2020

Carpenter: Framing Fourth Amendment Jurisprudence on a Textual Foundation

Seth Essendrop

Carpenter: Framing Fourth Amendment Jurisprudence on a Textual Foundation

Seth Essendrop*

I. Introduction

"This is a chance for you to say anything without repercussions," Michael Scott assured his employees, coaxing them into revealing times when they had violated "business ethics."[1] After several confessions of relatively minor infractions, including Scott's own admission of "time theft," Meredith Palmer copped to a jaw-dropping violation: "I've been sleeping with [a vendor] in exchange for discounts on our supplies and Outback Steakhouse gift certificates."[2] This revelation led to a conflict between the human resources representative who felt duty-bound to report this behavior, and the manager who insisted that his promise of immunity shielded Meredith from consequences for her misconduct.[3]

The scenario described above—a narration of an episode of the popular mockumentary, "The Office"—is entirely fictional, but is nevertheless an apt metaphor for the very real issue of determining how to apply Fourth Amendment protections in an increasingly digital world. While many believe that the Amendment protects their online activities from the prying eyes of government, courts have struggled to determine what data merits Fourth Amendment protections in an ever changing, ever expanding universe of digital information.

Ratified in 1791 as part of the Bill of Rights, the Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[4] As with much of the Bill of Rights, this amendment provided protection against abuses

* J.D. Candidate, 2020, Seton Hall University School of Law; B.E., Stevens Institute of Technology.
[1] *The Office: Business Ethics* (NBC television broadcast October 9, 2008).
[2] *Id.*
[3] *Id.*
[4] U.S. CONST. amend. IV.

suffered by colonial Americans at the hands of the British.[5] The specific evil this amendment sought to remedy was the issuance of "writs of assistance" and "general warrants" which granted law enforcement broad power to perform searches with minimal justification required.[6] The Fourth Amendment enshrined the common law protection of enumerated items—persons, houses, papers, and effects—which protection was grounded in property law, as set forth in *Entick v. Carrington* in 1765.[7] Though privacy was certainly an interest which was buttressed in the context of the textually articulated items aforementioned, the amendment did not guarantee a general right to privacy.[8] And even to the extent that privacy is a protected interest in the Fourth Amendment, its drafters could not possibly have foreseen the advent of the digital age, or the unique challenges presented by the ubiquitous devices and voluminous data that characterize today's world.

Even before the dawn of the digital revolution, the Supreme Court recognized that the property-based conception of the Fourth Amendment, requiring a physical trespass to trigger the warrant requirement, could not protect the privacy of citizens in the face of new technologies. Hence, in 1967, the Court ruled that absence of physical trespass alone could not obviate the need for a warrant.[9] Instead, an action would be a search—and thus require a warrant—if it violated an individual's reasonable expectation of privacy, that is, if the individual demonstrated a subjective expectation of privacy that society considered reasonable.[10]

The advanced technology considered in *Katz v. United States* was a microphone enabling eavesdropping into a phone conversation.[11] Since then, the proliferation of devices, types of data,

[5] Boyd v. United States, 116 U.S. 616, 625–27 (1885).
[6] *Id.*
[7] 95 Eng. Rep. 807, 817 (C.P. 1765).
[8] Katz v. United States, 389 U.S. 347, 350 (1967).
[9] *Id*. at 353 (stating that "the reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.").
[10] *Id*. at 351.
[11] *Id*. at 348.

volume and granularity of data, and the capabilities for using that data in an intrusive manner have added immense complexity to the questions of Fourth Amendment protections.

The number of devices in today's world collecting and transmitting information is staggering. Indeed, the Supreme Court noted in *Carpenter* that cell phones have become ubiquitous in the modern world, almost equating them to appendages of their users.[12] Cell phones have the ability to collect and transmit information regarding location, movement, and also chronicle information related to application usage, use patterns, internet search history, and a plethora of other data points.[13] So varied are the types of devices that can connect to the internet and transmit information that they cannot be generalized as simply phones, computers, sensors, or even smart devices, but are instead referred to generically as, the "Internet of *Things*" (IOT).[14]

The diversity of potential data sources is matched by the variety of data types these sources analyze and disseminate. Wireless carriers collect information relating to internet usage to enable billing.[15] Files and pictures contain metadata (data about data) that provide information about the file such as who created it, when it was created, where it was created, and, in the case of a photograph, who is in the picture.[16] Home devices may measure noise levels, temperature, motion patterns, and more.[17] Practically all smart phones and many other technological items are GPS-

[12] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018)
[13] *See, e.g.*, David Nleld, *All the Sensors in Your Smart Phone and How They Work*, GIZMODO (July 23, 2017, 11:49 AM), https://gizmodo.com/all-the-sensors-in-your-smartphone-and-how-they-work-1797121002.
[14] Dalmacio V. Posadas, Jr., *The Internet of Things: Abandoning the Third-Party Doctrine and Protecting Data Encryption*, 53 GONZ. L. REV. 90, 91–100 (2017)
[15] *Carpenter*, 138 S. Ct. at 2212.
[16] *See* Megan Logan, *The Coolest Stuff You Didn't Know Google Photos Could Do*, WIRED (June 8, 2015, 8:00 AM), https://www.wired.com/2015/06/coolest-stuff-didnt-know-google-photos/.
[17] *See, e.g., 26 Smart Home Sensors*, HOME STRATOSPHERE, https://www.homestratosphere.com/smart-home-sensors/ (last visited Jan. 10, 2019).

enabled and can track location information. Anymore, a large portion of a person's daily activities is chronicled and logged by the devices and applications with which they interact.[18]

Part of the issue, however, in applying Fourth Amendment protection to such data is that the data is actually stored, and in many cases owned by third parties.[19] Indeed, an individual may not even be privy to the information collected about them, much of which is used for business purposes by the entity collecting it.[20] This data, collected, owned, and stored by third-parties—often unbeknownst to the subject—cannot neatly fit within the items given explicit Fourth Amendment protection.

Additionally, while the raw data may be revealing enough, it is now possible to mine and analyze the information for the purpose of deriving powerful insights. Information about an individual's online activity is used to enhance the effectiveness of marketing to both that individual and the public.[21] Facial recognition technology has advanced to the point where persons in photographs can be automatically tagged and identified.[22] Banks and credit card companies are able to detect fraudulent activity by comparing transactions against the known patterns in a customer's financial history.[23] Political campaigns mine social media information to target voters

[18] *See* F.T.C., *Internet of Things: Privacy and Security in a Connected World* 14–15 (2015) (discussing the data-collecting capabilities of smart devices currently on the market).

[19] *See, e.g.*, *Privacy Policy*, GOOGLE (May 25, 2018), https://policies.google.com/privacy#infocollect (detailing various types of information Google collects on its users and how it collects this information. While some of this information is stored on the client side, the policy explicitly states that some of the technologies used to store information are "databases and server logs").

[20] *See, e.g.*, *Carpenter*, 138 S. Ct. at 2212 (discussing the fact that CSLI is collected for business reasons "including finding weak spots in their network and applying 'roaming' charges when another carrier routes data through their cell sites").

[21] *Privacy Policy*, *supra* note 19 ("We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results.").

[22] In fact, this is the subject of litigation against Facebook citing violation of privacy rights. *See* In re Facebook Biometric Info. Privacy Litig., 326 F.R.D. 535, 540 (N.D. Cal. 2018) (detailing the process by which Facebook automatically identifies persons in photographs and provides tagging suggestions on the basis thereon).

[23] Jungwoo Ryoo, *Machine Learning and Big Data Know It Wasn't You Who Just Swiped Your Credit Card*, GOVTECH (Nov. 27, 2017), http://www.govtech.com/fs/Machine-Learning-And-Big-Data-Know-It-Wasnt-You-Who-Just-Swiped-Your-Credit-Card.html.

and hone their message to appeal to those voters.[24] These and other evolving technologies and tools further encroach on the privacy of individuals, even when the data itself would not have been revealing without them.

Some may indeed be alarmed by the revelation that the technologies and services they use are in turn being used to monitor them. But, however uncomfortable it may seem, the collection of user data by private actors does not run afoul of the Fourth Amendment, even though a warrant may be required if the same surveillance were to be performed by state actors.[25] What result, then, when the government, without a warrant, co-opts a private party's legitimate surveillance data about their clientele?

Despite the contention of some that the Fourth Amendment should, and in fact, does provide protection for Americans' digital information, courts have been hesitant to provide blanket protection to this data.[26] In *Katz*, the Supreme Court announced a test, triggering the Fourth Amendment warrant requirement when a search violates an individual's reasonable expectation of privacy.[27] Such a privacy-based approach may seem to fortify data protection, but in reality, that has not been the outcome of its application in practice.[28]

---

[24] Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018) https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html (explaining how Cambridge Analytica analyzed Facebook profile information on 50 million American voters to provide insights enabling the influence of their votes).

[25] Even an unreasonable search conducted by a third party who then reveals the content searched to the police is not a Fourth Amendment violation, so long as the third party was not acting on behalf of the government. United States v. Jacobsen, 466 U.S. 109, 113–14 (1984). This is known as the private search doctrine, and is applied, for example in the context of illicit digital content that service providers may find in the accounts of their users. *See* United States v. Reddick, 900 F.3d 636, 638–40 (5th Cir. 2018). Companies continually scan user content, and when such illicit material is found, they report it to law enforcement. *Id.* Though, in effect, this is the same as 24-hour surveillance, the fact that it is done by third-parties shields such evidence from the Fourth Amendment warrant requirement. *Id*.

