2019

Protecting Online Privacy in the Digital Age: Carpenter v. United States and the Fourth Amendment's Third-Party Doctrine

Cristina Del Rosso
University of Central Florida

PROTECTING ONLINE PRIVACY IN THE DIGITAL AGE: CARPENTER V. UNITED STATES AND THE FOURTH AMENDMENT'S THIRD-PARTY DOCTRINE

by

CRISTINA DEL ROSSO

A thesis submitted in partial fulfillment of the requirements for the
Honors in the Major Program in Legal Studies in the
College of Community Innovation and Education
in The Burnett Honors College at the University of Central Florida
Orlando, Florida

Fall Term
2019

Thesis Chair: Dr. Carol Bast

ABSTRACT

The intent of this thesis is to examine the future of the third-party doctrine with the proliferation of technology and the online data we are surrounded with daily, specifically after the United States Supreme Court's decision in *Carpenter v. United States*. In order to better understand the Supreme Court's reasoning in that case, this thesis will review the history of the third-party doctrine and its roots in *United States v. Miller* and *Smith v. Maryland*. A review of Fourth Amendment history and jurisprudence is also crucial to this thesis, as it is imperative that individuals do not forfeit their Constitutional guarantees for the benefit of living in a technologically advanced society. This requires an understanding of the modern-day functional equivalents of "papers" and "effects." Furthermore, this thesis will ultimately answer the following question: Why is it legally significant that we protect at least some data that comes from technologies that our forefathers could have never imagined under the Fourth Amendment?

Looking to the future, this thesis will contemplate solutions on how to move forward in this technology era. It will scrutinize the relevancy of the third-party doctrine due to the rise of technology and the enormous amount of information held about us by third parties. In the past, the Third-Party Doctrine may have been good law, but that time has passed. It is time for the Third-Party Doctrine to be abolished so the Fourth Amendment can join the 21st Century.

ACKNOWLEDGEMENTS

I would like to thank everyone who helped me throughout my journey of writing this thesis. Thank you, Dr. Carol Bast, for being my thesis chair. I will never be able to express how thankful I am for your guidance, mentorship, and the overall positive impact you have had on my life.

Thank you, Dr. Barry Edwards and Dr. Brett Meltzer for your guidance. Thank you for your patience, support, and confidence in me throughout this process.

To my friends, thank you for your continued encouragement and understanding.

And most importantly, thank you to my family for cheering me on through every endeavor. I am so thankful for your endless support and love. Thank you for raising me into the woman I am today.

Table of Contents

INTRODUCTION

Our world has evolved. Modern society is largely dependent on technology, and there is a never-ending appetite for scientific development; there is often new technology released that is making our lives more convenient, and more connected, than ever. Each click and internet search leaves a digital trail to be stored and stitched together to reveal an individual's innermost private life. Current law provides little privacy protection to individuals, undermining our Fourth Amendment safeguard that many hold essential to our individual freedoms. The Fourth Amendment to the United States Constitution[1] states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no [w]arrants shall issue, but upon probable cause."

There is a consensus in the basic meaning of the Fourth Amendment; it is intended to guarantee Americans the right to be secure against "unreasonable searches and seizures" conducted by the government. The term "unreasonable" or reasonable has become a basic principle that has been used to guide authority. However, in today's increasingly digitally connected world where we have little choice but to use the internet to function in today's society, there is a concern as to what exactly is "reasonable" because many our smart devices share our information with third parties. In fact, in a world where digital technology has revolutionized the way we conduct our daily business, many of us increasingly feel like we do not have an expectation of privacy.[2]

---

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

[2] *See* Scenario ONE: The New Normal, Ctr. for Long-Term Cybersecurity, U.C. Berkeley, https://cltc.berkeley.edu/scenario/scenario-one/ (suggesting that by 2020, most of our information will be kept online, leaving people vulnerable to data breaches, government intervention, and public display of sensitive information) (last visited Oct. 26, 2019).

This sharing of information has led to a growing privacy gap that denies Fourth Amendment protection, specifically the "Third-Party Doctrine." In a briefing to Members of Congress, the Congressional Research Service described the Third-Party Doctrine as follows:

> In these cases, the Court held that people are not entitled to an expectation of privacy in information they voluntarily provide to third parties. This legal proposition, known as the third-party doctrine, permits the government access to, as a matter of Fourth Amendment law, a vast amount of information about individuals, such as the websites they visit; who they have emailed; the phone numbers they dial; and their utility, banking, and education records, just to name a few.[3]

In our increasingly digital world, companies hold a vast majority of information on behalf of their customers, which we have voluntarily provided. Information that is voluntarily provided is not protected by the Fourth Amendment, as the Court has held that the information that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[4] The doctrine has made it so the government can access information with a standard below probable cause.[5] This standard should be reassessed to fit into our digital age. Property law, reasonable expectation of privacy, and the trespass doctrine, to name a few standards of deciding what is private, are not promising steppingstones on which to continue to base Fourth Amendment claims.

---

[3] RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE, at 15 (2014).
[4] *Id.* at 10 citing Miller v. United States, 425 U.S. at 442 (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).
[5] Margaret E. Twomey, *Voluntary Disclosure of Information as a Proposed Standard for the Fourth Amendment's Third-Party Doctrine,* 21 MICH. TELECOMM. & TECH. L. REV. 401, 402 (2015).

Technological advancements and proliferation of third-party records since the doctrine's inception in two Supreme Court cases decided in the late 1970s, *United States v. Miller*[6] and *Smith v. Maryland*[7], raise questions about the stability of this Doctrine in modern society.

The way the Court has historically looked at the Fourth Amendment is analogous to a patchwork quilt; the Supreme Court tries to fix privacy concerns by considering technological advances one-by-one rather than considering what will come next or how one decision could impact future technologies. *Katz*,[8] *Jones v. United States,*[9] and *Riley v. California*[10] are historical Supreme Court cases that exhibit this piecemeal approach.

As technology transforms the way people participate in society, the core protections of the Fourth Amendment to feel secure in one's person, homes, papers, and effects are beginning to erode. Because of the third-party doctrine, the government can obtain any information a person has disclosed to a third party, as a warrant is not required for police to search and seize consumers' private data on the internet.[11] Instead, the government, or its actors, can issue a subpoena to a third party as a means to capture desired information.[12] For this purpose, a third party is a reference to any non-governmental institution. The third-party doctrine, therefore, allows the government to circumvent our Constitutional guarantees because they do not have a need for warrants. Through interpretation of the third-party doctrine, the Fourth Amendment would not guarantee the privacy of personal data held by private companies, should the government request the information.

---

[6] United States v. Miller, 425 U.S. 435, 436 (1976).
[7] Smith v. Maryland, 442 U.S. 735, 739 (1979).
[8] *Katz,* 389 U.S. at 347.
[9] United States v. Jones, 565 U.S. 400 (2012).
[10] Riley v. California, 573 U.S. 373 (2014).
[11] Christopher Slobogin, *Subpeonas and Privacy,* 54 DEPAUL L. REV. 805, 809 (2005).
[12] *Id.* at 810.

In this way, the third-party doctrine serves as a general warrant because it is a blanket request that provides government access to vast amounts of information retained by third-party service providers. General warrants were antithetical to the Founders wishes at the founding of our country, and this should be carried through in the interpretation today.

Carpenter v. United States is the most recent Supreme Court case that takes issue with the third-party doctrine, specifically focusing on the relatively new issue of cell-site location information, or CSLI. In writing for the majority, Chief Justice Roberts expressed that *Carpenter* was a narrow ruling that left existing precedent undisturbed and would not require, in most cases, a warrant for information held by third-party companies.[13] However, because the ruling was limited in only applying to CSLI, it remains unclear exactly what additional information is protected.

The claim raised is not only that we must reevaluate the Third-Party Doctrine and the way it impacts our life both now and, in the future, but also the impetus to reevaluate the Fourth Amendment as it relates to technology and the law. This thesis will first review the Court's 21st-century technology Third-Party Doctrine-related Fourth Amendment jurisprudence to examine how the current paved path for privacy rights is doomed to fail. This thesis will then examine how the current understanding of the Doctrine applies to certain digital information like the information in *Carpenter*. The author will then consider a few specific types of technology that stores our data and how the privacy we voluntarily share can be used against us in this digital age, particularly, how digital technologies threaten to exclude immeasurable quantities of personal information from Fourth Amendment protection. In conclusion, this thesis will review current theories of privacy and offer suggestions on how to proceed.

[13] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

THE LANGUAGE AND HISTORY OF THE FOURTH AMENDMENT

To discuss the inconsistencies of the Supreme Court's interpretation of the Fourth Amendment, a review of the origins and history is imperative. The first clause of the Fourth Amendment prohibits unreasonable searches and seizures, while the second clause explicitly bans the use of "general warrants."

The Warrant Clause, which is understood to be the second clause of the text, is thought to regulate warrant authority.[14] This clause is believed to ban the use of "general warrants," which are blanket warrants that can be obtained without an "adequate showing of cause."[15] They "allowed officers to search wherever they wanted and to seize whatever they wanted, with few exceptions."[16]

The Founding Fathers "sought to prevent unjustified searches and searchers" from occurring in the first place[17]; regardless of their location, the Founders desired protections for personal items.[18] Moreover, unlike the real property discussed in the text of the Amendment, effects could be carted away by the government. The Founders did not seek a post-intrusion remedy; instead they implemented a deterrent to the government issuance of a nonspecific warrant.[19] Should an officer seize an item without a valid warrant, and the officer's actions be deemed unreasonable, he could be sued by the citizen whose person, house, papers, or effects had been trespassed upon.[20]

---

[14] Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 557 (1999).
[15] *Id.* at 558.
[16] LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 153 (1999).
[17] *Id.* at 576.
[18] Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946, 985 (2016) ("Dictionaries from the period indicate that 'effects' was synonymous with personal property").
[19] LEVY, *supra* note 16, at 577.
[20] Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 SUFFOLK U. L. REV. 53, 60 (1996).

