secrecy Act carried no legitimate expectation of privacy when such transactions were voluntarily exposed in the normal course of business, imputing to the depositor an assumption of the risk that such information may be disclosed to the Government.[48] Also finding no appreciable property interest in the bank's records asserted by the defendant, the Court rejected the defendant's argument that the Fourth Amendment had been violated.[49]

[23] Three years later in *Smith*, the Court began its *Katz* analysis by dissecting the legitimate expectation of privacy into its two component parts: the subjective, personal expectation of privacy based on conduct; and the objective, societal expectation of privacy based on reasonable or justifiable recognition of the subjective expectation in relation to the circumstances involved.[50] Once again, the traditional element of trespass

[46] *See Katz*, 389 U.S. at 356 (majority opinion) (noting that a judicial search order could have accommodated the legitimate needs of the FBI by authorizing the limited use of electronic surveillance).

[47] *See Carpenter*, 138 S. Ct. at 2228 (Kennedy, J., dissenting).

[48] *See* United States v. Miller, 425 U.S. 435, 442–43 (1976).

[49] *See id.* at 445.

[50] *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

was absent from the facts of the case, which included a pen register device used to record the numbers dialed from the defendant's telephone.[51] Notably, the pen register was installed on the telephone company's property, and the device did not record the contents of any communications but merely registered the numbers dialed.[52] Thus, the Court found no property interest attached to the defendant on which to base a Fourth Amendment trespass inquiry and instead focused its attention on whether a legitimate expectation of privacy existed, as reminiscent of Justice Harlan's focus in *Katz*.[53]

[24] While the defendant argued that because he made the calls from within the privacy of his house, where the Fourth Amendment's protections are traditionally the strongest, the Amendment was violated, the Court concluded:

> Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.[54]

[25] Essentially, the Court found that no matter the location from which a telephone number is dialed, that voluntary act assumes the awareness of the dialer that the telephone company will necessarily route the call to the

[51] *See id.* at 741.

[52] *See id.*

[53] *See id.* at 741–42.

[54] *Id.* at 743.

recipient and record the details of that connection for business purposes, imputing the assumption of the risk of disclosure that vitiated the defendant's assertion of an expectation of privacy in the numbers he dialed.[55] Moreover, the Court considered the pen register device to be a very limited surveillance tool and stressed that the defendant voluntarily exposed the numbers to recordation by dialing them with an awareness of the telephone company's routing and business functions.[56]

[26] Following in *Katz*'s momentous wake, *Miller* and *Smith* certainly narrowed the field of legitimate expectations of privacy, barring such an expectation within third-party business records, especially when there is evidence of voluntary exposure leading to an assumption of the risk of potential disclosure.[57] Yet, comparing both the financial records in *Miller* and the pen register in *Smith* to the CSLI data in *Carpenter* is like comparing analog to digital: the similarities as business records are few, and the differences in detail and continuous creation are substantial.[58]

[55] *See id.*

[56] *See Smith*, 442 U.S. at 742, 744.

[57] *See* Carpenter v. United States, 138 S. Ct. 2206, 2228 (2018) (Kennedy, J., dissenting) ("The defendants in those cases could expect that the third-party businesses could use the records the companies collected, stored, and classified as their own for any number of business and commercial purposes."); *see also In re* Application of the United States of America for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (concluding that "[c]ell site data are business records and should be analyzed under that line of Supreme Court precedent.").

[58] *See Smith*, 442 U.S. at 751–52 (Marshall, J., dissenting) ("Accordingly, I would require law enforcement officials to obtain a warrant before they enlist telephone companies to secure information otherwise beyond the government's reach.").

D. Encouraging the Future: Novel Technological Challenges in *Kyllo* & *Jones*

[27] The new millennium ushered in technology capable of enhancing the limited perspective of human observation in ways previously unimaginable.[59] For instance, in *Kyllo v. United States*, the Court found itself considering the application of a thermal imager used to confirm suspicions of an indoor marijuana operation by detecting heat via infrared radiation, which led to a search warrant that exposed a major criminal enterprise within the petitioner's home.[60]

[28] From the outset, the Court admitted: "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[61] Accordingly, the Court held that information obtained via sense-enhancing technology that would not be otherwise obtainable without a physical intrusion into a constitutionally protected area constituted a search.[62] Moreover, by taking the "long view" perspective of the potential ramifications of its holding, the Court concluded that when "the Government uses a device . . . to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[63]

---

[59] *See generally* Kyllo v. United States, 533 U.S. 27 (2001).

[60] *See id.*

[61] *Id.* at 33–34.

[62] *Id.* at 34–35.

[63] *Id.* at 40 ("While it is certainly possible to conclude from the videotape of the thermal imaging that occurred in this case that no 'significant' compromise of the homeowner's privacy has occurred, we must take the long view, from the original meaning of the Fourth Amendment forward.").

[29] Then, in *United States v. Jones*, investigators utilized a GPS tracking device attached to Jones's wife's Jeep Grand Cherokee to continuously surveil his movements over a 28-day period.[64] The device logged over 2,000 pages of data and recorded Jones's location information with precision of 50 to 100 feet. At trial, the district court, relying on *United States v. Knotts*, admitted the majority of this data, applying the prior precedent that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[65] Previously in *Knotts*, the defendants, unaware of the investigator's ruse to hide a beeper within a chloroform container, unwittingly led narcotics officers to their secret base of operations by stealing the bugged container that transmitted its location along the way to Knotts's secluded cabin.[66]

[30] In contrast to *Knotts*, investigators attached the GPS device to the undercarriage of the vehicle, while it was parked in a public parking garage, in order to track Jones.[67] Further, the device was installed on the vehicle after the warrant expired and outside the authorizing court's jurisdiction.[68] While the Court noted that Jones was not the registered owner of the vehicle, his status as primary driver amounting to a bailee-type property interest was not in dispute and provided a sufficient basis to invoke the Fourth Amendment's protections.[69]

---

[64] *See* United States v. Jones, 565 U.S.400, 402–03 (2012).

[65] United States v. Knotts, 460 U.S. 276, 281 (1983).

[66] *See id.* at 278–79, 285 ("Admittedly, because of the failure of the visual surveillance, the beeper enabled the law enforcement officials in this case to ascertain the ultimate resting place of the chloroform when they would not have been able to do so had they relied solely on their naked eyes.").

[67] *See Jones*, 565 U.S. at 403.

[68] *See id.* at 402–03.

[69] *See id.* at 404, n.2.