[26] John M. Junker, *Criminal Law: The Structure of the Fourth Amendment: The Scope of the Protection*, 79 J CRIM. L. & CRIMINOLOGY 1105, 1125–26 (1989) (remarking that "*Katz* seems to have been to provide an additional ground for denying fourth amendment protection by refusing 'legitimacy' to assertions of privacy in [multiple contexts]").

[27] 389 U.S. 347, 352–54 (1967).

[28] Junker, *supra* note 2626, at 1125 (stating that "[w]hat is remarkable . . . is how little was changed by *Katz*'s abandonment of the 'trespass' standard of *Olmstead* . . . .").

This is due, in large part, to the development of the "third-party doctrine," which states that information willingly provided to a third-party is not subject to a warrant requirement.[29] A cursory glance at the privacy policies and terms of service of popular web sites, applications, and services will reveal that each is collecting data on their users, and storing this information on their technology infrastructure for use in a myriad of business applications.[30] Thus, the third-party doctrine placed a large amount of digital information outside Fourth Amendment protection, enabling law enforcement to procure through subpoenas the data to which the doctrine applies.

In *Carpenter v. United States*, however, the Supreme Court held that law enforcement is required to obtain a warrant before obtaining multiple days of cell-site location information ("CSLI") from a suspect's cellular service provider.[31] The holding of the case was limited to the factual circumstances at issue; the Court did not announce a rule, and did not clarify with precision where the government crossed the threshold triggering Fourth Amendment protections, only that law enforcement acted unconstitutionally.[32] But, the mere fact that the third-party doctrine did not control in this case is significant, and will lead lower courts to divine factors from the *Carpenter* decision which would mandate a warrant for searches which would otherwise be considered reasonable.[33]

In this Comment, I will suggest a rationale for the *Carpenter* decision which would both bind it explicitly to the text of the Fourth Amendment and simplify the application of the *Carpenter* ruling to other cases. Additionally, while acknowledging that some digital content falls within the

[29] *See* United States v. Miller, 425 U.S. 435, 440–43 (1976); *see also* Smith v. Maryland, 442 U.S. 735, 742–44 (1979).
[30] *E.g.*, *Privacy and Cookie Policy*, DUNKIN DONUTS, https://www.dunkindonuts.com/en/privacy-policy#whatcollect (last visited Nov. 10, 2018). Even a simple application such as the Dunkin Donuts "DDPerks" application collects a myriad of data on users including service use data, device connectivity data, location information, and more.
[31] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
[32] *Id.*
[33] *Id.* The same analysis may apply to other types of data presenting the same concerns, but now the bar will be lowered, as never before has the Court excepted such data from the third-party doctrine.

purview of the Fourth Amendment, I will caution against the expansion of its protections with no textual justification.

Accordingly, Part II will provide a history of the Fourth Amendment, and the pre-*Katz* property principles governing the determination of whether an activity constitutes a search. Part III will analyze *Katz* and its progeny and explore the outcomes of a privacy-based approach to the Fourth Amendment. Part IV will outline how a property-based approach has been applied in cases involving technological advancements post-*Katz*. Part V will discuss *Carpenter*, its holding, the rationale, and questions that will need to be answered in its wake. Part VI will argue for the abandonment of the *Katz* test when evaluating potential Fourth Amendment concerns with new technology. Part VII will introduce a potential property-oriented rationale for the holding in *Carpenter*, and the application of such a principle in future cases. Part VIII will argue for the role of the legislature in protecting the privacy of citizens in the absence of a clear Fourth Amendment proscription of a search and seizure.

II. Origins and Early Application of the Fourth Amendment

The Fourth Amendment was not a safeguard against theoretical abuse of government power, but a response to actual wrongdoing on the part of the British government. In *Brower v. County of Inyo*, the Supreme Court acknowledged that "writs of assistance [were] the principal grievance against which the Fourth Amendment was directed . . . ."[34]

These writs, which were a sub-species of general warrants, were instruments used in the American colonies to enable law enforcement to perform wide-ranging searches of "ships, warehouses, and homes, and all persons, papers, and effects contained therein . . . ."[35] Most often,

[34] 489 U.S. 593, 596 (1989).
[35] Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1244 (2016).

they were used to deter smuggling, the evasion of customs, and other trade and tax-related offenses.[36] Not only were these writs broad in terms of authority granted and items which could be searched, they also possessed an onerous temporal property. Once granted, these authorizations did not expire until the death of the sovereign under whose authority they were issued.[37] Thus, if a writ was issued against a citizen, the officers executing that writ would have carte blanche to search the subject's person, home, and place of business until the passing of the monarch.

The occasion of King George II's death and the impending expiration of writs of assistance issued during his reign provided the American colonists an opportunity to challenge the government's attempt to renew them.[38] In the ensuing action, "Paxton's Case", James Otis Jr. issued a forceful denunciation of the tyranny and excesses of general warrants and writs of assistance, asserting that their use would annihilate the freedom of "one's house."[39] Though Otis ultimately lost that case, the ensuing outrage proved an accelerant for the growing discontent with British rule, and John Adams, who was present at the proceedings, remarked that "[t]hen and there the child Independence was born."[40] Indeed, after the War of Independence, when the states were considering ratification of the proposed Constitution, some decried the document's silence as to general warrants, an omission they termed one of the "curses" of the new Constitution.[41]

The historical record certainly demonstrates colonial Americans' antipathy towards general warrants, but this was not unique to America, nor was the rationale an outgrowth of a distinctly American approach to law. The colonies were governed by English law, and the Americans inherited conceptions of freedom and rights from Great Britain. Even in "Paxton's Case" the

[36] *Id.* at 1242–49
[37] Tracy Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U.L. REV. 925, 946 (1997).
[38] Donohue, *supra* note 35, at 1248.
[39] Maclin, *supra* note 3737, at 946.
[40] Boyd v. United States, 116 U.S. 616, 625 (1886).
[41] Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 587 n.98 (1999).

colonials invoked "English liberties," and their case rested on the well-known maxim in English law that "a man's house is his castle."[42]

English common law did indeed provide rigid protection against invasion into a man's home. In fact, the seminal case on the topic, *Entick v. Carington*, was decided in 1765, and involved exactly the type of general warrant against which Otis argued in Paxton's Case.[43] *Entick* involved a general warrant issued for the search of libelous writings in the homes of individuals associated and allied with John Wilkes, a politician in England.[44] Though libel did not occur until publication, and the possession of libelous materials itself was not a crime, officers were directed to "make a diligent search" of Mr. Entick's home, and the homes of his confederates, to find these types of materials.[45]

Mr. Entick brought a trespass action against the officials who had searched his home and the Secretary of State that issued the warrants.[46] The court ruled in favor of the plaintiff, finding that the warrants in question were illegal, and thus, any search thereby authorized was a trespass.[47]

In *Entick*, the court rested its determination on the sanctity of an individual's property, and the strong protection afforded to such property by law against even government intrusion. "The great end for which men entered society was to secure their property," the court declared, adding that "every invasion of private property . . . is a trespass. No man can set his foot upon my ground without my license, but he is liable to an action, though the damage be nothing . . . [the] defendant is called to answer for bruising the grass and even treading on the soil."[48]

---

[42] Donohue, *supra* note 35, at 1251.
[43] 95 Eng. Rep. 807, 808 (C.P. 1765).
[44] *Id.* at 807–08.
[45] *Id.*
[46] *Id.*
[47] *Id.* at 818.
[48] Boyd v. United States, 116 U.S. 616, 627 (1886) (quoting *Entick*, 95 Eng. Rep. at 818).

Notably, however, in protecting the papers of the plaintiff, the court held that the "eye cannot by the laws of England be guilty of a trespass . . . ."[49] Simply viewing an individual's papers did not itself require a warrant, however, this invasion of privacy would serve to aggravate a trespass and increase damages where the papers were obtained without a valid warrant authorized by a magistrate.[50]

So famous and studied was this case that in *Boyd* the Court noted that "every American statesmen, during our revolutionary and formative period . . . was undoubtedly familiar with [*Entick*]" and its propositions provided the explanation for what constituted a search and seizure under the Fourth Amendment.[51] Though *Entick* is an English case from 1765, it has been cited in multiple Supreme Court decisions regarding the protections of the Fourth Amendment.[52] As recently as 2012, the Court has reaffirmed that *Entick* remains "'the true and ultimate expression of constitutional law' with regard to search and seizure."[53]

Accordingly, early Fourth Amendment jurisprudence did not require a warrant for law enforcement to perform searches that would not otherwise constitute a trespass. Thus, for example, in *Olmstead v. United States*, warrantless wire-tapping was deemed constitutional because in tapping phone lines, the government did not physically intrude onto an individual's person, house, papers, or effects.[54] Though some of the phones on which the government had set up monitoring were within individual homes, the Court did not look to the privacy of the individuals under surveillance, because no trespass had occurred to facilitate it.[55]

---

[49] *Id*. at 627–28.
[50] *Id*. at 628.
[51] *Id.* at 626–27.
[52] *See*, *e.g.*, Florida v. Jardines, 569 U.S. 1, 7–8 (2013); United States v. Jones, 565 U.S. 400, 405 (2012); Kyllo v. United States, 533 U.S. 27, 32 (2001); United States v. U.S. D., 407 U.S. 297, 327; *Boyd*, 116 U.S. at 627.
[53] *Jones*, 565 U.S. at 405.
[54] Olmstead v. United States, 277 U.S. 438, 466 (1928).
[55] *Id*.