The Founders' goal in eliminating general warrants was to ensure that the oppressive practices of the crown in Great Britain could not be used in their new nation. Famous English cases involving the search and seizure of papers in an effort to silence critics of the King struck a nerve with many of the Colonies. The first of these cases surrounds Mr. John Wilkes, who was accused of writing articles mocking the King and his ministers.[21] Wilkes was subjected to an invasive search under a general warrant and subsequently arrested.[22] Wilkes brought trespass actions against the officers who searched his property, enforcing his right to security in his house; the jury ruled in favor of Wilkes.[23]

The second case, which arose out of similar circumstances to *Wilkes*, was *Entick v. Carrington*[24] a cornerstone case that "foreshadowed the requirements of the fourth amendment's search and seizure clause by holding that seizures of certain papers are impermissibly intrusive."[25] In *Entick*, the Secretary of State authorized a warrant to search for some documents on Entick's land.[26] In carrying out the warrant, many of Entick's books, papers, and pamphlets were seized.[27] Entick sued for trespass, leading the court to condemn the search and seizure, the court holding that the government could not seize private papers even with a valid warrant.[28] For the court, the issue was

[21] Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 VA. L. REV. 869, 887 (1985).
[22] *Id.* at 887. Wilkes was not specifically named in the warrant, nor did the warrant specify items to be seized nor particular places to be searched.
[23] *Id.* at 879.
[24] 19 How. St. Tr. 1029, 95 Eng. Rep. 807 (C.P. 1765). For a complete account on the *Entick* decision, look to the Howell's State Trials. They present 'the Judgment itself at length, as delivered by the Lord Chief Justice of the Common-Pleas from written notes.' 19 How. St. Tr. at 1029.
[25] Schnapper, *supra* note 21, at 877.
[26] *Id.* at 881.
[27] *Id.* at 880 (citing 19 How. St. Tr. at 1030-32).
[28] *Id.* at 876-77 (citing *Entick*, 19 How. St. Tr. at 1073, 95 Eng. Rep. at 818).

much deeper than the physical trespass; rather it was "the indefeasible rights of personal security, liberty, and private property."[29]

The *Wilkes* and *Entick* controversies served as an impetus to the Founding Fathers to ensure these types of governmental overreach that had occurred at the hands of the British were not adopted in their new nation. Instead, the Framers believed judicial officers were more adept at determining whether a search was reasonable[30]; they favored judicial approval for specific warrants to determine whether there were adequate grounds for intrusion.[31]

Although the right to privacy is not expressly granted by the Constitution,[32] Fourth Amendment jurisprudence encompasses an expectation of privacy. In 1890, Samuel D. Warren and Louis D. Brandeis wrote about the legal right to privacy, declaring the right to privacy as an individual's "right of determining ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[33] Furthermore, they articulated privacy as a "right to be left alone."[34]

[29]Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1198 (2016).
[30] Davies, *supra* note 14, at 576.
[31] DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADE OFF BETWEEN PRIVACY AND SECURITY, 4 (2011).
[32] *See* Katz v. United States, 389 U.S. 347, 350 (1967) ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'").
[33] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
[34] *Id.*

THE THIRD-PARTY DOCTRINE AS A GENERAL WARRANT

The Framer's loathed general warrants primarily because they did not want one individual with arbitrary discretion to decide when someone or something would be searched, especially as it relates to "persons, houses, papers, and effects."[35]

The *Wilkes* and *Entick* cases exemplify a time where the English government used general warrants to invade its people at its own Will.[36] This behavior is similar to the third-party doctrine, as it allows for the exercise of broad discretion when dealing with an individual and their effects. Currently, the third-party doctrine enables the police and government to engage in surveillance and monitoring of one's daily life, similar to the general warrant that the Fourth Amendment ultimately intended to prevent. The Founding Fathers would have despised this doctrine.

In today's digitally connected world, police only need to issue a subpoena to a third party to request desired data; there is no warrant requirement.[37] Without a specific warrant, the government is conducting the very type of general searches the Fourth Amendment was adopted to prevent. Our constitutional guarantee to be free from arbitrary government intrusion is derived from this amendment. It rests on our right to be free from government surveillance unless there is probable cause.

The third-party doctrine ignores the warrant requirement in the Fourth Amendment and allows the police to circumvent a warrant request from a judge, undermining our free society and creating a society that can be routinely surveilled.

---

[35] U.S. CONST. amend. IV.
[36] *See* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 43, 56-58, 96-100, 439-40, 490-91 (2009).
[37] *See* Slobogin, *supra* note 11, at 826.

THIRD-PARTY DOCTRINE CASE REVIEW

The progression of case law can help determine whether the third-party doctrine should still govern access to information as technology becomes increasingly complex and common. The following Supreme Court cases detail the third-party doctrine progression.

Katz is the starting point for many of the Fourth Amendment cases because this is where the Court established the reasonable expectation of privacy test articulated by Justice Harlan in the concurrence.[38] Harlan's two-part framework first asks whether an individual retained an "actual (subjective) expectation of privacy," and second, whether that expectation is one that "society is prepared to recognize as 'reasonable.'"[39] The party must satisfy both prongs to this test to claim an intrusion under the Fourth Amendment. The Court has since validated this framework to be controlling in Fourth Amendment analysis.

In *Katz*, the Court held that electronically listening to and recording of the defendant's words, wiretapping, in a public phone booth with the door-closed violated the defendant's privacy upon which he relied.[40] Because the defendant in Katz took a reasonable step to protect his privacy by shutting the door to the booth,[41] he was likely more concerned about an "uninvited ear" than an "intruding eye."[42]

Prior to *Katz*, the Court had held that searches typically had to occur in someone's home. Following *Katz*, physical intrusions were no longer necessary to claim a search had occurred under

[38] *See Katz,* 389 U.S. at 347 (Harlan, J., concurring).
[39] *Id.* at 362.
[40] *Id.* at 352.
[41] *Id.* at 354.
[42] *Id.* at 352.

the Fourth Amendment.[43] In establishing this new provision, the Court reasoned that "the Fourth Amendment protects people, not places .... [W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[44]

Miller and *Smith* are two of the most important Fourth Amendment cases decided by the Supreme Court in the 20th century. Both of these cases came before the rise of the mass digital information aggregation, and since these cases, there has been a surge of data collection and processing. In *United States v. Miller*, Miller was suspected of running an illegal whiskey distillery.[45] Federal agents subpoenaed his bank records, and Miller objected, claiming his bank records were his private papers. The Court overruled this objection, holding that because the banking information was shared voluntarily with banks, Miller forfeited his privacy attached to his financial records.[46] Because the information was voluntarily shared, Miller was not searched under *Katz*. The Court, appealing to the *Katz* reasonable expectation of privacy test, noted that "[w]hat a person knowingly exposes to the public ... is not a subject of Fourth Amendment protection."[47] In reaching this conclusion, the Court distinguished "private papers" from "business records," finding bank records fit into the latter category.[48] *Miller* suggests that when documents are voluntarily conveyed to a third party, regardless of the purpose of conveyance, the individual relinquishes an expectation of privacy in those documents.

A few years later, the Supreme Court decided *Smith v. Maryland*, holding that a warrant was not required before the police seized the phone number records dialed by a customer from a

---

[43] *Id.* at 352.
[44] *Id.*
[45] United States v. Miller, 425 U.S. 435, 437 (1976).
[46] *Id.* at 435.
[47] *Id.* at 442.
[48] *Id.* at 441.

telephone company. [49] The Court considered that because most people at the time were aware that the phone company recorded the phone numbers they dialed by using the pen registers, there was not a legitimate expectation of privacy.[50] Additionally, because the information was voluntarily disclosed, Smith "assumed the risk" that the telephone company might hand over the information to the police.[51] The Court further reasoned:

> The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.[52]

In this case, the presence of technology did not alter the application of the third-party doctrine. The Court differentiated *Smith* from *Katz,* stating that the pen registers at issue in *Smith* "do not acquire the 'contents' of communications," such as in *Katz*.[53] Justice Stewart further clarified the distinction between content and non-content general records in his dissent in *Smith*:

> Nevertheless, the Court today says [Fourth Amendment] safeguards do not extend to the numbers dialed from a private telephone, apparently because when a caller dials a number the digits may be recorded by the telephone company for billing purposes .... The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet we have squarely held that the user of even a public telephone is entitled "to assume that the words he utters into the mouthpiece will not be broadcast to the world."[54]

---

[49] *Smith*, 442 U.S. at 735.
[50] *Id.* at 743.
[51] *Id.* at 744.
[52] *Id.* at 744-45 (citation omitted).
[53] *Id.* at 741.
[54] *Id.* at 746-47 (Stewart, J., dissenting) (quoting *Katz*, 389 U.S. at 352).

In his dissent, Justice Stewart identified a hindrance in the application of the third-party doctrine: that people should retain a reasonable expectation of privacy in their conversations regardless of where they occur.

In 2012, the Court decided *United States v. Jones*. In this case, government agents installed a Global Positioning System (GPS) tracking device on the defendant's vehicle without a valid warrant.[55] Ultimately, the placement of the device constituted a "search" within the meaning of the Fourth Amendment, with the majority returning to pre-*Katz* doctrine, emphasizing the fact that because the government had physically attached the GPS device to the vehicle (an effect), the government had physically intruded, and therefore, a search had occurred.[56]

A year later, the Court examined warrantless search and seizure of cellular telephone contents incident to arrest in *Riley v. California*.[57] The Court created yet another exception to the Fourth Amendment when they decided that a warrant must be obtained by a judicial officer before law enforcement officers can search the contents of a phone.[58] Although the third-party doctrine was not discussed at length in *Riley*, the opinion did demonstrate the Court's recognition of the difficulties that consumers and courts face when assessing whether an individual has a reasonable expectation of privacy for information stored on electronic devices. The importance of *Riley* comes into play when considering if the data the government is interested in resides on the device because then it should receive the same Fourth Amendment protections as if the data was on a computer or cellphone. The Court in *Riley* also considered the immense storage capacity that is available on

[55] Jones v. United States, 565 U.S. 400, 405 (2012).
[56] *Id.* at 406.
[57] Riley v. United States, 573 U.S. 373, 386 (2014).
[58] *Id.*

cellphones, in that modern cellphones gather information and store that information in one place and that the records can give a detailed look into an individual's life.[59]

Thus, *Jones* is controlling when a trespass arises without a physical intrusion—such as a GPS—whereas *Riley* is controlling when searching a cell phone's data requires a warrant. *Jones* and *Riley* were the Court's first steps in addressing technology in the digital age. The recent case of *Carpenter* is a blend of these two cases, from *Jones*—long term tracking and from *Riley*—a device that can pinpoint location with near-perfect accuracy.

In *Carpenter v. United States*, the petitioner was charged with aiding and abetting robbery that affected interstate commerce, after the FBI requested three orders from a magistrate judge for cell phone records[60] under the Stored Communications Act (18 U.S.C. 27039(d)).[61] This Act, enacted by Congress as Title II of the Electronic Communications Privacy Act (ECPA), set provisions regarding privacy expectations regarding means of electric transmission, which includes telephones and computers.[62] With *Carpenter*, it gave the government access to petitioner's cell-site location information (CSLI) obtained from a third-party cell-phone service provider that would otherwise be private information. CSLI is produced when a phone user sends or receives data, such as phone calls or text messages, that is then transmitted to the closest cellular tower through radio waves, thus producing precise records.[63] These records include the date and time of transmitted data and the approximate location where the call began and ended based on the location to the nearest cell

---

[59] *Id.* at 375.
[60] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018)
[61] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860-68 (codified as amended at 18 U.S.C. §§ 2701-2712 (2015)).
[62] *Id.*
[63] V. Alexander Monteith, *Cell Site Location Information: A Catalyst for Change in Fourth Amendment Jurisprudence*, 27-FALL KAN. J.L. & PUB. POL'Y 82, 84 (2017).

tower.[64] Under the Stored Communications Act, law enforcement does not need to obtain a search warrant from cell service providers for these records; rather, law enforcement must only obtain a court order by meeting reasonable suspicion standard, which is below the burden of proof of probable cause needed for a warrant.[65]

In the case of Mr. Carpenter, the police obtained a court order that allowed them to search Carpenter's cell records, pursuant to the Stored Communications Act.[66] In order to receive this order, law enforcement showed the government that they believed the records would be relevant to a robbery investigation after receiving tips from one suspect who provided the accomplice's cell phone number to the police.[67] The government collected "12,898 location points cataloging Carpenter's movements," which is "an average of 101 data points per day"[68] over 127 days.[69] Using these location points, Carpenter was placed at the scene of four robberies in question, leading to Carpenter's conviction and a prison sentence of one-hundred years.[70] Following the conviction, Carpenter appealed to the Sixth Circuit, then filed a petition for certiorari, which was granted by the Supreme Court.[71]

The New Rule of Carpenter

Prior third-party doctrine cases such as *United States v. Miller* and *Smith v. Maryland* left individuals with no legitimate fourth amendment expectation of privacy claim in information

[64] *Carpenter*, 138 S. Ct. at 2221.
[65]Monteith, *supra* note 63, at 83.
[66] *Carpenter*, 138 S. Ct. at 2212.
[67] *Id.*
[68] *Id.* at 2213.
[69] *Id.*
[70] *Id.* at 2212.
[71] *Id.* at 2213.

voluntarily shared with third parties.[72] At first blush, because CSLI is held by carriers (a third party) and not customers, it appeared to fall under this doctrine, leaving U.S. citizens vulnerable to retrospective location-tracking and warrantless searches on behalf of the government. Chief Justice Roberts, in writing for the majority took a different approach.