[31] As such, the Court distinguished *Knotts* by explaining that the "Government physically occupied private property for the purpose of obtaining information. . . . [leaving] no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[70] Moreover, the Court declared that "[b]y attaching the device to the Jeep, officers encroached on a protected area . . . enumerated in the Fourth Amendment."[71] Most pertinent to CSLI data, which lacks the familiar trespass element, the Court held that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis."[72] Ultimately, the Court in *Jones* affirmed the appellate court's reversal of Jones's conviction because the admission of the GPS evidence, obtained without a proper warrant, violated the Fourth Amendment.[73]

[32] With newfound abilities to see heat or observe a suspect with unescapable yet undetectable remote precision, *Kyllo* and *Jones* stand out as examples of modern technology foisting new challenges on the Court and adding novel layers of complexity to its interpretation of the Fourth Amendment.[74] From sense-enhancing technology to varying degrees of trespass and expectations of privacy, the Court will continue to face similarly perplexing issues as groundbreaking innovations and legal traditions clash along the borders of constitutional protections. The Court, as well as the country, will benefit most from a long-view approach underpinned by *obsta principiis* while anticipating future advancements and

[70] *Id.* at 404–05.

[71] *Id.* at 411.

[72] *Jones*, 565 U.S. at 411.

[73] *Id.* at 404, 413.

[74] *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) ("The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.").

its likely effects on privacy.[75] This approach serves to encourage the technological achievements of the future by avoiding undue restrictions, excepting those provided for in the Constitution, to protect property and its inseparable relation to privacy, and allows society time to react through market influence and political activities, demonstrating public approval or disapproval as a swift indicator of acceptance or condemnation of new technology and its ramifications on privacy.[76]

E. *Carpenter*'s Promotion of Privacy Expectations in CSLI Data to Trigger Fourth Amendment Protection

[33] After noting the unique question presented in *Carpenter*, Chief Justice Roberts, writing for the majority, began by pointing out the shocking statistic that cell phone accounts in the U.S. outnumber Americans by 70 million.[77] The majority opinion, joined by Justices Breyer, Ginsburg, Kagan, and Sotomayor, then relayed the process by which prosecutors requested Carpenter's CSLI data from Sprint and MetroPCS via the Stored Communications Act, resulting in the Government's acquisition of 12,898 location data points.[78] Finally, the Chief Justice reported that Carpenter's pre-trial motion to suppress this data as violative of the Fourth Amendment

[75] *See id.* at 40.

[76] *See* Nw. Airlines v. Minnesota, 322 U.S. 292, 300 (1944) ("[C]omplicated technological facilities that are on the horizon, raises questions that we ought not to anticipate; certainly, we ought not to embarrass the future by judicial answers which at best can deal only in a truncated way with problems sufficiently difficult even for legislative statesmanship.").

[77] Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

[78] *Id.* at 2212 ("That statute, as amended in 1994, permits the Government to compel the disclosure of certain telecommunications records when it 'offers specific and articulable facts showing that there are reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.'" (quoting 18 U.S.C. § 2703(d) (2019))).

was denied by the district court and that ruling was affirmed by the Sixth Circuit.[79]

[34] Moving into its analysis, the Court conceded that "[t]his sort of digital data—personal location information maintained by a third party—does not fit neatly under existing precedents."[80] Instead, the assertion of an expectation of privacy concerning a catalog of one's past movements and the third-party doctrine's preclusion of property and privacy assertions by customers in a company's business records combine in *Carpenter* to form a compromise in favor of privacy due to "the unique nature of cell phone location records" that silently and effortlessly log its user's location.[81] The Court emphasized that, without such a holding prioritizing privacy, the Government could "[w]ith just the click of a button . . . access each [cell phone] carrier's deep repository of historical location information at practically no expense."[82]

[35] Such access troubled the Court for a number of reasons, including its perception of CSLI as a "near perfect surveillance tool" because it follows its user endlessly from public to private places without interruption or scrutiny.[83] Distressingly, the *Carpenter* Court continued by warning that "[i]n fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*."[84] Moreover, the Court equated passively-created CSLI data to the active tracking of a

[79] *Id.* at 2212–13.

[80] *Id.* at 2214.

[81] *Id.* at 2217.

[82] *Id.* at 2218.

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

[84] *Id.*

physically attached ankle-monitor for its similarly inescapable, detailed, and precise catalog of the movements of the monitored person.[85]

[36] Additionally, the majority recognized that historically, investigations were restricted, unofficially but effectively, by a lack of resources and imperfect human faculties.[86] But now, with access to encyclopedic and unyielding CSLI data, investigators may "travel back in time to retrace a person's whereabouts . . . [with no requirement to] even know in advance whether they want to follow a particular individual, or when."[87] As such, the Court was understandably troubled by "this newfound tracking capacity [that] runs against everyone."[88]

[37] Accordingly, the Court rejected the Government's argument that the third-party doctrine should resolve *Carpenter*, stating: "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."[89] The Court's repudiation continued, stating: "The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years."[90]

[38] Moreover, the Court refused to apply the third-party doctrine because it doubted whether cell phone users truly intend to expose their

[85] *See id.*

[86] *See id.*

[87] *Id.*

[88] *Id.*

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

[90] *Id.*

movements to recordation or if participation in modern society's most prevalent and convenient means of communication entailed a voluntary assumption of the risk of disclosure of CSLI.[91] Consequently, the Court recognized Carpenter's claim of an expectation of privacy and that the Government's acquisition of his CSLI data constituted a search.[92] Upon this conclusion, the Court reinforced the typical probable cause requirement, declaring that "an order issued under Section 2703(d) of the [Stored Communications] Act is not a permissible mechanism for accessing historical cell-site records . . . . [but] the Government's obligation is a familiar one—get a warrant."[93] Further, the majority urged "the dissent . . . [to] recognize that CSLI is an entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power . . . . [and w]hen confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents."[94]

[39] Thus, *Carpenter* stands as a pillar of privacy in a rapidly changing world where technology upends traditions, such as the transformation of communication activities from pen and paper to stationary telephone landlines to ever-mobile and increasingly functional cell phones.[95] By

[91] *See id.* at 2220 ("[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.").

[92] *See id.*

[93] *Id*. at 2221.

[94] *Id*. at 2222.

[95] *See Carpenter*, 138 S. Ct. at 2223 ("We 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

rejecting the requested extension of the third-party doctrine and by recognizing the exceptional capacity of advanced business records like CSLI in *Carpenter*, the Court has begun to refine Fourth Amendment jurisprudence illuminated by revealing "modern lights."[96] Yet, the Court intentionally left unanswered the remaining question about what level of protection the acquisition of records detailing less than seven days' worth of CSLI should receive.[97] Consequently, this Article seeks to answer that question by referring to the evolutionary history of Fourth Amendment jurisprudence, the reasoning emphasized by the *Carpenter* Court to arrive at its holding, and the current status of further technological development concerning CSLI data. Finally, it will look to modern society's expectations of privacy in the Digital Age as it continues to disrupt traditions and create new methods of communication and connectivity.