Justice Brandeis objected to this formalistic and text-based approach in his dissent.[56] The Constitution, he asserted, was designed to be applied flexibly to situations which the drafters could not have imagined.[57] He looked beyond the "mischief which gave [the Fourth Amendment] birth" to the principle underlying the amendment's proscriptions.[58] In his view, the Fourth Amendment protected individuals from "all invasions on the part of the Government . . . of the sanctities of a man's home, and the privacies of life."[59]

Though Brandeis was a dissenter in *Olmstead*, his privacy-centered approach ultimately won vindication almost forty year later when the Supreme Court decided *Katz*.[60]

III. *Katz* and the Reasonable Expectation of Privacy

"We conclude that the underpinnings of *Olmstead* . . . have been so eroded . . . that the 'trespass' doctrine there enunciated can no longer be regarded as controlling."[61] With these words, the Supreme Court in *Katz* untethered the definition of a "search" from the text of the Fourth Amendment, and replaced the formalism that had hitherto characterized their approach with a new, privacy-centered test.[62]

The issue in that case was whether law enforcement's use of a listening device in a telephone booth for the purpose of eavesdropping on Mr. Katz violated his Fourth Amendment rights.[63] The government was attempting to find evidence that he was violating federal law by transmitting wagering information across state lines through the use of a telephone.[64] Though the government

[56] *Id.* at 472–74 (Brandeis, J., dissenting).
[57] *Id.*
[58] *Id.*
[59] *Id.* at 474.
[60] 389 U.S. 347, 353 (1967)
[61] *Id.*
[62] Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 247–50 (1993) (examining the *Katz* shift from the traditional property-based principles through the lens of pragmatism).
[63] *Katz*, 389 U.S. at 348.
[64] *Id.*

argued that a telephone booth was not a protected area, as set forth in the text of the Fourth Amendment, the Court declined to base its decision on the merits of that particular argument.[65] Instead, the Court focused on Mr. Katz's expectation of privacy, declaring that the "Fourth Amendment protects people, not places."[66] In overruling *Olmstead* and the trespass requirement, the Court lambasted the formalism of the prior approach, and held that Fourth Amendment protection "cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[67]

Justice Harlan's concurrence best articulates the "reasonable expectation of privacy" test, which replaced the trespass requirement as the judicial inquiry to determine if a search had occurred.[68] Under this new rule, a warrant would be required for investigative activities that violate an individual's reasonable expectation of privacy.[69] This determination hinges on two enquiries: (1) whether a person has shown an actual expectation of privacy in their activity and (2) whether society would recognize that expectation as reasonable.[70]

A. The Subjective Expectation of Privacy

In order to demonstrate a subjective expectation of privacy a person must have an intent to keep something private.[71] In some cases, the Court has identified specific behavior of an individual directed towards maintaining privacy. For example, though the majority opinion in *Katz* did not

[65] *Id*. at 351 (stating that the question of whether the phone booth is a constitutionally protected area is "misleading" and "deflects attention from the [real] problem presented in [the] case.").
[66] *Id.*
[67] *Id.* at 353.
[68] Cloud, *supra* note 62, at 249 (stating that the formula used in the opinion is an "amorphous standard" and was therefore replaced with the test used in Justice Harlan's concurrence).
[69] *Id*.
[70] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
[71] Smith v. Maryland, 442 U.S. 735, 740 (1979) (quoting *Katz*, 389 U.S. at 351).

address this prong, Justice Harlan identifies Mr. Katz's payment of a toll to use the phone, and his having closed the door behind him as manifestations of his intent to preserve his privacy.[72]

Often however, this intent must be inferred from the circumstances. When a person does something in plain view, he cannot claim an intent to keep private what anyone could easily observe.[73] A warrant is not required to monitor a car on the highway, for example, and the Court has held that when travelling in public roads the car and its contents are "in plain view" and thus, the operator has not shown an intent to preserve privacy.[74]

Revealing information to another undermines a subjective expectation of privacy, even when the audience to which the revelation is made is limited, and even where the information disclosed is confidential.[75] According to the Court, when a person knows or should know what he conveys to a third party will be somehow used by that party, he has no subjective intent to maintain the privacy of that information.[76] Thus, when a person dials a phone number, he cannot expect the number they dialed to be private, as that data point is used by the phone service providers to route the call, and for other business purposes.[77]

Additionally, though the Court acknowledges that subjective expectations of privacy are difficult to ascertain, historical determinations of what constituted a search and seizure when the Fourth Amendment was adopted should inform the analysis.[78] Therefore, for example, even when an individual does not specifically manifest an expectation of privacy, the very fact of being in

[72] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
[73] United States v. Knotts, 460 U.S. 276, 281–82 (1983).
[74] *Id*. at 285.
[75] United States v. Miller, 425 U.S. 435, 443 (1976) (holding that Mr. Miller did not have a reasonable expectation of privacy in bank records, despite the fact that he thought these were private).
[76] *Smith*, 442 U.S. at 742 (discussing the fact that telephone companies use the information around what phone numbers a subscriber dials for business purposes, among which are billing. Subscribers know or should know that telephone companies have the ability to record this information partly because it is the basis on which they are billed).
[77] *Id*.
[78] Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

one's home merits a strong presumption that such an expectation applies, because the home has always been afforded strong protections.[79]

B. Whether Society Is Prepared to Accept an Expectation of Privacy as Reasonable.

The simple fact that a person desires to keep something private does not, by itself, impose a warrant requirement upon law enforcement before a search may be conducted; that expectation must be one that society is prepared to recognize as reasonable.[80] The Court in *Katz* illustrated this by distinguishing the aspects of Mr. Katz's conduct that merited Fourth Amendment protection, and which did not.[81] In response to the government's contention that Katz was in plain view, and thus was not eligible for protection, the Court stated that phone booths are not meant to shield their occupants from view (notwithstanding the fact that the Man of Steel often resorted to such a booth to protect his identity while changing clothes).[82] They are, however, designed to maintain the privacy of the user's conversation.[83] Thus, applying Justice Harlan's reasoning, society is prepared to accept as reasonable a phone booth user's expectation of privacy. Insofar as reasonability is dependent on the views of society, this prong of the test is necessarily a normative determination.[84] Conceivably, then, as cultural mores and feelings on the topic change, so too do the boundaries of what would be protected.

Katz's departure from the trespass requirement may seem, at first glance, to expand privacy rights. In reality, however, courts have historically applied a conservative approach in its application, and have not, for the most part, wielded *Katz* to craft broader privacy protections.[85]

---

[79] Kyllo v. United States, 533 U.S. 27, 34 (2001).
[80] California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (holding that, despite clear intent on the part of Mr. Ciraolo to shield his home from view, society is "not prepared to honor" such an expectation as against aerial surveillance).
[81] Katz v. United States, 389 U.S. 347, 352 (1967).
[82] *Id.*
[83] *Id*.
[84] *See* Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 657 (2013).
[85] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809–11 (2004).

Generally, the Supreme Court has declined to find that society is prepared to recognize a privacy expectation as reasonable where an individual has taken the risk of exposing information either to a limited audience or the public at large.[86]

Thus, for example, in *California v. Ciraolo* the Court held that aerial surveillance does not run afoul of societal expectations of privacy.[87] It does not matter that an individual is in a remote location, or even on their own property or within the "curtilage" of their own home.[88] They have assumed the risk of exposing their location, and whatever outdoor activities they are doing; consequently, observing those activities is not a search.[89] Privacy rights, then, may just as easily be contracted under *Katz* as expanded, depending on the given court's view of society's expectations.

This holding on aerial surveillance also highlights another chink in *Katz*'s privacy-protecting armor. Namely that, when applying a *Katz* analysis of the reasonable expectation of privacy, the Court has repeatedly ruled that individuals are not necessarily shielded from increased surveillance capabilities available to today's law enforcement.[90] Modern technology allows law enforcement capabilities that are magnitudes greater than their colonial counterparts would have had. Nevertheless, increased efficiency in obtaining information and surveillance does not trigger Fourth Amendment protection.[91] While acknowledging that extended periods of surveillance may raise constitutional issues, the Court found no Fourth Amendment violation in a situation where police used a beeper to track a vehicle's movements.[92] That is not to suggest, however, that all

[86] Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002).
[87] 476 U.S. 207, 213–14 (1986).
[88] *Id.*
[89] *Id.*
[90] United States v. Knotts, 460 U.S. 276, 284 (1983).
[91] *Id.*
[92] *Id.* (stating that 24-hour surveillance drag-net style law enforcement practices may necessitate the application of different constitutional principles).

forms of surveillance may be employed without the necessity of first obtaining a warrant. The demarcation between permissible and constitutionally problematic monitoring hinges on the type of information the surveillance reveals.[93] If the information obtained through surveillance "could not otherwise have been procured without physical 'intrusion into the constitutionally protected area'" the Fourth Amendment requires a warrant.[94]

The third-party doctrine is another way in which society's determination of reasonableness abridges rather than enhances privacy. This doctrine states that, absent legislation to the contrary, "when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information . . . to law enforcement . . . ."[95] The rule first arose in the context of physical documents used in financial transactions.[96] In *United States v. Miller*, the Court ruled that a subpoena was sufficient authorization for obtaining bank records, regardless of Mr. Miller's expectation that his correspondence with his bank should remain private.[97] The holding of *Smith v. Maryland* extended this reasoning to a more technologically advanced fact-set, holding that the doctrine applied to the phone numbers a person dials.[98] An individual, by necessity, shares a phone number with a cellular provider when making a call, and that information is used to route the call to the correct party.[99] That information, being shared, loses Fourth Amendment protections. Notably, however, the contents of the call itself, the conversation, may not be subpoenaed from a provider, because the call itself was not shared with them.[100] Because the majority of data generated by and about

[93] Kyllo v. United States, 533 U.S. 27, 34 (2001).
[94] *Id.*
[95] SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984).
[96] 425 U.S. 435, 443 (1976).
[97] *Id.*
[98] 442 U.S. 735, 742–44 (1979).
[99] *Id.* at 744.
[100] *Id.* at 741 (distinguishing the device from that in *Katz* on the basis of the fact that a pen register does not facilitate listening to or recording calls, and thus the outcome would not be the same as that in *Katz*).

individuals today is stored by a third party, and because that data is not even generated by the user and thus is not content, the third party doctrine places a vast swath of data outside Fourth Amendment protection.