Chief Justice Roberts wrote, "As technology has enhanced the Government's capacity to encroach upon areas normally guarded against inquisitive eyes, this Court sought to "assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[73] He added that because "an individual maintains a legitimate expectation of privacy in the record of his physical movements," the third-party doctrine does not extend to mobile location information.[74]

Since CSLI is no more than a byproduct of owning a cellphone, the government generally needs a warrant to access those records, especially if the government is requesting more than seven days of records from the cell phone carrier.[75] The police cannot collect historical CSLI from a cell phone service provider, according to the majority in *Carpenter*, due to its "depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection."[76] If the depth and reach of the surveillance threaten "a too permeating police surveillance," it may be justifiable to designate the search as an intrusive search under the Fourth Amendment.[77]

---

[72] Smith v. Maryland, 442 U.S. 735, 743-44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).
[73] *Carpenter*, 138 S. Ct. at 2214 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).
[74] *Id.*
[75] *Id.* at 2235. The Court did not explain why seven days is the maximum for surveillance. Subsequent cases will have to weigh this cut off against privacy interests.
[76] *Id.* at 2223 ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection").
[77] *Id.* at 2217.

Due to the "world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today,"[78] the majority declined to extend the third-party doctrine to the government's request for CSLI.[79] Although the Court noted that "seismic shifts in digital technology" has transformed the traditional third-party doctrine, Chief Justice Roberts limited the language of *Carpenter* further beyond the application of *Smith* and *Miller*, stating the decision does not "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."[80]

Rather than close this gap in legislation, the Court in *Carpenter* crafted a narrow exception to the third-party doctrine for the "unique nature of cell phone location information, requiring the government to obtain a warrant before compelling carriers to relinquish customer's CSLI records."[81] The Court made sure to emphasize that this ruling did not impact *Miller* and *Smith*.[82]

This effort to limit the scope of *Carpenter* raises questions about the enormity of information that resides outside of the outdated pen registers discussed in *Smith v. Maryland* and the paper bank statements at issue in *United States v. Miller*. In *Carpenter,* "the Government can access each carrier's deep repository of historical location information" with "just the click of a button."[83] The Court also clarified that there is no distinction between the contents of cellphones and the CSLI metadata it

[78] *Id.* at 2219.
[79] *Id.* at 2220 (finding that CSLI "implicate[d] privacy concerns far beyond those considered in *Smith* and *Miller*").
[80] *Id.*
[81] *Id.* at 2217.
[82] *Id.*
[83] *Id.* 2217-18.

generates. The availability of all this information causes concern when considering how common technology is in our society and the vast amount of information that is shared online.

Carpenter raises questions about the validity of the *Katz* test in a digital world, with many questions challenging its continued value. This is because evolving technologies transform which expectations of privacy are considered "reasonable," as Justices Thomas and Gorsuch have noted.[84] At the time *Miller* and *Smith* were decided, forfeiting privacy rights on a tangible item like a pen register or bank documents seemed reasonable. Conveying the third-party doctrine to also apply to online activity where most of the data is stored in one place poses challenges. As Justice Sotomayor expressed in her concurrence in *Jones*:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[85]

Technology adds a complex layer to evaluating privacy expectations. The Court in *Carpenter* had a chance to set the record straight on exactly how the government can and should interact with technology. In spite of that, the rules for engagement are now even more confusing after the narrow ruling in *Carpenter*. It leaves many questions and invites relentless future arguments before the Supreme Court on the topics of technology and privacy. For example, open questions include exactly how much digital data law enforcement may possess without a warrant and when a third party is required to disclose its business records. While *Carpenter* did signal that the Fourth

[84] Carpenter, 138 S. Ct. at 2235-46 (Thomas, J., dissenting), 2261-72 (Gorsuch, J., dissenting).
[85] Jones v. United States, 565 U.S. 400, 417-18 (citation omitted) (Sotomayor, J., concurring) (2012).

Amendment may protect other types of personal information held by third parties, like records regarding location information, the case also raises questions about third-party files on a par with CSLI.[86] Because there was no constitutional limit discussed in *Carpenter* regarding CSLI, there is no legal limit to restrict location surveillance by law enforcement; the impacts of *Carpenter* reach far beyond CSLI, which fails to protect privacy interests while advancing the interests of government spying.

[86] *See infra* note 89 and accompanying text.

VOLUNTARY CONVEYANCE AND ASSUMPTION OF RISK

The crux of the Court deciding in favor of Carpenter was whether the automatic generation of CSLI is no more than a byproduct of having a cell-phone; cell-phones require no affirmative action on behalf of the user.[87] In other words, as long as the phone is powered on and there is a cell phone tower near the phone's location, the location is being recorded and transmitted to the third-party cell phone carrier.

Generally, voluntary conveyance is the premise that threatens the third-party doctrine in the technological era. For an action to be voluntary, it must have been intended, which presumes the individual knew the information would be conveyed.[88] Given how omnipresent and necessary technology and technological disclosures are, it is nearly impossible to deem these actions as voluntary.

Prior cases involving privacy have referred to this voluntary participation as an "assumption of risk."[89] Assumption of risk is "when a party reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs, the Fourth Amendment does not prohibit governmental use of that information."[90] Under the third-party doctrine principles of voluntary conveyance and assumption of risk, law enforcement and the government are entitled to investigate information disclosed to a third party businesses without a

---

[87] *Carpenter,* 138 S. Ct. at 2210.
[88] *See Definition of Voluntary by Merriam-Webster*, Merriam Webster (September 24, 2019), http://www.merriam-webster.com/dictionary/voluntary [https://perma.cc/TXS3-A3HP] ("voluntary: done by design or intention: intentional").
[89] *See Smith*, 442 U.S. at 745; *see also Miller*, 425 U.S. at 443; *see also Carpenter,* 138 S. Ct. at 2212.
[90] Denae Kassotis, Note, *The Fourth Amendment and the Technological Exceptionalism After Carpenter: A Case Study on Hash-Value Matching*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1243, 1275 (citing United States v. Jacobsen, 466 U.S. 109, 117 (1984)).

warrant. Merely allowing a device into one's living sphere should not be enough to void our privacy rights guaranteed to us since the time of this country's founding.

Recently, in *Carpenter*, the Court declined to extend the third-party doctrine to CSLI because voluntary exposure did not apply as carrying a cell phone has become commonplace; it was considered "indispensable to participation in modern society."[91] The same will be true of smart home devices, in addition to many of our other smart devices.

An individual may initiate self-surveillance, for example, by buying an Amazon Echo or using a smartwatch; therefore, it could be construed that while using the basic functions of the device the individual has affirmatively engaged the device to relay a multitude of information. However, the individual does not intend, nor could ever imagine, the depths of the information these devices share, especially when this information is sent to other third parties to market products to consumers.[92] We connect to technology to establish and maintain relationships and function in society. We voluntarily disclose detailed information about our private lives, such as information about our religious views or sexual preferences, to social media platforms, such as Facebook, Twitter, and LinkedIn so we can participate in digital social life. Many of these third-party service providers or social media platforms ask users to click "I Agree" after a long terms of service agreement or privacy disclosure agreement. However, the average person does not have time to read this lengthy document, and nor can they understand the complicated legalese that the agreement often contains. Or, if he can understand the complicated legalese, he fails to understand the ramifications of sharing the information or even the depths of information stored on him.

---

[91] *Carpenter*, 138 S. Ct. at 2220.
[92] *See e.g.* Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423 (2018).

THIRD-PARTY DOCTRINE IMPACT ON TECHNOLOGIES

Self-cyber-surveillance is the "intentional or consensual creation of mass information about oneself through electronic tracking or other means."[93] This self-cyber-surveillance has changed the daily lives of many individuals, including how private their information is. Assistive technologies present an issue in the accumulation of data retained by third-party businesses.[94] This data creation and collection is described loosely as the Internet Of Things, or IoT.[95] IoT is defined as the "aggregation of systems of networks connected by the Internet or other radio-type device," which "creates consensual mass self-surveillance."[96] Because this includes any device with an on/off switch to the Internet, a host of devices are included that seamlessly share information to "improve consumer, commercial, health, and other needs."[97] The records aggregated from these devices could be either metadata or content, or a mix of both. Examples of these devices include medicine dispensers that remind individuals to take their medicine,[98] thermostats that allow individuals to adjust their preferred settings from a smartphone,[99] or even a trashcan that "scans the barcodes of discarded products, automatically adds them to a smartphone's shopping list, and sends a text when

[93] Steven I. Friedland, *Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things is Changing the Face of Privacy*, 119 W. VA. L. REV. 891, 892 (2017).
[94] The issue raised is only when the data resides in the cloud or in the hands of a third-party service provider. If there is data that is housed in the device, it is protected under *Riley*.
[95] Friedland, *supra* note 93, at 892.
[96] *Id.*
[97] Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 814 (2016).
[98] Paul Kominers, *Interoperability Case Study, Internet of Things (IoT)*, Berkman Ctr. for Internet & Soc'y (Apr. 16 2012), https://cyber.law.harvard.edu/node/97248 [https://perma.cc/VG3W-4DER].
[99] *How Home/Away Assist Uses Your Phone's Location*, Nest, https://support.google.com/googlenest/answer/9262475?hl=en (last visited November 1, 2019).

the trashcan is full."[100] This also includes in-home technologies, such as the Amazon Echo and biometric data found on Apple Watches and FitBit Devices. The information shared with these devices can also be shared with other devices and applications. Many of these devices already work off the same passive data collection that smartphones do; similarly, the signals from the devices make them communication devices. Thus, they are synonymous and should be protected with the reasoning behind CSLI in *Carpenter*.[101]

The aggregation of smart technology data also allows the government to work with corporations to create detailed reports of unsuspecting individuals who may have committed crimes.[102] Since *Carpenter*'s narrow decision regarding CSLI, the third-party doctrine remains relatively undisturbed. However, more information will continue to be shared with third-party service providers, especially with the advent of new technology. This allows for the disjunction between our constitutional protections and technology surveillance and allows the gap between the two to become progressively more pronounced. In fact, the fear of government surveillance is not speculative; the government has requested data in the past, notably, to solve crimes, but it would not be far-out to imagine this data being used in nefarious ways.