III. ARGUMENT

[40] While the Court's reasoning in *Carpenter* is sound, it fails society by not categorically resisting the Government's utilization of CSLI records as a potentially omnipresent and infallible surveillance tool tirelessly tracking its user.[98] Admittedly, the temptation to provide law enforcement

gathered by a third party does not make it any less deserving of Fourth Amendment protection.").

[96] *Id.* at 2246 (Thomas, J., dissenting) (discussing the Fourth Amendment).

[97] *See id.* at 2217, n.3 ("[W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be.").

[98] *See* United States v. White, 401 U.S. 745, 756 (1971) (Douglas, J., dissenting) ("Electronic surveillance is the greatest leveler of human privacy ever known. How most forms of it can be held 'reasonable' within the meaning of the Fourth Amendment is a mystery . . . . [T]he concepts of privacy which the Founders enshrined in the Fourth Amendment vanish completely when we slavishly allow an all-powerful government, proclaiming law and order, efficiency, and other benign purposes, to penetrate all the walls and doors which men need to shield them from the pressures of a turbulent life around them and give them the health and strength to carry on.").

with a potent investigative arsenal is certainly difficult to overcome, but the Court has encountered similarly complex situations involving the competing interests of privacy and justice before.[99] In 1948, the Court cogently stated, "[T]he forefathers, after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of some criminals from punishment."[100] It is this greater danger—that CSLI may be used as an effortless and generally applicable surveillance tool to undermine privacy—that must be prevented either by continued judicial interpretation of the Fourth Amendment or by rousing Congress to action.

[41] Preventing the aforementioned dangers does not require alteration of the Constitution, but it does require flexible, judicial interpretation within circumstances far afield from the drafters' contemplation, yet similarly susceptible to their fear of an oppressive executive government corrupted by too much power and left unchecked by the other branches.[101] Any evaluation of constitutional issues raised by novel technology should channel not only the drafters' constructive brilliance to mitigate misconduct but also their hesitancy to provide any branch or group of state actors with the unchecked ability to tyrannize American citizens. Such tyranny would be inevitable by granting easy access to an encyclopedic record of a person's past movements with enough detail to humiliate, oppress, subjugate, or coerce, contravening our democratic goals.[102]

---

[99] *See* United States v. Di Re, 332 U.S. 581, 595 (1948).

[100] *Id.*

[101] *See* Rawlings v. Kentucky, 448 U.S. 98, 105 (1980) (quoting Rakas v. Illinois, 439 U.S. 128, 149–50 n.17 (1978)) ("[This Court has] emphatically rejected the notion that 'arcane' concepts of property law ought to control the ability to claim the protections of the Fourth Amendment.").

[102] *See* Boyd v. United States, 116 U.S. 616, 632 (1886) ("It may suit the purposes of despotic power, but it cannot abide the pure atmosphere of political liberty and personal freedom.").

[42] Conversely, Justice Thomas denounced the holding in *Carpenter*, lamenting in his dissent, "[w]hether the rights [the Founding Fathers] ratified are too broad or too narrow by modern lights, this Court has no authority to unilaterally alter the document they approved."[103] But such static rigidity forces stagnation and lethargy in interpretation; in fact, it is the thrust of this Article that the Fourth Amendment should be considered with both a firm grasp of the Founders' original intent and a steady eye towards the future in which "modern lights" lead the way.[104] Although the Constitution often serves to divide on matters of interpretation, perhaps an issue that affects almost everyone, like the use of CSLI as seen in *Carpenter*, will offer an opportunity for a collaborative resolution.

A. Advancing *Carpenter*'s Reasoning to its Logical End by Requiring a Warrant for any Amount of CSLI Data

[43] In his dissent in *Carpenter*, Justice Gorsuch questioned the majority's belief that acquisition of seven days' worth of CSLI data sufficed to establish that a search occurred.[105] This time-threshold question is left largely unanswered in the majority's opinion, but their focus seems to point to this number of days as representative of a sufficient amount of data from which to compile a mosaic of the individual's habits and routines, revealing "an intimate window into a person's life . . . ."[106] Professor Kerr named the mosaic theory while describing the D.C. Circuit's aggregation of the

[103] Carpenter v. United States, 138 S. Ct. 2206, 2246 (2018) (Thomas, J., dissenting) (discussing the Fourth Amendment).

[104] *See Boyd*, 116 U.S. at 635 ("[A]dhering to the rule that constitutional provisions for the security of person and property should be liberally construed. A close and literal construction deprives them of half their efficacy, and leads to gradual depreciation of the right, as if it consisted more in sound than in substance. It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon. Their motto should be obsta principiis.").

[105] *See Carpenter*, 138 S. Ct. at 2266–67 (Gorsuch, J., dissenting) (asking several additional questions to which he answers, "We do not know.").

[106] *Id.* at 2217.

challenged searches "as a collective sequence of steps rather than as individual steps."[107]

[44] Although data collected from sequential searches would often provide a more detailed extrapolation about the individual when, as in Carpenter's case, there is a focus on the individual's past movements during specific intervals, a single day's CSLI records—a solitary tile of the mosaic, as it were—could be just as damning as acquisition of CSLI records detailing years of location information.[108] Therefore, in appreciating the importance of CSLI data, its qualitative significance and its quantitative abundance vary in investigative value depending on its intended uses at trial. Moreover, the Court added another unique attribute by finding that "the retrospective quality of the data here gives police access to a category of information otherwise unknowable."[109] Knowing the unknowable, as in utilizing omnipresent CSLI records, likely leads not just to excessive investigative power but to an undeniable supremacy in surveillance tactics.[110]

[45] In avoiding a conclusive rule on this time-threshold requirement, the Court stated that "we need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from

[107] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 313 (2012) (describing how the D.C. Circuit applied that test in *Maynard* to GPS surveillance of a car, holding that GPS surveillance of a car's location over twenty-eight days in the aggregate triggers Fourth Amendment protection); *see* Maynard v. United States, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 565 U.S. 400 (2012).

[108] *See Carpenter*, 138 S. Ct. at 2212 (describing the Government's acquisition of records containing 12,898 location points cataloging Carpenter's movements with an average of 101 data points per day).

[109] *Id.* at 2218.

[110] *See* Kyllo v. United States, 533 U.S. 27, 40 (2001).