In fact, the application of *Katz* has been so tepid, some have argued that outcomes of cases analyzed under the *Katz* framework has not been appreciably different than would have been so under the common law.[101] Professor Orin Kerr even goes so far as to describe *Katz* as a "more of a revolution on paper than in practice."[102] Indeed, he contends that the Court could have reached the same result in the case had it applied Fourth Amendment trespass doctrine, and that the Court's explicit repudiation of this approach was therefore unnecessary.[103] This argument relies on the fact that a phone booth could arguably be considered a "house" for purposes of a Fourth Amendment search determination, providing a tie-in to the literal text of the amendment.[104]

While the reasonable expectation test looks past the text of the Fourth Amendment to the underlying principles, not text, courts have generally applied it conservatively. Due to the high degree of subjectivity inherent in assessments of both individual expectations of privacy and society's tolerance for those expectations, judges have broad discretion when defining these in the context of Fourth Amendment search determinations. Generally, even when an individual may harbor expansive expectations of privacy, the protections for this privacy are reined in by the second prong of the test.[105] Despite the concern expressed by Justice White in his dissent from the

[101] Kerr, *supra* note 85, at 824 (stating that the "Fourth Amendment today remains surprisingly similar to the Fourth Amendment before *Katz*").
[102] *Id.*
[103] *Id.* at 822 (postulating that the outcome of *Katz* was "correctly decided from the standpoint of [a] loose property-based approach").
[104] *Id.* at 809–11. *See infra* text accompanying note 134.
[105] There are several doctrines which limit Fourth Amendment protections, even where an individual desires to keep something private. Under the third-party doctrine, a person's communications with another are not protected by the Fourth Amendment, regardless of his intent. *See supra* text accompanying note 95. The private search doctrine disregards individual expectations of privacy where another party has already invaded that privacy. *See supra* note 25; *see generally* United States v. Jacobsen, 466 U.S. 109 (1984). Additionally, the open fields doctrine provides that

Katz decision, its application has not produced a radical departure from the text of the Fourth Amendment.[106]

IV. Trespass and Technological Advancement

Trespass theory, though wounded in *Katz*, did not die. Despite suffering a major setback with *Olmstead*'s reversal, some aspects survived, and some were folded into the reasonable expectation of privacy test. While *Katz* overturned *Olmstead*, holding that a trespass is not a prerequisite to a Fourth Amendment search, a physical trespass on a constitutionally protected area remains a search requiring a warrant.[107] The reasonable expectation of privacy test then did not replace trespass theory, but merely supplemented it. Therefore, where a trespass does occur on property enumerated in the text of the Fourth Amendment, the Court need not reach the question of whether there is a reasonable expectation of privacy and can instead proceed directly with common law trespass doctrine.[108]

Accordingly, there is a line of cases in which the occurrence of a Fourth Amendment search or seizure turns on the trespass doctrine without the need to resort to the *Katz* reasonableness enquiry. Significantly, the Court has declined to abridge property rights, specifically in the home when the *Katz* test might justify greater intrusion on the part of the government.[109] If an action

"an individual may not legitimately demand privacy for activities conducted out of doors in fields, except in the area immediately surrounding the home." Oliver v. United States, 466 U.S. 170, 178 (1984) (finding that there is no reasonable expectation of privacy in activities performed outside, even where the subject of surveillance has clearly expressed a intent to keep these activities private through the posting of "no trespass" signs).

[106] Katz v. United States, 389 U.S. 347, 373 (1967) (White, J., dissenting).

[107] United States v. Jones, 565 U.S. 400, 405 (2012).

[108] *Id.*

[109] Kyllo v. United States, 533 U.S. 27, 37–38 (2001) (reiterating the high degree of protection afforded the home, and that even the slightest details revealed about a home are intimate simply because they relate to it).

would have been an unreasonable search or seizure under the old trespass doctrine, it would still require a warrant; *Katz,* then, supplements trespass doctrine rather than supplanting it entirely.[110]

In *United States v. Knotts*, the Court ruled that a beeper in a barrel which transmitted a defendant's location to government authorities did not violate the Fourth Amendment.[111] While this case ultimately turned on a *Katz* expectation of privacy analysis, the Court notes that the defendant did not challenge the warrantless installation of the tracking device within the barrel that defendant bought, then transported to his cabin.[112] The defendant did not challenge on the basis of trespass on his car, due to the fact that he had placed the barrel within his car.[113] This distinction became relevant in *United States v. Jones*, which did, in fact, turn on the occurrence of a trespass on the car.[114]

In *Jones*, officers attached a tracking device to the undercarriage of the defendant's car.[115] The court held that a car constitutes an "effect" for Fourth Amendment purposes, and so, physically installing a tracking device thereon is a search.[116] The Court stated in simple terms that the "[g]overnment physically occupied private property for the purpose of obtaining information."[117] Because this trespass would have been considered a search at the time of the Fourth Amendment's adoption, it was considered a search, and there was no need to weigh the privacy considerations implicated.[118]

---

[110] Carroll v. United States, 267 U.S. 132, 149 (1925) ("The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens.").
[111] United States v. Knotts, 460 U.S. 276, 285 (1983).
[112] *Id.* at 280.
[113] *Id.* at 286 (Brennan, J., concurring).
[114] 565 U.S. 400, 404–13 (2012).
[115] *Id.* at 403.
[116] *Id.* at 404.
[117] *Id.*
[118] *Id.*

As technology has advanced, the Court has continued to protect the guarantee of privacy within one's house, which remains the "prototypical . . . area of protected privacy."[119] New innovations enable sophisticated surveillance without the need for a physical trespass, and it is possible that these developments could condition society to accept a reduction in privacy expectations in response to these capabilities.[120] When faced with this challenge, the court looks to the degree of privacy guaranteed at the time of the Fourth Amendment's adoption.[121] Put simply, if technology enables the acquisition of information that would not otherwise have been obtainable without a physical trespass on a constitutionally protected space, it is a search, and its use requires a warrant.[122]

Even under the subjective test of *Katz*, the Court remains zealously protective of the home. Before *Katz*, the mere act of cracking a door open and peeking inside was considered a search and invading a structure by so much as a portion of an inch was a trespass and required a warrant.[123]

As previously stated, the mere existence of a tracking device on a vehicle does not constitute a search if law enforcement did not physically place the instrument on the vehicle.[124] But, where such a device transmits information from within or at a defendant's "house," Fourth Amendment protections are activated.[125] It is true that any insights from a GPS transmitter on a car would be evident to police who physically monitored the car: an officer could certainly follow the car until

[119] Kyllo v. United States, 533 U.S. 27, 34 (2001).
[120] *See, e.g.*, *id.* at 37–38 (holding that thermal scanning, allowing police officers to view heat patterns emitted from the home is a search); *See also* California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (holding that there is no expectation of privacy against aerial surveillance because anyone may now fly over one's house).
[121] *Kyllo*, 533 U.S. at 34–35.
[122] *Id.*
[123] Silverman v. United States, 365 U.S. 505, 512 (1961).
[124] *See* United States v. Knotts, 460 U.S. 276, 284 (1983) (tracking device within a barrel loaded into a vehicle did not constitute a search); *see also* United States v. Jones, 565 U.S. 400, 403 (2012) (physical placement of a tracking device on a vehicle constituted a search because a trespass had occurred).
[125] *Knotts*, 460 U.S. at 284–85 (discussing the fact that no beeper information had been transmitted or relied upon from within the home in dismissing the claim of privacy invasion on that basis).

it parked at a house and wait until the car left again to continue pursuit.[126] Thus, it is not necessarily the nature of the information, but the mere fact that the information was collected within a constitutionally protected space that impedes its use.

While, in *Knotts*, the Court found that no search occurred where a tracking device was within a vehicle which was parked near, but not inside a home, they did provide some insight into what might constitute relevant factors in reaching a different result.[127] Specifically, the Court noted that future cases may raise issues of otherwise lawful surveillance techniques becoming unlawful when used to track individuals moving between private and public spheres.[128] Such monitoring may "push fortuitously and unreasonably into the private sphere protected by the Fourth Amendment."[129] But, the Court determined that as the barrel containing the beeper remained outside the house, nothing was revealed that would not have been visible to the naked eye should the police have relied on manual surveillance.[130]

An individual's residence is certainly afforded strong protections against government intrusion; however, it is important to note that the "house" referenced in the Fourth Amendment is not limited in its interpretation *solely* to a person's primary residence.[131] Central to the enquiry of whether a space is deemed a "house"—or, in today's legal parlance, whether an individual has the same reasonable expectation of privacy as he would in his home—is whether an individual possesses the right to exclude others from the space.[132] Renters, hotel room occupants, and even

[126] *See* Hester v. United States, 265 U.S. 57, 59 (1924) (holding that no search had occurred when officers observed illegal activity on private property because "the special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers, and effects,' is not extended to the open fields."). This doctrine was applied in *Knotts* where the Court held that the respondent did not have an expectation of privacy by simply arriving on his premises for actions which were visible to officers. *Knotts*, 460 U.S. at 282.
[127] *Knotts*, 460 U.S. at 284–85.
[128] *Id.*
[129] *Id.*
[130] *Id.* at 285.
[131] Kerr, *supra* note 85, at 809–11 (2004).
[132] *Id.*

guests where there is evidence their host devolved on them the right to exclude other from the space, would then qualify for Fourth Amendment protections in the respective spaces they occupy, albeit temporarily.[133] Professor Kerr even goes so far in his article as to suggest that by paying the toll in the phone booth and shutting the door, Mr. Katz thereby transformed it into a "house" for Fourth Amendment purposes, and this could provide a manner to reconcile the holding in *Katz* with the text of the Fourth Amendment.[134] This larger point may prove useful in rationalizing the Court's evident discomfort with long periods of retroactive surveillance, as such surveillance necessarily includes a "house" or multiple "houses" within its sweep.