---

[100] Ryan G. Bishop, Note, *The Walls Have Ears, And Eyes, And Noses: Home Smart Devices and the Fourth Amendment*, 61 ARIZ. L. REV. 667, 668 (2019).
[101] Christopher Mims, *All Ears: Always-On Listening Devices Could Soon Be Everywhere*, WALL STREET J. (July 12, 2018, 12:00 PM), https://www.wsj.com/articles/all-ears-always-on-listening-devices-could-soon-be-everywhere-1531411250.
[102] *See* Trevor Timm, *The Government Just Admitted it Will Use Smart Home Devices for Spying*, GUARDIAN (February 9, 2016), https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government/.

A. Smart-Home Devices

Smart-home devices "connect the devices and appliances in your home so that they can communicate with each other and with you."[103] These devices are a natural progression of the Internet of Things. Accordingly, a smart-home is defined by appliances or devices that are capable of connecting with one another through phone applications and the internet.

The Amazon Echo is a smart-home device that can respond to voice queries about the weather, turn down the lights or the temperature, or even order the groceries.[104] Alexa, Amazon's voice-activated digital assistant powers Echo devices.[105] For the Echo to respond to the owner's request, she listens for the device wake word, "Alexa."[106] Meanwhile, the Echo "records your voice and transfers it to a processor for analysis"; the recordings are streamed and stored remotely in the cloud and can be reviewed at a later date.[107] The preferences expressed by individuals to their smart home devices are used to create a comprehensive profile, which is shared by third parties, based on the specific consumer's activities, including his daily activities (through the calendar applications) or his health profile (through health monitoring applications).

---

[103] Molly Edwards & Nathan Chandler, HowStuffWorks.com, *How Smart Homes Work*, http://home.howstuffworks.com/smart-home1.htm (last visited October 25, 2019).
[104] Brief for Technology Companies as Amici Curiae in Support of Neither Party at 9, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).
[105] Anne Pfeifle, *Alexa, What Should We Do About Privacy? Protecting Privacy for Users of Voice-Activated Devices*, 93 WASH. L. REV. 421, 422. (2018) (citing Robert Hackett, *Amazon Echo's Alexa Went Dollhouse Crazy*, FORTUNE (Jan. 9, 2017), http://fortune.com/2017/01/09/amazon-echo-alexa-dollhouse/.
[106] *Id.* at 421-22. (citing Robert Hackett, *Amazon Echo's Alexa Went Dollhouse Crazy*, FORTUNE (Jan. 9, 2017), http://fortune.com/2017/01/09/amazon-echo-alexa-dollhouse/
[107] Eliott C. McLaughlin, *Suspect OKs Amazon to hand over Echo recordings in murder case*, CNN BUSINESS (April 26, 2017, 2:52 PM), https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html.

A specific example occurred in a widely publicized 2015 case where it was alleged an Amazon Echo picked up the audio of a man, James Bates, murdering his wife in his home.[108] Although Mr. Bates voluntarily consented to the release of records held by Amazon, this is a cautionary tale of the information the Amazon Echo retains and is later available information that the government can seize under the third-party doctrine. These records contain some of our innermost thoughts, including details about our familial, professional, and religious and political ties.

On the one hand, because the Echo users voluntarily convey this information to third parties, there are no Fourth Amendment protections involved. In contrast, Fourth Amendment jurisprudence has rendered the Home supreme.[109] In fact, Justice Scalia stood firm that the core idea of the Fourth Amendment is the right to be free from reasonable government intrusion, which should include an individual's right to retreat into his own home.[110] Furthermore, *Riley* concerns are implicated due to the capabilities of these smart home devices. The home has been considered a sacred place since the Framers and following through the Fourth Amendment history. However, IoT has grown, mostly unregulated, and it is threatening the sanctity of the home. If the police were to physically enter your house and seize your IoT device, later downloading the data, you would have a trespass to your property or effects, and therefore a violation of your privacy. This concept becomes hazy when discussing an interception of your data on the device. This is because, since the Echo is always listening, the device serves as a covert listening device, or—informally—"a bug," or

---

[108] *Id.*

[109] *See* Donohue, *supra* note 29, at 1188. *See also* United States v. Karo, 468 U.S. 705, 714 (1984) ("At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable.").

[110] Florida v. Jardines, 569 U.S. 1, 13 (2013) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)). *See also* Justice Scalia's reasoning in *Kyllo*, ""in the home ... *all* details are intimate details." Kyllo v. United States, 533 U.S. 27 at 37 (2001).

wiretap. While a user can delete the records that Alexa creates (although it is unclear how much of the records are deleted from the cache of information), it is strongly discouraged because the loss of records impairs the performance of the device.[111] Compelling individuals to give up their privacy rights to their information stored by third parties for the sake of convenience is not reasonable nor acceptable.

When an individual acquires a new device, he is most likely not rushing home to read the privacy policy. Rather, he rushes home to install the new piece of technology and start using it. This hastiness almost always results in the user giving up their data in exchange for the use of the new device. For example, in 2015, Samsung was in the news for a privacy policy related to the use of their Smart TV's.[112] The company had initially cautioned customers that, through the use of voice recognition, data would be transmitted to third parties.[113] It did not take long for consumers and news outlets to begin reporting on the issue, comparing the Samsung Smart TV to the telescreens featured in George Orwell's *1984*.[114] Following the backlash, Samsung changed the Smart TV privacy policy to state explicitly how Voice Recognition worked. The new policy is as follows:

> If you enable Voice Recognition, you can interact with your Smart TV using your voice. To provide the Voice Recognition feature, your voice commands will be transmitted (along with information about your device, including device identifiers) to us and we will convert your voice commands into text to provide the Voice Recognition features. In addition, Samsung may collect voice commands and associated texts so that we can evaluate and improve the features. Samsung will collect your voice commands when you make a specific request to the Smart TV by

[111] Jing Cao & Dina Bass, *Why Google, Microsoft, and Amazon Love the Sound of Your Voice*, BLOOMBERG TECH. (Dec. 13, 2016), https://www.bloomberg.com/news/articles/2016-12-13/why-google-microsoft-and-amazon-love-the-sound-of-your-voice [https://perma.cc/5DW7-ATQ8].
[112] *See, e.g.*, Andrew Griffin, *Samsung smart TV policy allows company to listen in on users*, INDEPENDENT (Feb. 9, 2015), http://www.independent.co.uk/life-style/gadgets-and-tech/news/samsungs-new-smart-tv-policy-allows-company-to-listen-in-on-users-10033012.html.
[113] Natasha Lomas, *Samsung Edits Orwellian Clause Out of TV Privacy Policy*, TECH CRUNCH (Feb. 10, 2015), http://techcrunch.com/2015/02/10/smarttv-privacy/#.puzvmzo:yfMB.
[114] *Id.*

> clicking the activation button either on the remote control or on your screen or by speaking a wake word…and speaking into the microphone on the remote control or Smart TV.[115]

Samsung also clarified that individuals could opt-out of voice recognition if they had privacy concerns, but the capabilities would be impacted.

B. Biometric Technology

FitBit devices, a computing watch designed to track physical activity, raise additional concerns. Typically, the FitBit monitors blood pressure, gives a sleep assessment, and counts steps, which is intended for consumers to gauge their personal health better.[116] This device also logs location information, uploading this information to a computer or mobile device if it is within range of a wireless internet source.[117]

This biometric data involves private information that, without the device, the individual otherwise most likely would not have; this information is extraordinarily intimate. However, this information can be "accessed, aggregated--even anonymized--and sorted by health companies or insurers to predict health trends and create more efficiencies in their businesses," which could pique the interest of other third parties and the government.[118] Anonymity may not be enough, though, to ensure our privacy is protected. In fact, according to one researcher, "[t] he way we move . . . is so unique that four points [of location information] are enough to identify 95% of people."[119]

---

[115] *Samsung Privacy Policy--SmartTV Supplement*, Samsung, http://www.samsung.com/sg/info/privacy/smarttv.html (last visited Oct. 22, 2019).
[116] Twomey, *supra* note 5, at 419.
[117] *Help Article: How do I get data from my tracker to the website?*, fitbit help, http://help.fitbit.com/articles/en_US/Help_article/How-do-I-get-data-from-my-tracker-to-the-website/?l=en_US&fs=RelatedArticle (last updated Aug. 13, 2019).
[118] Friedland, *supra* note 93, at 897.
[119] Jason Palmer, *Mobile Location Data 'Present Anonymity Risk,'* BBC NEWS (Mar. 25, 2013), http://www.bbc.co.uk/news/science-environment-21923360.

The technology behind Fit Bit devices is advanced enough that Fit Bits can track physical exertion consistent with violent acts[120] or monitor an elevated blood pressure under the influence of drugs.[121]

This newfound way of continued attachment to the digital world begs one major question: Would the information gathered, likely voluntarily, through various sources be a business record, thereby requiring third-party services to turn over the information on their customers?

C. Internet Tracking

It is unclear whether *Carpenter* applies consistently to all forms of location data, specifically geotags which are embedded in a digital photograph that describes the time, date, and GPS coordinates of where the photo was taken and where the individual logged on to the social media site if the photograph was posted.[122] They are similar to CSLI because they are automatically collected without affirmative action by the user. However, it is different because posting a picture on a public social media site is an affirmative action in which the user acknowledges that an indiscriminate group of people could see the post. This is what happened to millionaire John McAfee, founder of McAfee Security Software Company.[123] McAfee was wanted by law enforcement in connection with a crime, and although he threw out some taunts, authorities could

---

[120] Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 561 (2017) (citing Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 93 (2014)).

[121] *Id.* (*See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects 104* CALIF. L. REV. 805, 809-11, 825 (2016).

[122] Definition - What does *Geotagging* mean?, https://www.techopedia.com/definition/86/geotagging (last visited Nov. 1, 2019).

[123] Craig Timberg, *Hacker Locates John McAfee through Smartphone Tracks*, The Washington Post (Dec. 4, 2012), https://www.washingtonpost.com/business/economy/hacker-locates-john-mcafee-through-smartphone-tracks/2012/12/04/55a498d8-3e4a-11e2-bca3-aadc9b7e29c5_story.html.

not catch him, until a journalist took a photo with McAfee and uploaded it online.[124] This photo had been routinely geotagged, leading a computer hacker to MacAfee's exact location in a Guatemalan village.[125] While this case was a win for the police, this case should resonate with the average person. It was not difficult for this computer hacker to collect this information, even after MacAfee believed he had taken steps to conceal his location. Hackers with bad intentions could have received this geotagged location and took care of MacAfee, or in the case MacAfee had not been accused of anything, the police could have reviewed it for evidence.

The government also has access to many of our routine activities. As Eleventh Circuit Judge Beverly Martin expressed:

> Nearly every website collects information about what we do when we visit…the Fourth Amendment allows the government to know from YouTube.com what we watch, or Facebook.com what we post or whom we "friend," or Amazon.com what we buy, or Wikipedia.com what we research, or Match.com whom we date—all without a warrant. In fact, the government could ask "cloud"-based file-sharing services like Dropbox or Apple's iCloud for all the files we relinquish to their servers. I am convinced that most internet users would be shocked by this.[126]

We leave a digital footprint anytime we interact with devices that connect to the internet. Paul Ohm, professor at Georgetown Law Center and privacy advocate, testified to Congress with respect to the trove of data collected by sources:

> The list of websites an individual visits, available to a [broadband Internet access service] provider even when https encryption is used, reveals so much more than a member of a prior generation would have revealed in a composite list of every book she had checked out, every newspaper and magazine she had subscribed to, every theater she had visited, every television channel she had clicked to, and every bulletin, leaflet, and handout she had read. No power in the technological history of our nation has been able until now to watch us read individual articles, calculate how

[124] *Id.*
[125] *Id.*
[126] United States v. Davis, 785 F.3d 498, 536 (11th Cir. 2015) (Martin, J., dissenting).