Fourth Amendment scrutiny, and if so, how long that period might be."[111] Instead, the Court only reached the rather limited conclusion that "[i]t is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search."[112] Asking if acquisition of less than seven days of CSLI constitutes a search only repeats Justice Gorsuch's refrain, "[w]e do not know."[113]

[46] While the idea that seven days is sufficient seems to rest on the mosaic theory, that number does carry an impression of arbitrary speculation rather than resolute logic. The Court's reasoning supportive of a week-long threshold, if advanced to its logical conclusion, carries greater weight when the rationale to require a warrant extends to *all* CSLI data, regardless of the number of days obtained. In fact, such an extension circumvents Justice Kennedy's criticism that, although the Government requested seven days of CSLI records, it actually obtained only two days of CSLI records.[114] Moreover, even a single day, as in Carpenter's case, can log over 100 CSLI data points, meaning that a more abstract but still remarkably detailed mosaic of individual's past movements can be created without multiple days' records.[115] Accordingly, the Court's insistence on obtaining a warrant before disclosing seven days of CSLI records should be expanded to include *all* CSLI records to provide greater consistency and

[111] *Carpenter*, 138 S. Ct. at 2217 n.3.

[112] *Id.*

[113] *Id.* at 2267 (Gorsuch, J., dissenting). *But see* United States v. Chadwick, 433 U.S. 1, 9 (1977) ("What we do know is that the Framers were men who focused on the wrongs of that day but who intended the Fourth Amendment to safeguard fundamental values which would far outlast the specific abuses which gave it birth.").

[114] *See Carpenter*, 138 S. Ct. at 2226 (Kennedy, J., dissenting).

[115] *See id.* at 2212.

sharper logic pursuant to its *Katz* analysis in *Carpenter*, recognizing privacy expectations worthy of Fourth Amendment protection.[116]

B. Advancing Technology: Encouraging the Future Without Forfeiting Privacy

[47] Although it is impossible to predict an exact rate of progression for any technology,[117] CSLI capabilities should be evaluated in terms of their potential for quickly advancing technical precision now in development rather than their current limitations. Over seventy years ago, the Court, cognizant of rapidly developing technological innovations, endeavored to avoid "embarrass[ing] the future" with short-sighted, judicial opinions.[118] Likewise in *Carpenter*, the Court emphasized that its decision was narrow, refusing to address issues not directly involved in the case or to adopt an explicit rule for measuring what quantity of CSLI records constitutes a search.[119] Yet, it insisted that "the rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.'"[120]

[48] The Court's forward-thinking rule should be commended not only as encouraging future innovation, but also as maintaining a more efficient judicial role in contemplating the succeeding conflicts between law and technology, rather than a more restrictive or myopic perspective subject to frequent revision. Similarly, Professor Kerr has noted "the problem of

[116] *See* United States v. White, 401 U.S. 745, 761–62 (Douglas, J., dissenting) ("[The] extensive intrusions into privacy made by electronic surveillance make self-restraint by law enforcement officials an inadequate protection, that the requirement of warrants under the Fourth Amendment is essential to a free society.").

[117] *See e.g.*, James Bryan Quinn, *Technological Forecasting*, HARV. BUS. REV. (Mar. 1967), https://hbr.org/1967/03/technological-forecasting [https://perma.cc/57EK-2KA3].

[118] Nw. Airlines v. Minnesota, 322 U.S. 292, 300 (1944).

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

[120] *Id.* at 2218 (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).

technological and social change is particularly acute in Fourth Amendment law . . . . [Whereas the] problem of technological change is an occasional topic in many areas; in Fourth Amendment law, it is omnipresent."[121]

[49] While considering technological progress, a central issue in *Carpenter* related to the precision of CSLI data, both in terms of its current limitations and expected advancement.[122] The Court accepted the prediction that, as cell sites continue to proliferate around the country, thereby reducing the size of service areas, and as new technology develops to measure the exact angles of incoming cell signals, CSLI precision will continue to improve in urban as well as rural areas.[123] The majority expressed its awareness of rapid technological advances, stating that "the Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections."[124] Even in his dissent, Justice Kennedy conceded that "[i]t is true that the Cyber Age has vast potential both to expand and restrict individual freedoms in dimensions not contemplated in earlier times."[125]

[121] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 528 (2011).

[122] *See Carpenter*, 138 S. Ct. at 2218 ("The Government and Justice Kennedy contend, however, that the collection of CSLI should be permitted because the data is less precise than GPS information.").

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

[124] *Id.* at 2223 (alteration in original) (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967)).

[125] *Id.* at 2224 (Kennedy, J., dissenting) (citing Packingham v. North Carolina, 137 S. Ct. 1730 (2017)).

[50] Accordingly, CSLI should be evaluated in terms of its potential for quickly advancing technical precision rather than its current limitations, in order to instill greater judicial efficiency by accepting the implications of privacy concerns today and predicting those concerns in the near future.[126] On the horizon, the next generation of cell phones, named 5G, is already in development, and industry leaders forecast that by 2024, "5G will reach 40 percent population coverage and 1.5 billion subscriptions, making it the fastest generation ever to be rolled out on a global scale."[127] With 5G connectivity and the promise of quicker connections by using new frequencies of the radio spectrum, the likely result becomes the production of even more CSLI data with increasingly accurate precision.[128]

C. Society's High Expectations of Privacy in the Digital Age

[51] Societies all over the world have begun to wrestle with the competing and conflicting interests of privacy and convenience as new technology provides greater expediency and connectivity to the detriment of privacy concerns.[129] But before discussing society and privacy, an important distinction should be explained regarding communication information. As Professor Kerr, writing on the Stored Communications Act (SCA), concisely explained, "[t]he SCA gives greater privacy protection to content information for reasons that most people find intuitive: actual contents of messages naturally implicate greater privacy concerns than

[126] *See* Fredrik Jejdling, *Ericsson Mobility Report: Letter from the publisher*, ERICSSON 2 (Nov. 2018), https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-november-2018.pdf [https://perma.cc/LEU6-4CQC] ("As 5G hits the market, the mobile ecosystem is larger and more widespread and extensive than ever . . . . This is driven by new, innovative solutions that reuse existing infrastructure and available spectrum.").