Technology may not constitutionally allow invasion of a home's privacy which would otherwise require physical intrusion, but the mere fact that an activity was performed from within a house does not thereby provide absolute Fourth Amendment protections against warrantless surveillance.[135] Thus, in *Smith*, the defendant could not assert Fourth Amendment protection over the government's acquisition of pen register information, even though he physically dialed the phone numbers from within his house.[136] Phone conversations certainly were not possible at the time of the Fourth Amendment's adoption. To achieve such a communication, an individual would at least be compelled to open his window and conduct a conversation with a party outside his home. This conversation obviously would not be private, and one who observed such a conversation could not be said to have conducted a search.[137]

---

[133] *Id.*
[134] *Id.* at 822.
[135] *See, e.g.*, California v. Cirialo, 476 U.S. 207, 213 (1986) (stating that, even for constitutionally protected areas, there is no search where a police officer "observ[es] from a public vantage point where he has a right to be, and which renders the activities clearly visible[]"); *see also* Florida v. Riley, 488 U.S. 445, 449–51 (1989) (holding that there is no search where an officer is able with the naked eye to view activity within an edifice, even where that edifice is in the curtilage of a house).
[136] Smith v. Maryland, 442 U.S. 735, 742–44 (1979).
[137] *Cf.* United States v. Knotts, 460 U.S. 276, 284–85 (1983) (beeper did not reveal anything about the defendant's home that was not visible to the naked eye, and thus, did not violate the privacy of the home. This logic would apply to sounds from within the home as well).

The Fourth Amendment includes the house within its list of constitutionally protected areas.[138] In spite of *Katz*'s proclamation that this amendment protects "people not places," the home remains a constitutionally protected place, and government trespass thereon, by itself, is a violation of Fourth Amendment protections. This trespass need not be physical; modes of surveillance may be deemed a search if they achieve an affect that would have required a trespass had it been attempted without the enabling technology.[139] Finally, this protection is not immune from the caveat of the third-party doctrine: the government may, without a warrant, obtain information from a third party, regardless of whether that data originated from within the monitored individual's home.[140]

V. The *Carpenter* Decision

Carpenter provided an opportunity to consider the "dragnet-type law enforcement practices" and "twenty-four hour surveillance of . . . citizen[s]" to which the Court in *Knotts* acknowledged "different constitutional principles may be applicable."[141] Where *Knotts* involved a beeper, allowing law enforcement to track location, *Carpenter* deals with the subpoena of a form of historical location information, cell-site location information ("CSLI").[142] CSLI is a collection of timestamped records collected by cell service providers when a phone connects to a cell site, which in effect reveals the location of the cell phone at the time.[143] This information is used by cell phone companies for multiple business purposes, including determination of fee structures (for example when a user is "roaming") but also to drive business decisions around where to increase

[138] U.S. CONST. amend. IV. (providing in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" is protected through the warrant requirement).
[139] Kyllo v. United States, 533 U.S. 27, 34 (2001).
[140] *Smith*, 442 U.S. at 742–44.
[141] *Knotts*, 460 U.S. at 283–84.
[142] Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).
[143] Kyle Malone, *The Fourth Amendment and the Stored Communications Act: Why the Warrantless Gathering of Historical Cell Site Location Information Poses No Threat to Privacy*, 39 PEPP. L. REV. 701, 708 (2012).

coverage.[144] Because phones are constantly communicating with the network, whether the user is actively performing an action or not, and because in many areas, the towers gathering this information are closer and closer together, this information provides increasingly granular and accurate information about a cell phone user's movement that sometimes proves useful to law enforcement in investigations.[145]

The specific evidence at issue in *Carpenter* was 127 days' worth of CSLI data, composed of 12,898 discrete location records.[146] The Court declined to extend the third-party doctrine to this evidence, finding that a search had occurred.[147] In reaching this conclusion, it cited the accuracy, encyclopedic nature, and effortless collection of this type of data, and held that it is reasonable for an individual to expect privacy in his physical movements from records so collected.[148] Notably, however, this is not a categorical proscription on the use of CSLI. The Court stated explicitly that the decision is not binding for factual circumstances not before the Court.[149] In spite of the focus on the type of data at issue, CSLI, the Court explicitly excepted "real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval)" from the holding.[150] Importantly, this case does not hold that people may have a reasonable expectation of privacy in their location or their movements, but in the "whole of their physical movements."[151] The difference between the two is one of degree, and nothing in the

[144] *Carpenter*, 138 S. Ct. at 2212.
[145] Malone, *supra* note 143, at 708–09 (stating that a phone transmits CSLI approximately once every seven seconds, and that CSLI may be able to determine a phone's location to within 200 feet).
[146] *Carpenter*, 138 S. Ct. at 2212.
[147] *Id.* at 2217.
[148] *Id.* at 2216.
[149] *Id.* at 2220.
[150] *Id*.
[151] *Id*. at 2217.

opinion suggests that the Court now takes an unfavorable view towards location monitoring for shorter temporal periods.[152]

The departure from the third-party doctrine prompts two important inquiries: (1) why the doctrine does not apply to acquisition of long periods of CSLI information from a third-party provider and (2) what questions this raises for future cases involving similar types of records.

A. Why the Third-Party Doctrine Did Not Apply in *Carpenter*

There are two principle reasons the Court cites in support of its decision to distinguish CSLI from other data types previously considered, and hence, not to apply the third-party doctrine in *Carpenter*. First, because CSLI differs from the surveillance methods and data in prior cases as it constitutes a far more exhaustive record of a person's life, potentially exposing a wide panoply of otherwise private information.[153] Second, because CSLI—collected by "dint of operation" of the phone—is not affirmatively "shared" with the third-party, and therefore, individuals do not lose their expectation of privacy in this information.[154]

i. Difference Between CSLI and Traditional Records Subject to the Third-Party Doctrine

There are many ways in which the evidence at issue in *Carpenter* was broad and revealing. In a previous case, the Court, in dicta, stated that long-term surveillance may present different Fourth Amendment questions than 24-hour monitoring, or tracking a vehicle for discrete trips.[155] Here, the police obtained 127 days of location information, revealing all the movements of the target in such detail that would not have been practical, and perhaps not even possible by physical following at the time the Fourth Amendment was written.[156]

[152] *Carpenter*, 138 S. Ct. at 2220.
[153] *Id*. at 2217.
[154] *Id*. at 2220.
[155] United States v. Knotts, 460 U.S. 276, 284 (1983).
[156] *Carpenter*, 138 S. Ct. at 2217–19.

The sheer volume of records proves even more troubling because it allows a state actor to meticulously catalogue an individuals' life, and derive insights into their behavior.[157] Data of the type to which the third-party doctrine traditionally applied was relatively discrete.[158] From bank records, police could, perhaps, deduce spending habits or glean other financial records; similarly, phone call records reveal details about discrete calls.[159] Location information, however, when aggregated over a long period of time, reveals much more than simply where the person was, it can divulge, among other things, a person's "familial, political, professional, religious, and sexual associations."[160] As cellular providers increase their coverage and add cell towers, this information becomes even more precise and the location may be ascertained to a more granular unit of measurement.[161]

Perhaps as troubling is the fact that the information about any given suspect's location is already assembled and requires practically no effort from law enforcement to acquire. Previously, determining an individual's whereabouts at a given point in the past would have required finding a witness or some discrete evidence placing the suspect at a given time at a given place. No single

---

[157] *See* Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 561 (2017) ("Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble."). The aggregation of location information may also be overlaid with other data sets to produce even more insights. *See generally* Yan Huang et al., *Mining Co-Location Patterns with Rare Events from Spatial Data Sets*, 10 GEOINFORMATICA 239 (2006).

[158] *See, e.g.*, United States v. Miller, 425 U.S. 435, 442 (1976) (dealing with microfilm copies of checks and deposit slips); *see also* United States v. White, 401 U.S. 745, 751 (1971) (holding that conversations with an individual could be recorded and conveyed to police with no warrant required); Smith v. Maryland, 442 U.S. 735, 742–44 (1979) (upholding the use of a pen register, which simply recorded a list of the phone numbers an individual dialed).

[159] Prior cases dealt with limited data sets about specific activities. *See supra* note 159. Modern data mining, data analytics, and artificial intelligence capabilities, however, require massive data sets in order to derive insights. *See, e.g.*, Nick Ismail, *The success of Artificial Intelligence Depends on Data*, INFORMATION AGE (Apr. 23, 2018) https://www.information-age.com/success-artificial-intelligence-data-123471607/ (stating that "AI works best when large amounts of rich, big data are available").

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

[161] *See* David Oscar Markus & Nathan Freed Wessler, *That '70s Show: Why the 11th Circuit was Wrong to Rely on Cases from the 1970s to Decide a Cell-Phone Tracking Case*, 70 U. MIAMI L. REV. 1179, 1183–84 (2016).

witness could testify to everywhere an individual had ever been.[162] Thus, while at any given time, a person may be conveying his location to "anyone who wanted to look," the same cannot be said of *all* his movements, taken together.