> long we linger on a given page, and reconstruct the entire intellectual history of what we read and watch on a minute-by-minute, individual-by-individual basis.[127]

Our web browsing records allow the government an unprecedented amount of information, and a staggering amount is left unprotected. For instance, individuals share information about themselves simply by surfing the web because of the tracking methods websites use to store information.[128] One way websites track us is through cookies, which are small pieces of code sent back to the company that details "whether you are a returning user, the sites you visited before, and after visiting their web site, the items you view on a web site, and sometimes even the information you enter into the computer while on the web site."[129]

D. Storage in the Cloud

In today's era, much of our private data is held in the "cloud," which is defined as a "combination of structured, semistructured, and unstructured data collected by organizations that can be mined for information and used in…advanced analytics applications."[130] Essentially, the user "rents space" on a trusted server.[131] They may do this either because their computer cannot store enough on its hard-drive, for additional protection should a file be wiped off their computer, or both. Many users find cloud storage extremely convenient, largely because the cloud can be accessed

---

[127] *FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the H. Subcomm. on Commc'n & Tech. of the H. Comm. on Energy & Commerce*, 114th Cong. 5 (2016) (statement of Paul Ohm, Professor, Georgetown University Law Center).
[128] Derek S. Witte, *Bleeding Data in a Pool of Sharks: The Anathema of Privacy in a World of Digital Sharing and Electronic Discovery*, 64 S.C. L. REV. 717, 731 (2013).
[129] *Id.*
[130] Margaret Rouse, *Big Data*, *Tech Target: AI in IT Tools Promises Better, Faster, Stronger Ops* (last visited October 31, 2019), https://searchdatamanagement.techtarget.com/definition/big-data.
[131] Erik C. Shallman, Comment, *Up in the Air: Clarifying Cloud Storage Protections*, 19 INTELL. PROP. L. BULL. 49, 54 (2014).

remotely. Nevertheless, cloud storage is problematic because it requires users to give their data to a third-party service provider who will then store this vast quantity of information.

Apple's iCloud Privacy Policy relating to cloud storage and law enforcement provides:

> You acknowledge and agree that Apple may, without liability to you, access, use, preserve and/or disclose your Account information and Content to law enforcement authorities, government officials, and/or a third party, as Apple believes is reasonably necessary or appropriate, if legally required to do so or if Apple has a good faith belief that such access, use, disclosure, or preservation is reasonably necessary to: (a) comply with legal process or request; (b) enforce this Agreement, including investigation of any potential violation thereof; (c) detect, prevent or otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of Apple, its users, a third party, or the public as required or permitted by law.[132]

This privacy policy affords very little protection to consumers' data once the data is transferred to the Apple iCloud.

[132] *iCloud Terms and Conditions*, APPLE, https://www.apple.com/legal/internet-services/icloud/en/terms.html (last revised Sept.19, 2019).

THE FUTURE OF THE CLOUD

The Stored Communications Act (SCA) that is part of the Electronic Communications Privacy Act (ECPA) was an act created to regulate electronic communications.[133] However, it reflects the technology of the 1960s, thereby rendering it nearly ineffective to support privacy intrusions from the government on third-party servers that store and process the data that emanates from our modern devices.[134]

At the time of the SCA's enactment, "digital information still resided in large data centers" and "the data stored in data centers were not readily transportable."[135] Because we, and companies, store our data everywhere, the question becomes how we should interpret the SCA in the digital age. According to the SCA, a warrant is not required if the data has been stored for more than 180 days.[136] This stipulation made sense during this time, as the online storage of data in the cloud was extremely costly, and the Internet of Things had not begun to ubiquitously aggregate data as it does now. Privacy expectations should not diminish merely because 180 days has elapsed, just as privacy expectations do not diminish solely because time has passed.

This outdated language leads to another problem. The SCA defines electronic storage "both as 'any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof' and 'any storage of such communication by an electronic communication service for purposes of backup protection of such communication.'"[137] Privacy

---

[133] Witte, *supra* note 128, at 748.
[134] Mark Wilson, Comment, *Castle in the Cloud: Modernizing Constitutional Protections for Cloud-Stored Data on Mobile Devices*, 43 GOLDEN GATE U. L. REV. 261, 263 (2013); Witte, *supra* note 128, at 748.
[135] Wilson, *supra* note 134, at 263.
[136] 18 U.S.C.A. § 2703(a) (Westlaw 2012).
[137] Wilson, *supra* note 134, at 277 (citing 18 U.S.C.A. § 2510(17) (Westlaw 2012).

protections hinge in these crucial distinctions, but this second definition will cause problems with the popularity of the cloud, as the language of the statute excludes much of the currently stored data.[138] It also does not account for how quickly and easily information can be accessed by a third party, which traditionally might have been stored on a computer's hard drive or in a file cabinet. The immense information stored on a Cloud should be afforded greater protections than are currently provided. For example, much of the information stored through the third-party service Dropbox, which is a well-known cloud service provider, should be covered under the SCA.[139]

Essentially, the files in these servers are "papers" in modern electronic communications, leaving cloud storage as an extension of Fourth Amendment protection if one acknowledges the modern-day technological equivalence of physical storage. In fact, the cloud is merely an illusion, as information is stored on a physical server rather than a far-off intangible place, as the name would suggest.[140] The significant difference is that physical limitations found in traditional Fourth Amendment cases with a physical intrusion are no longer commonplace in the digital age. In relation to the third-party doctrine, it remains unclear if cloud data is a business record.[141]

Cloud storage should be an extension of Fourth Amendment protection if one acknowledges the modern-day equivalence of storage. The significant difference is that physical limitations found in traditional Fourth Amendment cases with a physical intrusion are no longer commonplace in the digital age.

---

[138] Shallman, *supra* note 131, at 67.
[139] *Id.* at 50. Dropbox is a remote file-storage application that automatically syncs digital files to its servers upon the user's action.
[140] Wei Chen Lin, *Where Are Your Papers?: The Fourth Amendment, The Stored Communications Act, The Third-Party Doctrine, The Cloud, and Encryption*, 65 DEPAUL L. REV. 1093, 1107 (2016).
[141] *See* Erik C. Shallman, Comment, *Up in the Air: Clarifying Cloud Storage Protections*, 19 INTELL. PROP. L. BULL. 49 (2014).

DISCUSSION OF CURRENT PRIVACY THEORIES

It is imperative the Supreme Court establishes a new precedent for government access to third party records. These theories will only be described insofar as they relate to technology.

A. Reasonable Expectation of Privacy Test

Four decades have passed since Justice Harlan opined the reasonable expectation of privacy test in his *Katz v. United States* concurrence, and the meaning of the phrase is still cloudy. However, it remains the cornerstone of many of the protected privacy rights cases.

The reasonable expectation of privacy test is subjective and outdated. This test assumes that judges can effectively assess what a "reasonable" person would expect; however, there are two issues that arise from this test. First, by assuming a judge can discern what a reasonable person might feel about a specific type of technology, we also assume that the judge is up to date on all of the technologies many people use on a daily basis. Additionally, it does not leave room for reasonable individuals to have a differing opinion on what they see as, in this case, a reasonable intrusion of privacy. Put simply, in a society that normalizes comprehensive surveillance, how "reasonable" are the average people, and who is the society? Does the average person's opinion come from the majority of people through a poll or survey? If so, this binds the minority thinkers to the preferences of the majority, thus ignoring the goal of the Bill of Rights in the Constitution of limiting the will of the majority.[142] The second issue is the outdated context of the test. It requires judges to consider new technology and then create policy based on how they perceive Americans might understand the latest technology and how the technology in question works.

[142] SOLOVE, *supra* note 31, at 117.

As it is currently understood, the expectation of privacy test is often the dominant theory cited when questioning Fourth Amendment protections.

B. Property/Trespass Theory

Physical intrusions, regardless of how major or minor the interference, can generate a Fourth Amendment violation under the trespass theory.[143] "The property-based approach emphasizes the historical reverence of property rights in the colonial era leading up to the American Revolution."[144] This approach was frequently used up until the 1960s before the *Katz* balancing test replaced it, and it required individuals to prove that the government had physically trespassed into their property before Fourth Amendment relief could be considered.[145]

In 2012, *Jones v. United States* dusted off the old trespass doctrine when the court decided that a GPS attachment to a car used to monitor the vehicle's movement was a physical trespass.[146] In writing for the majority, Justice Scalia stressed the physical aspect of the search, reasoning that the Government had intruded on the defendant's privacy when they "inserted [an] information gathering device."[147] However, the majority did not disturb the long-held privacy formulation defined in *Katz*, signaling an era in which Fourth Amendment protections were subjective based on the type of trespass that occurred. .[148] Justice Scalia most likely chose the property approach over the

[143] *See* United States v. Jones, 565 U.S. 400 at 402 (2012) (holding that placement of the GPS device without any other intrusion was a search).
[144] Bishop, *supra* note 100, at 673.
[145] Brady, *supra* note 18, at 949. *See also* Katz v. United States, 389 U.S. 347, 352-53 (1967) (rejecting the notion that physical penetration into a protected area is required to show a Fourth Amendment search).
[146] *Jones*, 565 U.S. at 405, 410.
[147] *Id.* at 410.
[148] *Id.* at 411.

reasonable expectation of privacy test established in *Katz* because it was more straight-forward than the *Katz* test.

C. Mosaic Theory

Privacy activist Orin Kerr explains the Mosaic Theory as an "aggregated set of data acquisitions," noting that a set of non-searches can amount to a search because the collection of the data and following analysis creates a revealing mosaic of a person's private life.[149] It is the aggregation of these movements, regardless of whether the movements occurred in the public view, that is worthy of protection. A mosaic search might bring together locations and timeframes that illustrate a comprehensive picture of a suspect's life. The main issue with the Mosaic Theory that draws a parallel to the issues with the current reasonable expectation of privacy is the subjective nature of a violation. The quality of the mosaic will be different for each person, especially when considering the different kinds of surveillance tools, which then raises its own reasonableness concerns.[150] Courts will then be forced to determine a framework for deciding how much information, or what kind of information can be gathered before it is a "search."