[127] *Id.*

[128] *See id.*

[129] *See infra* notes 140–53 and accompanying text.

information (much of it network-generated) [like CSLI] about those communications."[130] This difference in classification prescribes a higher burden on law enforcement seeking disclosure of content—probable cause for a search warrant—than does the "reasonable grounds" required for disclosure of non-content records.[131]

[52] While a large portion of society may be familiar with the words "probable case," many may be unsure of what that standard means legally. Previously, the Court defined probable cause "under the Fourth Amendment [as] where the facts and circumstances within the affiant's knowledge, and of which he has reasonably trustworthy information, are sufficient unto themselves to warrant a man of reasonable caution to believe that an offense has been or is being committed."[132] This higher standard restrains improper actions to satisfy "official curiosity" more so than the lower "reasonable grounds" standard required by the SCA, in which "law enforcement need

[130] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1228 (2004); s*ee also id.* at 1243 (noting, as professors are wont to do, that: "[t]he SCA needs significant legislative attention to bring its grade up from a 'B' to an 'A.'"); Riley v. California, 573 U.S. 373, 386 (2014) (holding that police officers must generally secure a warrant before conducting a search of a cell phone's contents).

[131] *See* 18 U.S.C. § 2703(d) (2012); Alexandra D. Vesalga, *Location, Location, Location: Updating the Electronic Communications Privacy Act to Protect Geolocational Data*, 43 GOLDEN GATE U. L. REV. 459, 472 (2013) ("In addition to the status of a communication as 'stored,' the distinction between 'content' and 'non-content' has a substantial effect on the way communications data may be obtained by the government. By the SCA's standards, when the 'content' of a communication is sought, a search warrant is required in most cases. However, when 'non-content' records of stored communications or subscriber information are sought, they can be obtained directly from the third party that stores the individual's information, such as a website, ISP, or mobile service provider, through a court order.").

[132] Berger v. New York, 388 U.S. 41, 55 (1967).

only show that the cell-site evidence *might* be pertinent to an ongoing investigation."[133]

[53] Following disputes involving CSLI, courts that have classified CSLI data have generally determined it to be "stored records," not amounting to content that is worthy of the higher standard of protection.[134] But preceding those disputes, the Senate report referring to the Electronic Communications Privacy Act (ECPA) in 1986, of which the SCA is a part, described the belief that the ECPA "represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies."[135] Unfortunately for the prolonged efficacy of the ECPA, society and technology have grown by leaps and bounds since 1986; as law enforcement seeks to satisfy investigative needs with innovative tools, a clear imbalance has resulted with public outcry demanding revision in favor of increasing privacy protections.[136]

1. Modern Reality of Cell Phone Usage

[54] The growing number of cell sites and the increasingly creative placement of these sites represent the exponential growth of cell phone usage.[137] Additionally, this usage reflects the expansive functionality of

[133] United States v. Morton Salt Co., 338 U.S. 632, 640, 652 (1950); 18 U.S.C. § 2703(d) (2012); Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (emphasis added).

[134] *See, e.g.*, *In re* United States, 727 F. Supp. 2d 571, 574 (W.D. Tex. 2010) ("Most courts have assumed (with little or no discussion) that historical CSLI may be obtained under the SCA because it only amounts to stored records.").

[135] S. REP. NO. 99-541, at 5 (1986).

[136] *See* Steven M. Harkins, *CSLI Disclosure: Why Probable Cause is Necessary to Protect What's Left of the Fourth Amendment*, 68 WASH. & LEE L. REV. 1875, 1894 (2011).

[137] *See Carpenter*, 138 S. Ct. at 2211 ("Although cell sites are usually mounted on a tower, they can also be found on light posts, flagpoles, church steeples, or the sides of buildings.").

smart phones, including the obvious communication functions but also applications for everything from mobile banking to navigation assistance that frequently connect with cell sites to send and receive data.[138]

[55] Cell carriers collect this data not only to log roaming charges and improve coverage, but also to sell the aggregate location data to data brokers after removing individual identification information.[139] These sales belie an important fact of CSLI data collection: location data must be worth something; however, after reports of mishandling this information surfaced, some carriers vowed to limit this practice of selling cell phone location data to protect its customers.[140] If private companies acknowledge the dangers of allowing CSLI data to fall into the wrong hands, public policy should likewise endeavor to protect this sensitive data by establishing a high burden for disclosure.[141]

[138] *See id.* ("Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features.").

[139] *See id.* 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. In addition, wireless carriers often sell aggregated location records to data brokers, without individual identifying information of the sort at issue here.").

[140] *See* Jennifer Valentino-DeVries, *Largest Cellphone Carriers to Limit Sales of Location Data*, N.Y. TIMES (June 19, 2018), https://www.nytimes.com/2018/06/19/technology/verizon-att-cellphone-tracking.html [https://perma.cc/PT2X-JYUG].

[141] *See id.*

2. New Legislation Including California's Consumer Privacy Act & the European Union's General Data Protection Regulation

[56] On May 25, 2018, the European Union's General Data Protection Regulation (GDPR) became effective and introduced a novel privacy paradigm, wherein personal privacy is protected by insisting that companies maintain only the least amount of personal data and only for as long as strictly necessary for a specific purpose.[142] Further, the GDPR enjoys an extended reach beyond its territorial borders, wherein U.S. companies with no physical presence in Europe may still be subject to the GDPR.[143] Generally, the GDPR seeks to encourage more attention to designing effective privacy protocols and establish a baseline of privacy interests by statute.[144] Specifically, Article 25 of the GDPR "requires that organizations (i) only collect personal information for a specified purpose; (ii) retain the minimum amount of personal information necessary; and (iii) retain such personal information only as long as necessary."[145] As such, the GDPR makes privacy a priority in an attempt to stay in lockstep with technology and the potential for exposure of sensitive records, and some commentators view the GDPR as "likely [to] become the global standard for data privacy."[146]

---

[142] *See* Kyle Petersen, *GDPR: What (and Why) You Need to Know About EU Data Protection Law*, UTAH B.J., July–Aug. 2018, at 12,16.

[143] *See id.* at 12 ("[The] GDPR applies to organizations established outside the EU that: (i) process . . . personal data of individuals located in the EU; (ii) offer goods or services to individuals located in the EU; or (iii) monitor behavior of individuals located in the EU.").

[144] *See* Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free movement of Such Data and Repealing Council Directive 95/46/EC, 2016 O.J. (L 119) 1, 48.

[145] Petersen, *supra* note 142, at 16.

[146] *See id.* at 15–16.