The outstanding question, then, is how much information is too much? At what point, or for what interval of time are constitutional protections trigged? Though *Carpenter* is limited to CSLI, the answer to that question would apply in any context involving the tracking of a person's location, including, as the Court acknowledged, the use of beepers and GPS trackers on vehicles.[163]

ii. Absence of Voluntary Exposure of Information Shared

One justification for the third-party doctrine is that a person assumes a risk, in revealing information to another, that the other will reveal it to a state actor.[164] Part of the reason the Court in *Carpenter* declined to apply the third-party doctrine to the data at issue was due to the involuntary nature of the conveyance.[165] The indispensable nature of the phone and the method in which the phone transmits CSLI are the factors that led the Court to this outcome.[166]

Ninety-five percent of adults in America own a cell phone, and seventy-five percent own a "smart phone."[167] The cell phone is ubiquitous, not only in terms of ownership, but also of location relative to its owner. Increasingly, these devices accompany the user everywhere they go, so much so that the Court characterizes it as "almost a 'feature of human anatomy . . . .'"[168]

---

[162] *Carpenter*, 138 S. Ct. at 2219 (observing that "Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible.").
[163] *Id*. at 2215. This assertion is made on the basis of the fact that the Court cites to the dicta in *Knotts* and concurring opinions in *Jones* to establish that continual surveillance would present a unique constitutional question, distinct from the constitutionality of the type of data in use. *Id*.
[164] *See* United States v. Miller, 425 U.S. 435, 443 (1976) (denying Fourth Amendment protection to records on the grounds that an individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government").
[165] *Carpenter*, 138 S. Ct. at 2218.
[166] *Id.* at 2210.
[167] *Mobile Fact Sheet*, PEW RESEARCH CENTER (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/.
[168] *Carpenter*, 138 S. Ct. at 2218.

Additionally, as the phone is carried everywhere, it is transmitting CSLI information on a regular basis, whether in use or not.[169] If it is both turned on and connected to the network, this information continues to flow to the wireless provider.[170] This is not a feature that the user may enable, opt out of, or even see; it is collected for the wireless provider's use by dint of the phone's operation.[171]

There are, however, methods by which a phone's owner may avoid such continual monitoring, should he so desire. He could turn off his phone, he could disconnect it from the network, or he could always decline to possess it on his person, at least for the period he does not want to be tracked. Though the Court acknowledges these possibilities, it finds the compulsive use of cell phones in today's modern world renders the act of always carrying a connected and powered-on phone involuntary.[172]

B. Issues Likely to Arise from *Carpenter*

The *Carpenter* decision has impacts beyond the explicit limits to the third-party doctrine as well. In limiting the third-party doctrine as it does in *Carpenter*, the Court creates a Fourth Amendment right of an individual in the business records of another.[173] Though an individual may have no knowledge of their CSLI being generated, and no involvement in creating the records, they nevertheless have a right to assert warrant protection for those records by virtue of the fact that they are "about" them.[174]

[169] Malone, *supra* note 14343, at 708.
[170] *Carpenter*, 138 S. Ct. at 2220.
[171] *Id.*
[172] *Id.*
[173] CSLI is generated without the input of the user and is only ever recorded by a third party. *Id.*
[174] *Id.*

Additionally, though the Court recognizes the unique nature of location data in protecting the privacies of life,[175] this decision creates much uncertainty about the Fourth Amendment protections of other data generated through IOT and smart devices, for example, which reveal certain insights about users through the dint of their operation. Now that the Court has found a category of data to which the third-party doctrine does not apply, lower courts will be challenged to classify the numerous other species of data generated by devices on a constant basis.[176] Whereas the third-party doctrine provided a relatively simple answer to the *Katz* enquiry for data, this decision opens the door for challenges to the warrantless acquisition of numerous other forms of digital information.

Though the surveillance in *Carpenter* was not performed by law enforcement, but by a private actor, the Court nevertheless treated the acquisition of this data as a search, as if the police had conducted the surveillance themselves.[177] This distinguishes this case from many of the prior Fourth Amendment cases addressing surveillance, and raises questions around when private actions can be attributable to the government in a way that requires a warrant. For example, hitherto, under the private search doctrine, law enforcement need not obtain a warrant for searches conducted on items which a third-party has already searched, whether that party was entitled to perform the search or not.[178] This doctrine currently facilitates the cooperation of private companies with government agencies in finding and identifying users of child pornography for the

[175] *Carpenter*, 138 S. Ct. at 2217.
[176] *See, e.g.*, Supplemental Brief of Appellant-Petitioner at 20, Holyoak v. Gaos, 2018 U.S. S. Ct. Briefs LEXIS 4654 (2018) (in which the petitioner argues that the reasoning of *Carpenter* should be extended to protect Google search terms).
[177] *Id.* at 2218 (noting that when the government acquires CSLI on an individual, that individual "has effectively been tailed every moment of every day . . . and the police may . . . call upon the results of that surveillance without regard to the constraints of the Fourth Amendment.").
[178] United States v. Jacobsen, 466 U.S. 109 (1984).

purpose of combatting child abduction and exploitation.[179] Technology companies are able to compare the digital signature of files in user's accounts (a hash) to the signature for known child pornography media.[180] This scan is run on a continual basis, and when the company finds an image that matches the description, it alerts the government to the existence of the file, and the identity of the owner of said file.[181] Because the company has already abridged the user's privacy by identifying the file, the government is not required to obtain a warrant to verify the contents of the file.[182] In effect, the scanning required to identify these files constitutes twenty-four hour surveillance. For all intents and purposes, the government is facilitating the invasion of privacy by a private party not bound by Fourth Amendment search requirements and is able to create a loop-hole by which it can constantly surveil the defendant's files for contraband. Given that the Supreme Court found a subpoena of information maintained and exploited by a third-party problematic in *Carpenter*, this may initiate the partial undermining of the private search doctrine as well.[183] Can a company voluntarily surrender to the government non-content data on its users which would otherwise require the state to obtain a warrant?

VI. The Shortcomings of *Katz* in the Context of Technological Advances

The third-party doctrine has held at bay many issues arising from the application of *Katz* to new technological paradigms. But, in carving out an exception, *Carpenter* generates uncertainty

[179] United States v. Stevenson, 3:12-cr-00005, 2012 U.S. Dist. LEXIS 194725 (2012) (in this case, AOL reported child pornography images it detected to the National Center for Missing and Exploited Children, which then reported it to local law enforcement).
[180] *Id*.
[181] *Id*.
[182] *See, e.g.*, United States v. Reddick, 900 F.3d 636, 638–40 (5th Cir. 2018).
[183] Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018). If it is unconstitutional for the government to subpoena a third party for information that party has on an individual, it may be unconstitutional to have a system set up that amounts to continual government surveillance of emails or other online activities.

around application of the test to other novel surveillance questions and may thus inject more subjectivity in Fourth Amendment jurisprudence.

One problem in applying a test which relies on societal norms is that, by definition, there is no societal norms around the treatment of new technology. Society has not yet established norms and expectations around new technologies, and courts will thus be left to guess what society might be prepared to accept in such cases.[184] This essentially places judges in the role of policy-makers, and rather than determining what society's expectations are, they will be enabled and even expected to announce what society's expectations should be instead.[185] Indeed, there are few guidelines in determining what society is prepared to accept as reasonable. In *Ciraolo*, for example, the Court upheld aerial surveillance because, it reasoned that individuals have no expectation of privacy in what is visible to the naked eye, and further, are aware that aircraft are flying overhead.[186] Thus, the knowledge that information is visible to others, and the general knowledge that surveillance is occurring could conceivably create a cycle of diminishing privacy expectations. Already, society is aware of data breaches, hacks, corporate misuse and improper sharing of information, in addition to potentially improper government surveillance.[187] Because society has thus been conditioned to expect and grown accustomed to a reduced expectation of privacy, should this mean that the *Katz* test allows technology advancements to rob Americans of

[184] *See* Selbst, *supra* note 84, at 659 (observing that society's reasonable expectation of privacy is dependent on its knowledge about surveillace occurring); *see also* Levinson-Waldman, *supra* note 157, at 551–52; *see generally* Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173 (1979) (discussing the circularity of premising the reasonability of an individual's expectation of privacy on societal norms) [hereinafter Posner, *Uncertain Protection*].
[185] Kerr, *supra* note 85, at 808.
[186] California v. Ciraolo, 476 U.S. 207, 213–14 (1986).
[187] *See, e.g.*, Taylor Armerding, *The 17 Biggest Data Breaches of the 21st Century*, CSOONLINE (Jan. 26, 2018, 3:44 AM), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

privacy rights? In *Kyllo*, the Court acknowledges the possibility of such a cycle, and technology's erosion of privacy rights through the "reasonable expectation" prong of the *Katz* test.[188]

The *Katz* test's potential to create results that are "subjective and unreasonable"— which the Supreme Court acknowledges—might have been an acceptable trade-off if it achieved the goal of protecting the privacy that underlies the Fourth Amendment.[189] But it is not completely certain whether the *Katz* approach provides greater or lesser protection than the text of the Fourth Amendment itself, and the trespass approach. In the cases of aerial surveillance and the use of a pen register to capture phone numbers dialed from within a home, for example, application of the *Katz* test resulted in reduced privacy expectations, rather than more.[190] Further, the circularity of the reasonable expectation of privacy, and the potential subjectivity of its application have led to criticism that the doctrine is a "black hole" that "has never been able to do the work required of it."[191]

Additionally, *Katz*, though formulated to deal with advanced technological capabilities and the challenges associated therewith, presents a more fundamental challenge, that of reconciling it with the text of the Fourth Amendment. In his dissent from *Katz*, Justice White lamented the Court's attempt to "keep the Constitution up to date," warning that the "effort would make [the Supreme Court] a continuously functioning constitutional convention."[192] As noted earlier, though the language of the *Katz* test does not require a touchpoint to the text of the Fourth Amendment, courts have been conservative in their application, such that the use of the *Katz* test has not resulted in vastly different outcomes than would reliance on common law trespass doctrine. Given that

[188] Kyllo v. United States, 533 U.S. 27, 33 (2001).
[189] *Id.* (quoting Posner, *Uncertain Protection*, *supra* note 184, at 188).
[190] *Ciraolo*, 476 U.S. at 213–14 (allowing aerial surveillance of an individual's home); Smith v. Maryland, 442 U.S. 735, 742–44 (1979) (upholding the use of a pen register, despite the fact that the numbers dialed were dialed from within the home).
[191] Jeb Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 103 (2008).
[192] Katz v. United States, 389 U.S. 347, 373 (1967) (White, J., dissenting).