D. Positive Law Theory

When courts apply the positive law model, they are considering whether there is a law (or statute, rule, code), other than the Fourth Amendment, that restricts the government's invasion.[151] Positive law questions whether a search or seizure occurs by determining whether a private party could lawfully conduct the action the government engaged in.[152] Accordingly, instead of the court being concerned about a "reasonable search," the court would ask whether in completing the search

[149] *Id.* at 321.
[150] *Id.* at 329.
[151] Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 516 (2007).
[152] Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. F. 313, 314 (2016).

if the government official violated "general applicable law or avail themselves of a governmental exemption from it."[153]

Positive law may be problematic when new technologies arise because the cornerstone of this theory relies on existing law. The rate at which technology changes and adapts will make it nearly impossible for legislators to keep up with regulating emerging technologies, and even if they try, a backlog may result due to ever-changing technology. It is also possible that some kinds of technology are so obscure that any sort of law regulating its use would be ill-advised.[154] Another roadblock keeping this theory from becoming a guiding precedent is technologies that only the government has access to. It could be possible for lawmakers to tweak the laws to allow private properties access to the technology to avoid Fourth Amendment scrutiny, fully knowing the private party will never have access to the device.[155]

E. Equilibrium-Adjustment Theory

Equilibrium-Adjustment Theory is defined by privacy scholar Orin Kerr as the idea that the courts adjust "legal rules to restore the preexisting balance of police power."[156] Under this theory, if a case arises, the judge would adjust the level of protection for new technology to maintain this balance of power.[157] Kerr argues that the courts should decide this protection to restore a time in

---

[153] William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1826 (2016).
[154] *See Kyllo v. United States* where the Court held that if the government used a device to complete a search that is not available to the general public, the search is unreasonable and requires a warrant. Kyllo v. United States, 533 U.S. 27, 36 (2001). Although you may now buy the device used in question in *Kyllo*, it is not hard to convey this same holding to other devices not yet available to the public.
[155] Baude, *supra* note 153, at 326.
[156] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 482 (2011).
[157] *Id.* at 501.

which he calls "Year Zero."[158] Year Zero is a fictional time that is used as a basis to discern how the "introduction of new tools poses a constant challenge to any legal system that seeks to regulate police investigations."[159]

It considers the dynamic nature of technology and social change,[160]and realizes that new tools and attitudes threaten the security and privacy balance between criminals and police because they allow both sides to "accomplish tasks they could not before" or do those tasks "more easily and cheaper than before."[161] The police should not have so much power that they infringe on an individual's civil liberties, but they also must be powerful enough to enforce the law.[162] This theory is more about maintaining the status quo of power, rather than an effort to restore the Amendment to the Founder's original intent.

This theory exacerbates the Fourth Amendment privacy judicial delay problem that the courts already face. Kerr argues this delay would be encouraged to ensure the courts do not make decisions too soon about technology.[163] However, this delay would only complicate decisions due to the difficult to predict and progressive nature of IoT. This theory also requires judges to project their opinion on various technology cases.

---

[158] *Id.* at 483.
[159] *Id.*
[160] *Id.* at 485.
[161] *Id.* at 486.
[162] *Id.* at 526.
[163] *Id.* at 539.

THIRD-PARTY DOCTRINE AFTER CARPENTER

Carpenter could have been used for fundamental change to the third-party doctrine, but due to the narrow ruling in the case, concerns and questions about what kinds of digital data and how much data the government may access without a warrant will likely continue to arise in lower courts and possibly become future certiorari petitions. *Carpenter* does, however, provide a roadmap for future decisions as it disfavored the government's ability to claim, "a significant extension of [the third-party doctrine] to a distinct category of information."[164] The Court acknowledged that in order to live in modern society, the use of smart technologies is always encouraged and sometimes required.

The online vendor where I occasionally order products analyzes my buying preferences to suggest future, related purchases. There is an electronic trail of when I send emails and to whom they are sent. My favorite search engine collects my inquiries and stores them in case I need to revisit an old search. The news application on my phone filters stories and suggests new ones based on what I have been interested in in the past. I can monitor my home security cameras from my cell phone and lock the doors and windows to my house from my smartphone.

Professor Daniel Solove, an expert in the privacy field, considered the third-party doctrine to be "one of the most serious threats to privacy in the digital age."[165] The abandonment of the third-party doctrine should be favored and replaced with an approach that is neutral regardless of the type of technology to eliminate uncertainty and confusion over whether society has a reasonable expectation of privacy in the presence of certain technologies. In theory, a new approach should also

[164] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).
[165] Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L REV 747, 753 (2005).

allow the market to create new technologies and help them to fully understand the privacy implications of the devices they purchase so they can make an informed decision about their use of the device. A new theory should also preclude the need to prosecute the privacy concerns over every new application or device or company that maintains records about us.

As Justice Gorsuch explained in his dissent in *Carpenter*, the third-party doctrine is woefully incapable of reconciling Fourth Amendment protections in the modern age, stating "[e]ven our most private documents--those that, in other eras, we would have locked safely in a desk drawer or destroyed--now reside on third-party servers."[166]

The third-party doctrine should not apply because much of the information forfeited by individuals is completed on behalf of their devices. To waive Fourth Amendment protections, the information given to a third-party must be voluntary on the part of the individual. However, many device users do not voluntarily give up information; rather, when the devices are powered on, information is sent on behalf of the individual to third parties. No voluntary action triggers this collection, and warrantless government searches conducted on the authority of the third-party doctrine should be unconstitutional. Because this is like the reasoning in *Carpenter*, this data collection should be given the same protections as CSLI.[167]

It is estimated that by 2025, 55 billion IoT devices will be in use, up from 9 billion in 2017.[168] This rapid expansion highlights the importance of establishing protection for data held by third parties, rather than just protecting CSLI.

---

[166] *Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J, dissenting).
[167] *See supra* note 76 and accompanying text.
[168] Peter Newman, *IoT Report: How Internet of Things technology growth is reaching mainstream companies and consumers*, BUSINESS INSIDER (Jan. 28, 2019), https://www.businessinsider.com/internet-of-things-report.

REVISITING THE FOURTH AMENDMENT IN THE DIGITAL AGE

A comprehensive awareness of the text and history of the Fourth Amendment and an understanding of modern technology is required for deciding privacy cases in the digital age. The understanding of what areas are constitutionally protected has grown to reflect changes in society and technology, with even originalist, conservative judges willing to expand protections to cover modern technologies.[169] In his dissenting opinion in *Carpenter*, Judge Gorsuch explained the importance of preserving the privacy that was intended since the adoption of the Fourth Amendment, further stating that the Fourth Amendment must protect "specific rights known at the founding" and also their "modern analogues."[170]

The modern definitions of "papers" and "effects" are very complex compared to what the Framers had at the time of the Fourth Amendment. However, through the jurisprudence of the Fourth Amendment, they essentially provide the same purpose; emails are modern letters[171] , and computers are like file cabinets.[172] The computers and software that store our digital footprint hold enormous amounts of data that could equal the massive amounts of data of the "papers" and "effects" the Founders envisioned. Professor Davies, a well-known privacy scholar, has stated:

> In sum, although the evidence on this point is less than definitive, the available linguistic and statutory evidence suggests that "persons, houses, papers, and effects" was understood to provide clear protection for houses, personal papers, the sorts of domestic and personal items associated with houses, and even commercial products

[169] For example, Justice Scalia recognized in *Kyllo*, "While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development" Kyllo v. United States, 533 U.S. 27, 36 (2001).
[170] Carpenter, 138 S. Ct. at 2271 (Gorsuch, J, dissenting).
[171] *See, e.g.*, United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010).
[172] *See, e.g.*, United States v. Williams, 592 F.3d 511 (4th Cir. 2010) ("At bottom, we conclude that the sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents.").

> or goods that might be stored in houses--while leaving commercial premises and interests otherwise subject to congressional discretion.[173]

The text of the Fourth Amendment expresses the "right to be secure" in one's person, house, papers, and effects; the Framers intended to preserve that liberty against undue infringement, specifically state intrusion, by government officers regardless of inevitable shifting cultural norms. Old-fashioned deposit receipts have been replaced by a digital paper.[174] When cars pass through a toll booth, an electronic record is created that logs the location and time of the passing.[175] All the files the Framers might have had in their desks are now available in digital format located on a computer.[176] Because of the history and purpose of the Fourth Amendment, "papers" should be read as an expressive analog to the more conventional, physical papers. This reading allows us to retain our guaranteed constitutional rights while also recognizing the role of technology and how it has altered the world. It is also necessary for this framework to work along a continuum. Information that is freely shared with others, for example, revealing comments left on public social media pages, deserves little to no protection.[177] Data that the user takes a concerted effort to restrict access to, data that contains deeply revealing information, or data that would typically be covered under the Fourth Amendment should be protected. This is due to the large amount of information that is held by third parties that if shared, would threaten to expose some of our innermost thoughts

---

[173] Davies, *supra* note 14 at 714. Various courts have interpreted Fourth Amendment "effects" to cover personal property, possessions, or objects.
[174] Ferguson, *supra* note 120, at 598.
[175] *Id.*
[176] *Id.* at 598-99.
[177] Most data collected by smart devices will not be in "plain view" as it has been commonly understood. However, information that is readily shared with information online through a public forum, with no additional skills or information required to achieve this information, will be an exception to the Fourth Amendment's warrant requirement.

and questions, even bordering on characteristics that one would only share with their private diary or journal.

Under the existing doctrine, a gap exists in how to classify an "effect." The term "effect" has long been understood as an extension to personal property; in fact, the Court has referenced objects such as automobiles[178] and luggage[179] as "effects" throughout its history. Many scholars have suggested a broader reading of "effects" due to the digital age to cover computers, telephones, and other storage devices.[180] There is no reason why "effects" cannot be updated to be consistent with Fourth Amendment principles, as it would include the smart data, as well as signals emanating from the device.

The Internet of Things offers new surveillance possibilities that do not require physical intrusion, resulting in the possibility for increased government surveillance than can reveal daily routines.

The Fourth Amendment was not intended to define privacy, rather like the rest of the Constitution, it is meant to recognize the necessity of limiting the government's power and discretion. Despite new breakouts of technology, it is crucial that the Fourth Amendment is

---

[178] *See* Cady v. Dombrowski, 413 U.S. 433, 439 (1973) ("Although vehicles are 'effects' within the meaning of the Fourth Amendment, 'for the purposes of the Fourth Amendment there is a constitutional difference between houses and cars.'"); United States v. Jones, 565 U.S. 400, 404 (2012).

[179] United States v. Place, 462 U.S. 696, 705-06 (1983); Florida v. Jimeno, 500 U.S. 248, 253 (1991) ("Luggage, handbags, paper bags, and other containers are common repositories for one's papers and effects, and the protection of these items from state intrusion lies at the heart of the Fourth Amendment.").

[180] Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 51 (2013) ("Portable devices like cellphones and flash drives are 'effects' subject to search and seizure like briefcases and backpacks."); Richard Sobel et al., *The Fourth Amendment Beyond* Katz*,* Kyllo *and* Jones*: Reinstating Justifiable Reliance as a More Secure Constitutional Standard for Privacy*, 22 B.U. PUB. INT. L.J. 1, 8 (2013).

reevaluated to provide for traditional privacy limits because with current interpretations, the Fourth Amendment is ineffective against government intervention.

A. Technology or Privacy: Do you have to choose just one?

Often, many people explain away their privacy by stating they have "got nothing to hide," and because they are not doing anything wrong, they need not worry about the government having access to their information.[181] These explanations are known, respectively, as Nothing to Hide and All-or-Nothing.