[57] Similarly proactive, the Swiss government overhauled its surveillance laws in 2011 by enacting the Swiss Criminal Procedure Code (CrimPC) to regulate law enforcement surveillance.[147] By way of comparison, an important distinction is revealed: when "new surveillance methods come online, U.S. agents freely use them unless and until Congress tells them not to through regulation, but Swiss agents may not use them unless and until their Legislature authorizes them to do so."[148] A system like the Swiss CrimPC, although likely incompatible with criminal procedure in the United States, prevents improper applications of new technology by prohibiting the use of that technology until instructed and regulated by the Legislature.[149]

[58] Domestically, California has been willing to enact privacy legislation, and the California Consumer Privacy Act of 2018 (CCPA), which is similar in many aspects to the GDPR, became effective on January 1, 2020.[150] According to the CCPA, "Personal Information" broadly includes any information that "identifies, relates to, describes, is capable of being associated with . . . [or could] reasonably be linked, directly or indirectly, with a particular consumer or household . . ." that is not available to the public.[151] The CCPA seeks to protect personal information, such as "biometric data, internet activity, and consumer profiles based on inferences

[147] *See* Susan Freiwald & Sylvain Métille, *Reforming Surveillance Law: The Swiss Model*, 28 Berkeley Tech. L.J. 1261, 1263 (2013).

[148] *Id.* at 1266 ("For example, before CrimPC, law enforcement agents could use GPS surveillance only in those [areas] that authorized it by statute. In the United States, the FBI felt free to use GPS devices to conduct surveillance without warrants, and scrambled to remove them only after the Supreme Court ruled that such surveillance was a search.").

[149] *See id.* at 1265–66.

[150] *See* Kevin Angle et al., *California Passes Consumer Privacy Act*, WESTLAW J. COMPUTER & INTERNET, Aug. 24, 2018, at 1, 1–2.

[151] *Id.* at 2.

from various bits of data."[152] In fact, the CCPA information website encourages Californians to support the CCPA agenda, which would allow residents to essentially "Own [Their] Personal Information."[153] This potential ownership interest, even if marginal or inferior to other interests, would provide a more traditional basis to assert the protections granted by the Fourth Amendment.[154]

[59] At the federal level, the ECPA Modernization Act of 2017, introduced by Senator Mike Lee and referred to the Judiciary Committee in 2017, sought "to update the privacy protections for electronic communications information that is stored by third-party service providers and for geolocation information in order to protect consumer privacy interests while meeting law enforcement needs, and for other purposes."[155] As of late 2018, this bill is considered to have died in committee.[156]

[60] These pieces of legislation, both foreign and domestic, add credence to the objective aspect of the *Katz* analysis, wherein society expects greater privacy protection and regulation of data collected and maintained by various companies even if simply held as business records.[157] In sum, the

---

[152] *Id.*

[153] CALIFORNIANS FOR CONSUMER PRIVACY, *Own Your Personal Information*, https://www.caprivacy.org/facts/information-ownership [https://perma.cc/268L-GVAL] (providing that a Californian has a property interest in their personal information collected by third parties to parallel the interest in one's papers or other effects kept in a personal safe in the security of their home).

[154] *See* U.S. CONST. amend. IV, cl. 1; *see also* United States v. Jones, 565 U.S. 400, 405 (2012) (asserting that the text of the Fourth Amendment is closely connected to property, through the phrase "in their persons, houses, papers, and effects").

[155] ECPA Modernization Act of 2017, S. 1657, 115th Cong. (2017).

[156] *See S. 1657: ECPA Modernization Act of 2017*, GOVTRACK.US, (last visited Oct. 20, 2018), https://www.govtrack.us/congress/bills/115/s1657 [https://perma.cc/F9YA-HFD6].

[157] *See* Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014) (concluding "that such a subjective expectation of privacy of location as signaled by one's cell phone—even on

GDPR demands companies play by a new privacy rulebook, the Swiss rewrote the investigator's rulebook, and California's CCPA not only marks the frontlines of a privacy battle within that state but is also representative of most, if not all, of the same privacy concerns within every state.[158] Although any piece of legislation must overcome legislative inertia, much like constitutional challenges must overcome *stare decisis*, to enact change, public pressure to advance privacy protections will likely be most effective to achieve those goals.[159]

D. *Carpenter*'s Dissenters: Show Me the Property Interest

[61] Justice Thomas's dissent, in particular, vehemently rejected the idea that the Fourth Amendment could be invoked within a search of someone else's property, meaning that without a property interest or an ensuing trespass vested in the person raising the objection, the Fourth Amendment has no application.[160] Justice Alito continued in a similar vein, denouncing the majority's view that a compulsory process used by the Government to obtain third-party records could constitute a search.[161] In his dissent in *Carpenter*, Justice Kennedy argued that "[t]he last thing the Court should

public roads—is an expectation of privacy that society is now prepared to recognize as objectively reasonable under the *Katz* 'reasonable expectation of privacy' test.").

[158] *See* Petersen, *supra* note 142, at 16; Freiwald & Métille, *supra* note 147, at 1265; Angle et al., *supra* note 150, at 1.

[159] *See* Boyd v. United States, 116 U.S. 616, 635 (1886).

[160] *See* Carpenter v. United States, 138 S. Ct. 2206, 2244 (2018) (Thomas, J., dissenting) ("In cases like this one, a subpoena for third-party documents was not a 'search' to begin with, and the common law did not limit the government's authority to subpoena third parties.").

[161] *See id.* at 2251 (Alito, J., dissenting) ("So by its terms, the Fourth Amendment does not apply to the compulsory production of documents, a practice that involves neither any physical intrusion into private space nor any taking of property by agents of the state.").

do is incorporate an arbitrary and outside limit . . . and use it as the foundation for a new constitutional framework."[162]

[62] To reconcile the dissenting opinions' major objection of a lacking property interest, the creation of a marginal property interest in an individual's CSLI data would align with the traditional trespass element required to invoke the Fourth Amendment's protections against unreasonable searches. In fact, such an interest would serve to bolster the objective prong of the *Katz* analysis by creating a statutory property interest that in turn implicates a reasonable expectation of privacy.[163] California's CCPA may be closest to such a statutory creation and, once operable, will serve as a proof-of-concept that could be used elsewhere as a model of pro-privacy legislation, wherein a consumer who creates business records, like CSLI, by simply going about his or her day would maintain an interest in those records to monitor their proper use until destroyed.[164]

[63] Further, by way of analogy, the Supreme Court could apply the concept of curtilage that extends the protected area of the home beyond the exterior walls of the house to cell phones and CSLI.[165] For example, an individual who owns a cell phone arguably expects that any data created by

[162] *Id.* at 2233 (Kennedy, J., dissenting).

[163] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also* United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) ("Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them upon society. The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement.").

[164] *See* Angle et al., *supra* note 150, at 1.