Carpenter has created a crack in the third-party doctrine, however, it is conceivable that courts could craft responses and tests for what constitute a search that would have no possible justification in the text or historical understanding of the Fourth Amendment.

VII. Reconciling *Carpenter* with the Text of the Fourth Amendment

Given the subjectivity of the *Katz* doctrine and the Court's own admission in *Kyllo* of its problematic application, courts should adopt an interpretation of the *Carpenter* decision that is grounded in the text of the Fourth Amendment and common law trespass doctrine, and which minimizes subjectivity when defining what constitutes a search in novel technological scenarios. In so doing, courts should recognize that, while the Fourth Amendment protects a degree of privacy, the framers could not possibly have conceived of today's technology. Thus, it is not a foregone conclusion that individuals have a reasonable Fourth Amendment expectation of privacy in their data. Rather than crafting new protections, and thus fulfilling Justice White's fear of the court devolving into a constitutional convention of its own, courts should refrain from making policy decisions where the Constitution is silent.

Accordingly, the Court should afford new protection only when a government action potentially violates the privacy or security of one's person, house, papers, or effects. When determining the contours of what qualifies for these designations, courts will be forced to grapple with tough questions, but this mitigates some of the concern of judicial abuse of power. In the context of the IOT, smart devices, and even computers generally, some records may be easily analogized to the physical items originally protected by the Fourth Amendment. For example, an individual's computer files could easily be related back to the "papers" mentioned in the Fourth

Amendment.[193] Indeed, the naming of files and folders in the computer context is an implicit acknowledgement that they are the functional equivalent of physical papers, and the Court already distinguishes between content and non-content data.[194] As to devices, however, it is more difficult to draw a neat analog to the founding days, or even trespass principles. Some have suggested the concept of categorizing smart devices as "effects," and protecting their associated data through a theory of "digital curtilage."[195] Debating the wisdom of a given classification is beyond the scope of this article, however, the very existence of a textual hook provides greater certainty and mitigates concerns of judicial activism. To disregard the enumeration of protected properties in the Fourth Amendment is to imply that they are gratuitous, and unnecessary to the Amendment. Courts may desire to protect the privacy that was perhaps the object of the Fourth Amendment, but they should avoid the temptation to disregard the letter of the law in their zeal to fulfill the spirit.

It is possible that such an approach, though it may change the outcome in certain cases, may not even diminish privacy protections. As previously noted, the current *Katz* test as applied is already a mixed-bag in terms of its effect on privacy rights. While acknowledging that there will be some normative violations of individual privacy that are beyond the scope of Fourth Amendment protection, as defined in the text of the amendment, the Court should provide strong and liberal protection where an analog can be shown to the items enumerated in the constitution.[196]

---

[193] *See generally* Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L., 112 (2011).
[194] Smith v. Maryland, 442 U.S. 735, 741–43 (1979) (distinguishing between the content of the call and the information about the call, e.g. the number that was dialed).
[195] Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 809 (2016).
[196] *See, e.g.*, *Katz*, 389 U.S. at 373 (White, J., dissenting) (opposing the majority's departure from the text of the Fourth Amendment, Justice White evinces a willingness to go "as far as a liberal construction of the language [of the Fourth Amendment] takes me" in protecting the privacy of individuals).

In the case of *Carpenter*, evaluating the ruling in light of the protections outlined in the text of the Fourth Amendment would provide clarity to some of the concerns raised by the ruling and eliminate others.

It is important to acknowledge that, when dealing with time-series data, as in *Carpenter*, law enforcement is actually performing surveillance, albeit retroactively.[197] The records the government may attempt to acquire from a company have already been collected by that company. But, for Fourth Amendment search purposes, this data should be treated as if the government had collected it, because acquiring examining these records is the functional equivalent to performing the surveillance in real-time.[198] The Court in *Carpenter* and in *Knotts* expressed reservations about the implications of twenty-four-hour surveillance, and, in the case of *Carpenter*, the use of data even when held by a third party.[199] While the reasoning in *Carpenter* was couched in the language of privacy, the truth is, allowing the government to benefit from a private entity's constant surveillance of an individual enables law enforcement to trespass in constitutionally protected areas with impunity. In *Kyllo*, the Court emphasized the need to "assure preservation of that degree of privacy that existed when the Fourth Amendment was adopted."[200] This concern resulted in a prohibition on the warrantless acquisition of information about a house that previously could not be obtained without physical intrusion.[201] By the same token, increased efficiency due to

[197] The Court in *Carpenter*, while not explicitly endorsing this proposition, analogized retroactive data collection to physical surveillance. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018). Further, it notes that society would not expect that police officers could or would physically perform the surveillance yielding the equivalent volume and type on information which historical CSLI provides. *Id.* at 2217–18.
[198] This is not to imply that an agency relationship exists, but merely a realization of the reality that when law enforcement obtains this information, it is as if they were performing the surveillance themselves.
[199] The fact that CSLI is held by a third party was ultimately irrelevant to the outcome of *Carpenter*, as the Court found that the nature and quantity of this data placed it beyond the scope of the third-party doctrine. *Carpenter*, 138 S. Ct. at 2216–17.
[200] Kyllo v. United States, 533 U.S. 27, 34 (2001).
[201] *Id.*

technology advances in the field of surveillance does not, in itself, pose a constitutional conundrum.[202] This is especially the case when law enforcement could have obtained the same information through constitutionally permissible means in the absence of the technology.[203] The common thread is that technology, while enhancing law enforcement capabilities, cannot provide access to what would have required a trespass. While there was no concept of the comprehensive historical time-series data in the founding era, utilizing this information is the functional equivalent of performing surveillance, and the limits that would apply to physical surveillance should apply equally in this context, irrespective of the involvement of a third party.

If information is not simply fair game because it is held by a third party, courts need not address whether an individual actively shared information or not. Indeed, it is difficult to determine whether an individual has shared something with a third-party, as demonstrated in *Carpenter*. The conclusion that location sharing is involuntary because avoiding it would require turning off the phone, disconnecting it from the network, or not carrying it constantly is troubling because it premises the outcome of the case on the implied lack of agency when it comes to phone discipline.[204] It is well-known that cell phones track a user's location. Therefore, by carrying a cell phone and not taking precautions against this tracking, individuals assume the risk of broadcasting their location. But, if the relevant enquiry is not solely whether the information about the user is shared with a third party, but instead, whether lawful police surveillance would have been able to achieve the same result, the problem of voluntary versus involuntary sharing drops out of the equation. There are too many devices, broadcasting too much information, for too many

[202] United States v. Knotts, 460 U.S. 276, 284 (1983).
[203] *Id.*
[204] When discussing the relationship between an individual and his phone, the *Carpenter* Court did not focus on the individual effort required to avoid such tracking, but simply noted the fact that people carry their phones "compulsively" such that the phone has almost become a "feature of human anatomy." *Carpenter*, 138 S. Ct. at 2218.

purposes, with too many metrics to make determinations for each whether active sharing has occurred.[205] Indeed, the way individuals interact with their technology is continuing to change at a rapid pace and creating a coherent rule regarding a user's expectation for each technology would be an exercise providing little clarity, and one that would likely be repeated frequently as new technologies emerge. Instead, the Court should distinguish between affirmative acts by the user, and autonomous recording by the device. Where an individual consciously shares something with a third party, less privacy should be afforded, consistent with *Miller*.[206] At the same time, where a device can be co-opted to perform surveillance retro-actively, the data associated with that device should be subject to the same limitations that would be applicable if the government were performing physical surveillance. This solution would both protect the privacy of the house against technological erosion of Fourth Amendment protections and provide greater clarity as to when the information could be used.