Nothing to Hide

When discussing data privacy and technology, many people respond with they have nothing to hide. Variations of this argument include:

- If you have nothing to hide, you have nothing to fear.[182]
- "Like I said, I have nothing to hide. The majority of the American people have nothing to hide. And those that have something to hide should be found out, and get what they have coming to them"[183]
- "Do I care if the FBI monitors my phone calls? I have nothing to hide. Neither does 99.99 percent of the population. If the wiretapping stops one of these Sept. 11 incidents, thousands of lives are saved"[184]

The issue with this line of thought is that it assumes everything should be public knowledge because it cannot be used against you. One journalist, in a *Time* Article asserted: "'[T]he more I learned about data-mining, the less concerned I was. Sure, I was surprised that all these companies are actually keeping permanent files on me. But I don't think they will do anything with them that does me any

[181] SOLOVE *supra* note 31, at 21.
[182] Daniel J. Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 748 (2007).
[183] *Id.* at 749 (citing Polls Suggest Americans Approve NSA Monitoring (NPR radio broadcast, May 19, 2006), available at 2006 WLNR 22949347).
[184] *Id.* (citing Joe Schneider, Letter to the Editor, NSA Wiretaps Necessary, ST. PAUL PIONEER PRESS, Aug. 24, 2006, at 11B).

harm," further stating he was not worried because no human being ever reads your files.[185] This line of thinking is dangerous because first, it fails to consider that some information may be perceived by government officials to be a pattern of criminal behavior, thereby giving the government a valid reason to monitor for criminal activity, and second, because these individuals sacrifice the rights of others because they do not care what happens to them.[186] Furthermore, individuals *could* read the files if they choose, and if they were ever implicated in a crime, the government *could* seize the files and easily read about the individual's whereabouts going back possibly decades.[187]

This mindset is overall detrimental, as it assists in the slow erosion of our privacy rights over time.[188] For example, let us say the government begins to record our telephone conversations arbitrarily. The individuals who support the nothing to hide theory may shrug their shoulders and brush the records off as minimal or non-invasive because the telephone conversation recording is not widespread and according to them, may cause at least one crime to be solved. To them, the benefits outweigh the risks. Alternatively, let us say the government begins monitoring some people's credit card statements in hopes of finding suspicious purchases. The individuals have not been flagged for suspicious purchases, rather the decision on whom to monitor is pure chance. They may claim the government does not want to cause harm, which may very well be true, but the release of records may cause inadvertent harm. The more people who have access to records the more of a chance they will be leaked or the wrong person will gain access to the records. At first blush, these two examples may sound incremental, but after a while, the government will have

[185] Witte, *supra* note 128, at 738-39.
[186] SOLOVE, *supra* note 31, at 29.
[187] Witte, *supra* note 128, at 739.
[188] *Id.* at 30.

collected information on each of us. What if the government takes this information and infers criminal activity?

All or Nothing

Privacy and national security need not be mutually exclusive; surrendering privacy does not necessarily make us more secure, but surrendering security does not necessarily equate to an erosion of our Fourth Amendment rights. It is possible to allow government oversight with "a degree of limitation" because the Fourth Amendment works by judicial oversight.[189]

This framework does not account for the nuance of technology. What if I want to use Amazon Alexa to help organize my day, but I do not want it to provide my daily activities to the government freely? Currently, there are no provisions in place that would allow for me to accomplish this, other than not purchasing an Alexa (or other technology), due to the implementation and analysis of the third-party doctrine.

This all or nothing mindset encompasses the third-party doctrine as it relates to technology not considered in *Carpenter*. Concerning CSLI and privacy cases that came before it, the All or Nothing Framework is better classified as Mostly All or Nothing.

[189] SOLOVE, *supra* note 31, at 35.

ALTERNATIVE SOLUTIONS

The Court is likely to address privacy jurisprudence, and new technologies, in the same piece-meal, incremental approach that has plagued old-fashioned common law. The Court has been reluctant to decide more than what stands before it, likely because judges do not feel they are able to fully understand contemporary technology or society's increasing desire to incorporate technology into daily routines. Because this is the same issue that has brought us through *Carpenter*, it is imperative that society encourages private businesses or the legislature to step in and acknowledge our privacy rights. To incentivize companies to participate in safeguarding our privacy, it must be "valued by consumers as a commodity in its own right, much like organic foods have become a valued food type."[190]

Companies should be held liable for the safety in the collection and transfer of data, whether using encryption on behalf of the company or partnerships with the government to encourage transparency. The technology giants, such as Apple and Microsoft, should stand on behalf of their customers against governmental intrusion. We rely on them to protect our interests because the government requests our data from them.

A. Encryption

Encryption is "the process of encoding information such that a key is required to decode it."[191] Encryption helps keep the information secret from anyone who is not intended to have access to it unless they possess a decryption key.[192] Encryption prevents the government, or anyone else,

[190] Friedland, *supra* note 93, at 912.
[191] David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2217 (2009).
[192] Riana Pfefferkorn, *Everything Radiates: Does the Fourth Amendment Regulate Side-Channel Cryptanalysis?*, 49 CONN. L. REV. 1393, 1397 (2017).

from gaining access to personal files and communications. Currently, encryption is used to secure a safe environment for internet commerce as well as institutional commerce, so it is not far off to assume wide deployment of encryption to the public in the future.[193] This type of personal encryption would result in negative consequences for law enforcement, because encryption "makes it impossible, irrespective of warrants, for law enforcement to recover" the previously encrypted information.[194]

One privacy scholar contends that encryption to protect against a cyber-intrusion is analogous to physical locks, bolts, and alarms in a physical intrusion.[195] When encryption is afforded by companies, rather than individual consumers, the companies may provide discretionary access to the government as they have the key to decrypt. For example, WhatsApp offers end-to-end encryption for messages, voice calls, and videos.[196] Nonetheless, it also stores this encryption and makes it available to law enforcement, if required.[197]

In contrast, Apple has shown its unwillingness to support the government, despite its privacy policy.[198] The most notable of these circumstances was when Apple would not create a backdoor for a deceased terrorist, Syed Farook, in San Bernardino, who had encrypted his cellphone.[199] Apple was ordered by a federal magistrate judge to provide a backdoor to the government to allow federal

---

[193] Lin, *supra* note 140, at 1095-96.
[194] *Id.* at 1096.
[195] Couillard, *supra* note 191, at 2225 (citing 1 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 2.6(f), at 721 (4th ed. 2004)).
[196] Pfefferkorn, *supra* note 192, at 1404 (citing Martin Shelton, *Upgrading WhatsApp Security*, Medium (Feb. 6, 2017), https://medium.com/@mshelton/upgrading-whatsapp-security-386c8ce496d3#.ze0z63ifv [https://perma.cc/9BKP-72AM].
[197] *Id.*
[198] *See supra* note 132 and accompanying text.
[199] *Apple Still Doesn't Know How FBI Hacked San Bernardino Terrorist's iPhone Without Their Help*, FOX NEWS CHANNEL (Mar. 30, 2016), https://www.foxnews.com/tech/apple-still-doesnt-know-how-fbi-hacked-san-bernardino-terrorists-iphone-without-their-help

investigators to see whether the terrorist was working alone.[200] Apple denied this request, asserting its commitment to ensuring the privacy of its millions of customers.[201] In the end, the government hacked the terrorist's phone, no longer requiring Apple's assistance.[202] However, this is not to say Apple never hands over our data to the government; in fact, Apple can and does disclose Cloud data to law enforcement.[203] The difference, theoretically, between these two cases is that in the terrorist attack, by providing the backdoor for the terrorist's phone, the government could conceivably hack all iPhone users with the touch of a button, whereas with the Cloud the government must contact Apple in order to receive the information. It may also be possible that the market will provide and encourage individuals to better protect their privacy. As two technology advocates, Gershenfeld and Vasseur conclude:

> By extending cryptography down to the level of individual devices, the owners of those devices would gain a new kind of control over their personal information. Rather than maintaining secrecy as an absolute good, it could be priced based on the value of sharing. Users could set up a firewall to keep private the Internet traffic coming from the things in their homes--or they could share that data with, for example, a utility that gave a discount for their operating their dishwasher only during off-peak hours or a health insurance provider that offered lower rates in return for their making healthier lifestyle choices.[204]

This suggestion allows consumers to choose whether or not they want to participate in the Internet of Things, and it gives them the privacy many individuals desire while also allowing them to stay connected.

---

[200] *Id.*
[201] *Id.*
[202] *Id.*
[203] Pfefferkorn, *supra* note 192, at 1412-13.
[204] Neil Gershenfeld & J. P. Vasseur, *As Objects Go Online: The Promise (and Pitfalls) of the Internet of Things*, FOREIGN AFFAIRS, Mar.-Apr. 2014, http://www.foreignaffairs.com/articles/140745/neil-gershenfeld-and-jp-vasseur/as-objects-go-online.

B. Right to be Forgotten

Many legal scholars have suggested a "right to be forgotten" law, which draws its support and history from European countries.[205] This law is intended to secure private information for private individuals, as it allows individuals to have certain information deleted from search engines or places where internet records are stored.[206] It strives to balance data protection and right of privacy with the public's interest in access to the information. Critics contend that if a similar "right to be forgotten" law is adopted into law by Americans, there would be profound impacts on our First Amendment Constitutional rights of freedom of speech and freedom of the press.[207] They claim it would be antithetical to one of our nation's founding principles, the free flow of information; they claim it amounts to censorship.[208] Secondly, they claim to allow private companies to remove certain information puts corporations in charge of enforcing our privacy rights; they would be the ones in charge of enforcing the balance between free speech and privacy.[209] On the other hand, supporters of a right to be forgotten law in the United States say it will allow individuals to control their personal data. They argue that much of the information online can be used to damage individuals and their future.[210]

Currently, there are laws that cover many aspects of personal privacy in transactions, but they are not as encompassing as the right to be forgotten. For example, there is the Health Insurance

[205] John W. Dowdell, *An American Right to be Forgotten*, 52 TULSA L. REV. 311, 315 (2017).
[206] *Id* at 321.
[207] *Id* at 334.
[208] May Crockett, Comment, *The Internet (Never) Forgets*, 19 SMU SCI. & TECH. L. REV. 151, 174 (2016).
[209] *Id.* at 178.
[210] *Id.* at 174.

Portability Accountability Act and the Electronic Communications Privacy Act.[211] Both of these acts regulate the use of personal information.[212]

C. Congressional Interception

An essential feature in our society is the relationship between humans and the government; specifically, the checks and balances system that has been around since our nation's founding enacted through the founding documents and the nature of our Republic. However, new developments in technology will continue to minimize third-party disclosures as consumers continue to prioritize the convenience given to them by smart technologies against their constitutional rights. Individuals should be more vigilant about what information they disclose. Additionally, companies should be held liable for the safety in the collection and transfer of data, whether through the use of encryption on behalf of the company or partnerships with the government to encourage transparency. Congress has the opportunity to craft legislation, with the Constitution in mind, that is amicable to law enforcement and the public, unlike the courts, which can only rule on cases and laws that come before it.

Consumers could benefit from federal privacy legislation, as this would ensure at least a baseline that all companies would follow.[213] As long as this baseline had consequences for those who do not comply, it would allow for nearly all companies to play by the same rules because the internet and other online devices cross state lines.[214] The legislation should be broad enough to account for

---

[211] *Id.* at 171.
[212] *Id.*
[213] Jack Karston, How Should the US Legislate Privacy?, https://www.brookings.edu/blog/techtank/2018/07/30/how-should-the-us-legislate-data-privacy/
[214] *Id.*

rapidly changing technology, but narrow enough to ensure data security and privacy. If companies wanted to take additional precautions to protect privacy, they should be welcome to do so.