[165] *See* Florida v. Jardines, 569 U.S. 1, 5-6 (2013) (defining curtilage as "an area . . . immediately surrounding [a] house . . . which we have held enjoys protection as part of the home itself.").

that cell phone functions within and through the cell phone's local operating system.[166] As such, the cell phone as an "effect" protected by the Fourth Amendment becomes the operable property interest, and CSLI data, which in some ways encompasses all of the activities of that cell phone, becomes the related but separate area of *digital curtilage*.[167] Any transference of digital material from that cell phone would carry the attached property interest along the way. It would be as if CSLI created by an individual's cell phone and then sent to a cell carrier for recordkeeping carried not only the enclosed CSLI data but the initial property interest in the cell phone as an effect with it to the cell carrier's repository. The CSLI data becomes the *digital curtilage* of the cell phone or, perhaps, an effect of my effect (i.e., a cell phone's CSLI data as an effect of an effect or digital papers created by an effect). While such an analogy may strain the traditional concepts of curtilage and effects, digital information will likely continue to incorporate more and more personal information, pushing privacy concerns that may originate in an enumerated, protected area into other areas not yet considered to be protected by the Fourth Amendment.[168]

[166] *See* Georgia v. Randolph, 547 U.S. 103, 111 (2006) ("The constant element in assessing Fourth Amendment reasonableness … is the great significance given to widely shared social expectations, which are naturally enough influenced by the law of property, but not controlled by its rules.").

[167] *See* Andrew Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 809 (2016) (proposing "a theory of 'digital curtilage' as a framework to address the definitional and security questions presented by the Internet of Things.").

[168] *See* Brinegar v. United States, 338 U.S. 160, 180–81 (1949) (Jackson, J., dissenting) ("[T]he human personality deteriorates and dignity and self-reliance disappear where homes, persons and possessions are subject at any hour to unheralded search and seizure by the police . . . . [T]he right to be secure against searches and seizures is one of the most difficult to protect.").

E. Further Statutory Action is Needed but Continuing Judicial Interpretation is More Likely

[64] Simply recommending legislation to create either a marginal property interest in CSLI data or a blanket requirement for warrants based on probable cause before the Government may obtain *any* CSLI data, absent exigencies, is not very difficult. It is much more difficult to endure the legislative process. Unfortunately, partisan politics often distracts from, and impedes, worthy legislation, but even hospitable political climates are limited by the substantial amount of time it takes to draft and implement new policies.[169] Therefore, the Supreme Court will likely continue interpreting the Fourth Amendment against new challenges faster than Congress can agree on new legislation. So, the recommendation to insist upon a judicially authorized warrant to obtain *any* CSLI data will resonate most clearly and effectively with the judiciary.[170]

[65] Although, in fairness, Congress passed the Electronic Communications Privacy Act (ECPA) in 1986 to update the wiretap law provision of the Omnibus Crime Control and Safe Streets Act of 1968, seeking to "protect against the unauthorized interception of electronic communications."[171] Even in 1986, the report noted:

> When the Framers of the Constitution acted to guard against the arbitrary use of Government power to maintain surveillance over citizens, there were limited methods of intrusion into the "houses, papers, and effects" protected by the [F]ourth [A]mendment. During the intervening 200

[169] *See* Boyd v. United States, 116 U.S. 616, 635 (1886).

[170] *See Brinegar*, 338 U.S. at 181 (Jackson, J., dissenting) ("Since the officers are themselves the chief invaders, there is no enforcement outside of court."); *see also* Illinois v. Gates, 462 U.S. 213, 275 (1983) (Brennan, J., dissenting) (recognizing "the judiciary's role as the only effective guardian of Fourth Amendment rights . . . .").

[171] S. REP. NO. 99–541, at 1–2 (1986).

> years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions. The telephone is the most obvious example.[172]

This report displays congressional recognition of privacy concerns that follow the introduction of new technology. Despite these concerns, the ECPA authorized law enforcement, upon issuance of a warrant, to use a tracking device, which it defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[173] Cell phones, by way of CSLI, arguably fit this definition.[174] Some courts, however, have disagreed.[175]

[66] Then, in 1999, Congress passed the Wireless Communications and Public Safety Act (WCPSA) "to upgrade 911 emergency services for cell phones around the country."[176] As Owsley explained, "The legislative history of the [WCPSA] reveals that members of Congress were deeply concerned about the statute's privacy protections . . . . [and] manifests congressional intent to safeguard cell phone subscriber's location information."[177] Owsley continued by noting that the Communications Assistance for Law Enforcement Act (CALEA) "not only contemplates the use of location tracking capabilities that cell phones have, but more importantly bars the use of this technology to track a cell phone," and

[172] *Id.*

[173] 18 U.S.C. § 3117(b) (2019).

[174] *See* Brian L. Owsley, *Cell Phone Tracking in the Era of United States v. Jones and Riley v. California*, 48 TEX. TECH L. REV. 207, 220 (2015).

[175] *See In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 150 (E.D.N.Y. 2013) (concluding that CSLI data did not equate to a tracking device).

[176] Owsley, *supra* note 174, at 222.

[177] *Id.* at 223, 225.

concluding that both the WCPSA and CALEA "prevent the government from obtaining location information from cell phone data."[178] But, "[t]he Federal Communications Commission [(FCC)] and its Enhanced 911 initiative requires cell phone carriers to be able to pinpoint the location of their customers in case of an emergency call."[179] Evidently, Congress has attempted to balance privacy interests with exceptions for efficient emergency services.[180]

[67] Yet, in 2011, Harkins wrote "while courts have been struggling with CSLI disclosure order cases for some time, Congress has only recently taken notice and reform legislation does not appear imminent."[181] Of course, Congress has limited capacity each session to accomplish many goals.[182] So, it may be more likely, even probable, that the Court will decide how to handle CSLI data by defining CSLI searches and expounding upon reasonable expectations of privacy.[183] Moreover, "[w]hat is reasonable is a measure for the judiciary to decide when the legislative measure fails . . . . [and] courts must strive to develop a long-lasting jurisprudence based on principles, not technology."[184]

---

[178] *Id*. at 227.

[179] *In re* Application, 727 F. Supp. 2d 571, 580 (W.D. Tex. 2010) ("And although the main motivation behind the 911 initiative has been public safety, it is not surprising that companies are now trying to turn those required investments into commercial opportunities by offering non-emergency tracking for a monthly fee.").

[180] *See id.*

[181] Steven M. Harkins, *CSLI Disclosure: Why Probable Cause Is Necessary to Protect What's Left of the Fourth Amendment*, 68 WASH. & LEE L. REV. 1875, 1922 (2011) (footnotes omitted).

[182] *See id.*

[183] *See id.* at 1922–23.

[184] Mary Graw Leary, *The Supreme Digital Divide*, 48 TEX. TECH L. REV. 65, 95 (2015); *see also* Kerr, *supra* note 121, at 491 ("Skeptics claim that the only guide to what makes an expectation of privacy 'reasonable' is that five Justices say so . . . .").