In *Carpenter* as in *Knotts*, the Court expresses discomfort regarding the possibility of 24-hour surveillance.[207] While holding that the facts in *Carpenter* required a warrant, however, the Court did not announce a rule that could be applied consistently.[208] Instead, the Court noted the sensitive information about the "privacies of life" location data would expose.[209] But, this concern is present whether surveillance occurs for one or 20 days, the difference is simply a matter of degree. *Knotts*,

[205] There are over seven billion IOT devices, and over seventeen billion devices connected to the internet as a whole, including smart phones, tablets, etc. Knud Lasse Lueth, *State of the IoT 2018: Number of IoT Devices now at 7B—Market Accelerating*, IOT ANALYTICS (Aug. 8, 2018), https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.
[206] United States v. Miller, 425 U.S. 435, 443 (1976) ("when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information . . . to law enforcement.").
[207] Carpenter v. United States, 138 S. Ct. 2206, 2216–17 (2018).
[208] "Our decision today is a narrow one. We do not express a view on matters not before us . . . or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information." *Id*. at 2220.
[209] *Id*. at 2217.

while not ruling directly on the topic, framed the problem as one of moving between public and private spheres, and thus while the method of surveillance may be warranted, the constitutionality may turn on the time and location during which surveillance is taking place.[210]

When requesting time-series data from a past time period one would necessarily be ignorant as to its contents until examining it. Thus, it is possible, for example, that for records requested in a given time period, the data would include information that is collected from within the surveilled party's home, giving rise to Fourth Amendment concerns.[211] This fact, however, should not preclude the gathering of any data whatsoever. Instead, *Carpenter* could be applied to preclude government from subpoenaing time-series records (location or otherwise) that would almost certainly contain information protected by the Fourth Amendment due to its likelihood to reveal something about the home. This would entail limiting subpoenaed documents to periods of time that are not certain to include time where the defendant would be at his house, for example. When requesting documents, the government would be limited to time ranges beneath twenty-four hours, as an individual is almost certain to be at his house at some point within that interval. Even if not at his own house, he would be somewhere that would still qualify as a "house" be it a hotel room a guest room in another's house, or another temporary residence.[212] This would not necessarily burden law enforcement unduly. In *Carpenter*, for example, the government was attempting to link Carpenter to known crimes.[213] Thus, in reality, there were certain time ranges in which the government was truly interested that would have provided the evidence of his proximity to the

[210] *Knotts*, 460 U.S. at 284.
[211] *Cf.* United States v. Jones, 565 U.S. 400, 403 (2012). The District Court ordered the suppression of any GPS data obtained while the vehicle was parked at the defendant's home. In so doing, the Court recognized the Fourth Amendment implications of multi-day monitoring, and the need to protect the privacy of the home.
[212] Kerr, *supra* note 85, at 819.
[213] Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018) (the police were investigating a series of robberies at nine different stores).

crimes.[214] Much of the information obtained by the government was gratuitous, and there was not necessarily a basis for suspecting the defendant of nefarious activity in that time.[215] A subpoena requesting the time ranges corresponding to the known crimes would have served the government's purpose, respected privacy rights, and would have been consistent with the holding in *Carpenter*.

Applying a likelihood of trespass approach to subpoenaed time-series data would not only limit the government from obtaining broad swathes of time, for which a small percentage is actually relevant to the crime under investigation, it would also provide further protection to individuals with respect to, for example, the time of day for which records could be requested. If there is no reason to believe an individual is out of his home at 1:00 am, then subpoenaing information for that time would amount to a trespass, as it is more likely than not that an individual would be home. The suspicion, however, that an individual committed nefarious acts at that time, supported by any evidence would reduce the likelihood that particular individual would have been in their home at that time, and would provide justification for the subpoena. This approach would provide clarity in the application of *Carpenter*, provide a textual basis for judicial holdings, and enhance Fourth Amendment protections for individuals while still affording law enforcement the ability to perform needed investigative work without the burden of obtaining a warrant.

VIII. Alternatives to New Judicial Standards

This Comment does not seek to take a position on the desirability or detriment of increased protections for privacy given the ever-changing technological landscape. What it does argue, however, is that threats to individual privacy and the need for protection does not justify the

[214] The police matched the CSLI to the locations and times of the robberies, which were already known. *Id*. at 2213.
[215] *Id.*

invocation of the Fourth Amendment in cases where doing so requires a departure from the text itself. Ultimately, even given the contention of some that the Constitution and its provisions were designed to have enough flexibility to handle novel situations, it must be admitted that the drafters of the Fourth Amendment could not possibly have imagined the challenges attendant to technology today.[216] Resorting to their underlying intentions, then, is a futile exercise because there are many scenarios faced today which bear no resemblance, and cannot be analogized to the specific problems the Founders sought to address with the Fourth Amendment.[217] That is not to say that all technology is beyond the scope of Fourth Amendment protection. But it does mean that we should acknowledge the possibility that there are some things that may not be rationalized to the text of the amendment, and threats to privacy notwithstanding, the Amendment should not be adjusted to cover such gaps.

One of the ironies of a judicial standard which requires a court to ascertain what society at large finds reasonable is that judges are uniquely ill-equipped to grapple with this question. The Supreme Court has even conceded to the criticism of *Katz*'s application as being "circular, and hence subjective and unpredictable."[218] In cases that involve items mentioned in the text of the Fourth Amendment, the application is straightforward: society presumptively accepts an expectation of privacy in those things to which the Constitution explicitly grants protection.[219] In

[216] *See, e.g.*, Katz v. United States, 389 U.S. 347, 373 (1967) (White, J., dissenting) ("Since I see no way in which the words of the Fourth Amendment can be [applied,] . . . that closes the matter for me. . . . I willingly go as far as a liberal construction of the language takes me, but I simply cannot in good conscience give a meaning to words which they have never before been thought to have and which they certainly do not have in common ordinary usage."). *But see* Olmstead v. United States, 277 U.S. 438, 472–74 (1928) (Brandeis, J., dissenting) (speaking of the application of constitutional provisions to new and unforeseen circumstances, Brandeis writes, "[t]he future is their care and provision for events of good and bad tendencies of which no prophecy can be made.").
[217] One such example is Google search terms. *See, e.g.*, *supra* note 176.
[218] Kyllo v. United States, 533 U.S. 27, 34 (2001).
[219] *See id.* (acknowledging the difficulties of determining what society deems reasonable, but that for a prototypical area of protection, such as the home, which has deep common law protections and has been heavily litigated, the answer is evident).

Carpenter, however, the Court looked to historic law enforcement capabilities and reasoned that, because surveillance yielding the type of information at issue would have been costly and practically impossible prior to the digital age, society recognizes an expectation of privacy against it as reasonable today.[220] It is true, however, that society's tolerance changes over time, and thus, it is unclear why the Court chose to reference pre-digital age society in that case to determine reasonableness. Because this is a subjective test, the sword cuts both ways. Indeed, were that logic applied to *Ciraolo*, the Court would perhaps have found the defendant's expectation of privacy against aerial surveillance reasonable. After all, before flight became common-place, this would not have been possible.[221] Though society's expectations may change, these decisions have precedential effect, and thus become evidence of what society would find reasonable.

As it happens, there is a mechanism through which society may express its views on what constitutes a reasonable expectation of privacy: the legislative process. Where the Constitution does not mandate a warrant, Congress and the states may nonetheless add however much protection they deem necessary to sufficiently protect the privacy of their respective citizens. In fact, there are many examples of Congress doing just that. The Health Insurance Portability and Accountability Act—while not going so far as to mandate a warrant when the government seek to obtain medical information from a provider—does require that provider to notify the patient before the records are disclosed, giving them the opportunity to object in court.[222] The Stored Communications Act provides several protections for data that is stored by a third party, even requiring law enforcement to obtain a warrant before it may request certain information.[223]

---

[220] *Carpenter*, 138 S. Ct. at 2217.
[221] California v. Ciraolo, 476 U.S. 207, 213–14 (1986).
[222] Natalie F. Weiss, *To Release or not to Release: An Analysis of the HIPAA Subpoena Exception*, 15 MICH. ST. J. MED. & LAW 253, 260–63 (2011) (citing 45 C.F.R. § 164.512(e)(1)(ii)(A) (2011); 45 C.F.R. § 164.512(e)(1)(iii) (2011)).
[223] 18 U.S.C. § 2703(a). *See* William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1208 (2010).

Even where the Court has not found a violation of the Fourth Amendment, Congress has, at times, stepped in to impose privacy requirements. In fact, the Right to Financial Privacy Act was passed in response to *Miller*, prohibiting the government conduct which the Court held not to be violative of the Fourth Amendment.[224] Similarly, 18 U.S.C. § 3121(a) now prohibits law enforcement from installing a pen register without a Court order, another activity which the Court found to be compatible with Fourth Amendment protections.[225]

These examples show that Congress is both willing and able to act in order to protect privacy, and that it is not necessary for the Supreme Court to go beyond the text of the Fourth Amendment to achieve the same result. Indeed, Congress is better suited to handle such questions as it is more representative than the courts, and is vested with considerable fact-finding capabilities, allowing it to better tailor solutions.[226] When the Court acts to expand the Fourth Amendment, it short circuits the process, robbing society of the benefit of a needed robust debate on the issue. Rather than attempting to fix an issue, or guarantee privacy not explicitly guaranteed in the Constitution, the Court, in strictly interpreting textual provisions should allow inconsistencies and inadequacies in the law to manifest themselves, allowing the legislators to address these in a manner that accords with the will of the people.

IX. Conclusion

The *Katz* test, with its focus on privacy, may seem to provide flexibility for Fourth Amendment protections in the context of a digital world, but in reality, it has not produced a great shift in

[224] SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 745 (1984) (stating explicitly that the Right to Financial Privacy Act, 12 U.S.C. § 3401, was passed in response to the Court's ruling in *Miller*).
[225] 18 U.S.C. § 3121(a). The Court upheld the use of a pen register under the third-party doctrine. Smith v. Maryland, 442 U.S. 735, 742–44 (1979).
[226] Richard J. Pierce Jr., *The Due Process Counterrevolution of the 1990s*?, 96 COLUM. L. REV. 1973 (1996) (stating that legislatures and agencies "are far better than courts at performing the difficult empirical work required to estimate the costs and benefits of alternative decisionmaking procedures.").

outcomes. Similarly, though the *Carpenter* decision departs from the third-party doctrine, announcing a right of privacy in the whole of one's physical movements, the case need not be disruptive of the Fourth Amendment status quo. As technology continues to advance, however, it becomes clearer that the Fourth Amendment may not continue to stretch and provide protection to privacy generally without completely detaching it from the literal text.

Courts should see in *Carpenter* an opportunity to take a more text-based approach and return to property concepts on which the Fourth Amendment was based. Indeed, there is no need for courts to assume the role of guardians of privacy as that is both the province of Congress, and something they have shown themselves capable of addressing.