CONCLUSION

The digital transition from physical papers and the well-known concept of "effects" is a dangerous time for our civil liberties. The enumeration of the Fourth Amendment protections reflects the Founders' commitment to the development of thoughts, ideas, and beliefs. It is necessary that we read the Fourth Amendment to apply to all of the digital information, as a functional equivalent to the physical papers and effects that existed during the time of the Founding Fathers if we are to preserve the right to privacy for the future generations. The Founding Fathers could not have ever imagined the progression of technology, but their ideas and the foundation for why the Fourth Amendment protected certain things remains the same.

Jurisprudence regarding privacy from the Supreme Court has been plentiful, but the Court's decisions have focused on the devices rather than focusing on the types of information collected by devices in general. The cornerstone for many of these decisions have been the Fourth Amendment concept of reasonableness, but what is reasonable with electronic data is not consistent. As Smart devices and internet tracking become even more prevalent, there is an urgent need to end the third-party doctrine and also reconsider the outdated nature of the Stored Communications Act. *Carpenter* was a step in the right direction for CSLI, but it does not consider the vast array of technologies and their ways of data collection yet to emerge.

We *must* ensure the rights that were guaranteed by the Constitution at the time of founding is still applicable for digitization, regardless of the new technologies that develop in the IoT. The Constitution may have been written a long time before cellphones and the internet was devised, but the unwavering beliefs of personal autonomy and privacy.

Today, most of our information is stored on third-party servers; if this information can be obtained without a warrant, our Fourth Amendment privacy protections are meaningless. If the third-party doctrine, as it stands, were to be applied to the third-party doctrine and IoT, the government would be provided unlimited access to an individual's personal information as part of a comprehensive IoT profile.

In *Carpenter*, the Court declined to extend the third-party doctrine to the data collected by cell phones, but this narrow interpretation only leaves more questions than it answered. The smart home will soon be as much of a necessity to modern life as cell phones. This questions the very roots of the third party doctrine of voluntary conveyance and assumption of risk, thereby requiring a re-examination of the third-party doctrine.

We must encourage consumers to care about their privacy, and also advocate to private business the importance of privacy. If lawmakers wish to be involved, they should develop a comprehensive, timeless protocol to guide law enforcement in digital searches.

LIST OF LEGAL REFERENCES

18 U.S.C.A. § 2703(a).

19 How. St. Tr. 1029, 95 Eng. Rep. 807 (C.P. 1765).

Carpenter v. United States, 138 S. Ct. 2206 (2018).

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860-68.

Florida v. Jardines, 133 S. Ct. 1409 (2013)

Katz v. United States, 389 U.S. 347 (1967).

Riley v. California, 573 U.S. 373 (2014).

Smith v. Maryland, 442 U.S. 735 (1979).

U.S. CONST. amend. IV.

United States v. Davis, 785 F.3d 498, 536 (11th Cir. 2015).

United States v. Miller, 425 U.S. 435 (1976).

United States v. Jones, 565 U.S. 400 (2012).

LIST OF ADDITIONAL REFERENCES

Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 SUFFOLK U. L. REV. 53 (1996).

Andrew Griffin, *Samsung smart TV policy allows company to listen in on users*, The Independent (Feb. 9, 2015), http://www.independent.co.uk/life-style/gadgets-and-tech/news/samsungs-new-smart-tv-policy-allows-company-to-listen-in-on-users-10033012.html.

Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805 (2016).

Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547 (2017)

Anne Pfeifle, *Alexa, What Should We Do About Privacy? Protecting Privacy for Users of Voice-Activated Devices*, 93 WASH. L. REV. 421 (2018).

Apple Still Doesn't Know How FBI Hacked San Bernardino Terrorist's iPhone Without Their Help, FOX NEWS CHANNEL (Mar. 30, 2016), https://www.foxnews.com/tech/apple-still-doesnt-know-how-fbi-hacked-san-bernardino-terrorists-iphone-without-their-help

Brief for Technology Companies as Amici Curiae in Support of Neither Party at 9, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).

Christopher Mims, *All Ears: Always-On Listening Devices Could Soon Be Everywhere*, Wall Street J. (July 12, 2018, 12:00 PM), https://www.wsj.com/articles/all-ears-always-on-listening-devices-could-soon-be-everywhere-1531411250.

Christopher Slobogin, *Subpeonas and Privacy,* 54 DEPAUL L. REV. 805 (2005).

Craig Timberg, *Hacker Locates John McAfee through Smartphone Tracks*, The Washington Post (Dec. 4, 2012), https://www.washingtonpost.com/business/economy/hacker-locates-john-mcafee-through-smartphone-tracks/2012/12/04/55a498d8-3e4a-11e2-bca3-aadc9b7e29c5_story.html.

Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L REV 747 (2005)

Daniel J. Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007).

DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADE OFF BETWEEN PRIVACY AND SECURITY (2011).

David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205 (2009).

Definition of Voluntary by Merriam-Webster, Merriam Webster (September 24, 2019), http://www.merriam-webster.com/dictionary/voluntary [https://perma.cc/TXS3-A3HP] ("voluntary: done by design or intention: intentional").

Definition - What does *Geotagging* mean?, https://www.techopedia.com/definition/86/geotagging (last visited Nov. 1, 2019).

Denae Kassotis, Note, *The Fourth Amendment and the Technological Exceptionalism After Carpenter: A Case Study on Hash-Value Matching*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1243 (2019).

Derek S. Witte, *Bleeding Data in a Pool of Sharks: The Anathema of Privacy in a World of Digital Sharing and Electronic Discovery*, 64 S.C. L. REV. 717 (2013).

Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49 (2013)

Eliott C. McLaughlin, Suspect OKs Amazon to hand over Echo recordings in murder case, CNN Business (April 26, 2017, 2:52 PM), https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html

Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 VA. L. REV. 869 (1985).

Erik C. Shallman, Comment, *Up in the Air: Clarifying Cloud Storage Protections*, 19 INTELL. PROP. L. BULL. 49 (2014).

FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the H. Subcomm. on Commc'n & Tech. of the H. Comm. on Energy & Commerce, 114th Cong. 5 (2016) (statement of Paul Ohm, Professor, Georgetown University Law Center).

Help Article: How do I get data from my tracker to the website?, fitbit help, http://help.fitbit.com/articles/en_US/Help_article/How-do-I-get-data-from-my-tracker-to-the-website/?l=en_US&fs=RelatedArticle (last updated Aug. 13, 2019).

How Home/Away Assist Uses Your Phone's Location, Nest, https://support.google.com/googlenest/answer/9262475?hl=en (last visited November 1, 2019).

iCloud Terms and Conditions, APPLE, https://www.apple.com/legal/internet-services/icloud/en/terms.html (last revised Sept.19, 2019).

Jack Karston, How Should the US Legislate Privacy?, https://www.brookings.edu/blog/techtank/2018/07/30/how-should-the-us-legislate-data-privacy/

Jason Palmer, *Mobile Location Data 'Present Anonymity Risk,'* BBC News (Mar. 25, 2013) http://www.bbc.co.uk/news/science-environment-21923360.

Jason Tanz, *The CIA Leak Exposes Tech's Vulnerable Future*, Wired (Mar. 8, 2017), https://www.wired.com/2017/03/cia-leak-exposes-techs-vulnerable-future/

Jing Cao & Dina Bass, *Why Google, Microsoft, and Amazon Love the Sound of Your Voice*, BLOOMBERG TECH. (Dec. 13, 2016), https://www.bloomberg.com/news/articles/2016-12-13/why-google-microsoft-and-amazon-love-the-sound-of-your-voice [https://perma.cc/5DW7-ATQ8].

John W. Dowdell, *An American Right to be Forgotten*, 52 TULSA L. REV. 311 (2017).

Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181 (2016).

Leonard W. Levy, Origins of the Bill of Rights (1999).

Margaret Rouse, *Big Data*, Tech Target: AI in IT Tools Promises Better, Faster, Stronger Ops (last visited October 31, 2019), https://searchdatamanagement.techtarget.com/definition/big-data.

Margaret E. Twomey, *Voluntary Disclosure of Information as a Proposed Standard for the Fourth Amendment's Third-Party Doctrine,* 21 MICH. TELECOMM. & TECH. L. REV. 401 (2015).

Mark Wilson, Comment, *Castle in the Cloud: Modernizing Constitutional Protections for Cloud-Stored Data on Mobile Devices*, 43 GOLDEN GATE U. L. REV. 261 (2013)

Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946 (2016).

May Crockett, Comment, *The Internet (Never) Forgets*, 19 SMU SCI. & TECH. L. REV. 151 (2016).

Molly Edwards & Nathan Chandler, HowStuffWorks.com, *How Smart Homes Work*, http://home.howstuffworks.com/smart-home1.htm, (last visited October 25, 2019).

Natasha Lomas, *Samsung Edits Orwellian Clause Out of TV Privacy Policy*, TECH CRUNCH (Feb. 10, 2015), http://techcrunch.com/2015/02/10/smarttv-privacy/#.puzvmzo:yfMB.

Neil Gershenfeld & J. P. Vasseur, *As Objects Go Online: The Promise (and Pitfalls) of the Internet of Things*, FOREIGN AFFAIRS, Mar.-Apr. 2014,

http://www.foreignaffairs.com/articles/140745/neil-gershenfeld-and-jp-vasseur/as-objects-go-online

Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007).

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

Paul Kominers, *Interoperability Case Study, Internet of Things (IoT)*, Berkman Ctr. for Internet & Soc'y (Apr. 16 2012), https://cyber.law.harvard.edu/node/97248 [https://perma.cc/VG3W-4DER].

Peter Newman, *IoT Report: How Internet of Things technology growth is reaching mainstream companies and consumers*, BUSINESS INSIDER (Jan. 28, 2019), https://www.businessinsider.com/internet-of-things-report.

Riana Pfefferkorn, *Everything Radiates: Does the Fourth Amendment Regulate Side-Channel Cryptanalysis?*, 49 CONN. L. REV. 1393 (2017).

Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. F. 313 (2016).

RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE (2014).

Ryan G. Bishop, Note, *The Walls Have Ears, And Eyes, And Noses: Home Smart Devices and the Fourth Amendment*, 61 ARIZ. L. REV. 667 (2019).

Samsung Privacy Policy--SmartTV Supplement, Samsung, http://www.samsung.com/sg/info/privacy/smarttv.html (last visited Oct. 22, 2019).

Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

Steven I. Friedland, *Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things is Changing the Face of Privacy*, 119 W. VA. L. REV. 891 (2017).

Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547 (1999).

Trevor Timm, *The Government Just Admitted it Will Use Smart Home Devices for Spying*, The Guardian (February 9, 2016), https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government/

V. Alexander Monteith, *Cell Site Location Information: A Catalyst for Change in Fourth Amendment Jurisprudence*, 27-FALL KAN. J.L. & PUB. POL'Y 82 (2017).

Wei Chen Lin, *Where Are Your Papers?: The Fourth Amendment, The Stored Communications Act, The Third-Party Doctrine, The Cloud, and Encryption*, 65 DEPAUL L. REV. 1093 (2016).

William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821 (2016).