[68] If the Court must take on the challenge of protecting Americans regarding CSLI disclosures, then Professor Amsterdam's sentiments about the Court will be on full display.[185] He wrote that from "the Supreme Court's difficulties in grappling with the [F]ourth [A]mendment, we observe the Court in the throes of one of its noblest labors."[186]

[69] Similarly laborious, Magistrate Judge Andrew W. Austin suggested the following limitations on CSLI search warrants, stating that "[t]he warrants will be granted only on a showing of probable cause, may only last 45 days (in the case of prospective warrants), and notice on the person tracked is required (although it may be delayed)."[187] He continued by warning that "if all the Government must prove to receive CSLI is that the target has a cell phone and probably engages in crime, then a CSLI warrant would be issued in *every* criminal investigation."[188] By insisting on a showing of probable cause, the protections granted by the Fourth Amendment are enforced, and the further proposal that disclosure of even a single day of CSLI records constitutes a search capable of triggering the Amendment provides the greatest measure of personal privacy and reduces the potential for investigative abuse.[189]

[70] Finally, the Court denied certiorari for a capital murder case with many horrifying details that challenged several evidentiary issues, including

[185] *See generally* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974) (discussing the fluctuation of Supreme Court decisions).

[186] *Id.* at 353.

[187] *In re* Application, 727 F. Supp. 2d 571, 584 (W.D. Tex. 2010).

[188] *Id.* (emphasis in original) (denying a warrant because the request failed to demonstrate probable cause that disclosure would result in the discovery of evidence of a crime. *See id.* at 585).

[189] *See id.* at 576.

the use of historical CSLI data.[190] Even with this denial, the specific contours of how many days' worth of CSLI records constitutes a search and the nuances of privacy expectations will likely be clarified, if not by Congress, then by the Court when later cases provide such an opportunity.

[71] As such, the membership of active Supreme Court Justices will determine the outcome of later challenges. Chief Justice Roberts wrote the majority opinion in *Carpenter*, joined by Justices Ginsburg, Breyer, Sotomayor, and Kagan.[191] Justices Ginsburg and Breyer were born in 1933 and 1938, respectively.[192] Justice Kennedy, born in 1936, retired shortly after writing his dissenting opinion in *Carpenter*.[193] On October 6, 2018, Justice Kavanaugh joined the Court.[194] Among the dissenting Justices in *Carpenter*—Kennedy, Thomas, Alito, and Gorsuch[195]—Justice Kavanaugh may replace Justice Kennedy's seat with a similar ideology on CSLI and the Fourth Amendment, but only time will tell for sure.

IV. CONCLUSION

[72] Nearly every American adult, and those adolescents who have persuaded their parents to get them a cell phone, unwittingly produce an enormous amount of CSLI data that could be used to map a comprehensive history of their past movements, revealing the location and duration of every activity in which they engage. While most of these individuals may never

---

[190] *See* United States v. Torrez, 869 F.3d 291, 295, 299 (4th Cir. 2017) (affirming conviction), *cert. denied*, 139 S. Ct. 2712 (2019).

[191] *See* Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

[192] *See Current Members*, SUP. CT. OF THE U.S., https://www.supremecourt.gov/about/biographies.aspx [https://perma.cc/G3XV-BYMX].

[193] *See id.*

[194] *See id.*

[195] *See Carpenter*, 138 S. Ct. at 2211.

face criminal charges, this data has other, more pernicious applications, such that some cell carriers have discontinued selling aggregate CSLI data to protect their customers' data from abuse. Likewise, the *Carpenter* Court extended the protections of the Fourth Amendment to include reasonable privacy expectations for individual CSLI records by requiring a warrant for disclosure of records of seven days or more.

[73] Yet, from the moment of our nation's founding, we inherited a strong dislike for generally applicable warrants abused by those who would wield them as a weapon against anyone they choose. Resisting this encroachment on privacy is simply another chapter in the book of American resistance to oppressive power without meaningful limits or recourse. Or, perhaps, in the vein of Alexis de Tocqueville's observations, the American experiment continues to add new variables, such as CSLI and other modern technology, that threaten to topple democracy when allowed to be used as a surveillance tool with little judicial oversight. Still, much work remains to adequately protect privacy. If the Fourth Amendment is allowed to erode and become bereft of its core principles to subvert tyranny when those in a position to apply its spirit to modern situations fail or refuse to do so, then more than history will be lost: the future will lose its connection to the accumulation of past experiences and wisdom incorporated within our founding documents.

[74] As societies all over the world react to the privacy dilemma created by advances in technology, many have already instituted greater privacy protections. Similarly, by adhering to the *Katz* analysis to determine reasonable expectations of privacy, the U.S. Supreme Court began to limit the use of CSLI as a surveillance tool in *Carpenter*. But *Katz* and society demand more than the limited holding in *Carpenter*, and the greatest security against its corruptive potential is an all-encompassing warrant requirement inclusive of *all* CSLI disclosures. Until the Court or Congress acts to limit the prospect of the oppressive surveillance power of CSLI data, Americans are vulnerable to abusive instances of "official curiosity" and warrantless searches that would have infuriated the drafters of the Fourth Amendment.

[75] Although carrying a cell phone is a choice, societal expectations dictate the applicability of *Katz* and reject a voluntary exposure argument as seen in *Miller* and *Smith*. Further, this choice carries few alternatives for convenient communication, making cell phone use a ubiquitous activity across the country. As such, digital connectivity and cell phone use will likely continue to increase, as will the ensuing privacy concerns.

[76] Analogizing the protections granted by the Fourth Amendment as a shield to protect, as a mirror to reflect, or even as an antenna to receive input from the past helps to symbolize its importance as a perennial guardian of liberty. An even better fitting metaphor for the Amendment, though, might be as a bridge, connecting our foundational core beliefs to modern reality and linking law with society. Such a bridge provides context and experience to solve any problem because history is the greatest teacher, just as facing new challenges is a great opportunity to learn. If we learn anything from CSLI and its effect on privacy and policy, perhaps it will be that technological convenience for business purposes is easily translatable to investigative purposes, and an Orwellian skepticism may be justly deserved. Therefore, cell phone users as a group consisting of almost every American is too big to allow surveillance of records generated by those cell phones, as they accompany us everywhere and permeate society.

[77] So, when countries around the world enact new privacy legislation, it signals a clear privacy concern; when domestic cell carriers stop selling aggregate CSLI to their detriment, it signals the same; and when California and the *Carpenter* Court begin to address privacy concerns in personal data collected as business records, the pro-privacy signal has been sent successfully. But will it be received, and by whom?