An Analogue Precedent in a Digital World: Exploring the Applicability of the Third-Party Doctrine in the Modern Technology Era

Nathaniel L. Siegler
Trinity College, Hartford Connecticut, nsiegler@trincoll.edu

Follow this and additional works at: https://digitalrepository.trincoll.edu/theses
Part of the Law Commons, Political Science Commons, and the Public Affairs, Public Policy and Public Administration Commons

Recommended Citation
Trinity College Digital Repository, https://digitalrepository.trincoll.edu/theses/733
An Analogue Precedent in a Digital World: 
Exploring the Applicability of the Third-Party Doctrine in the 
Modern Technology Era

By

Nathaniel L. Siegler

A thesis submitted in partial fulfillment of the requirements for the Degree of Bachelor of Arts 
with Honors in Public Policy and Law

TRINITY COLLEGE

Hartford, Connecticut

Fall 2017-Spring 2018
Acknowledgments

This thesis is dedicated to my parents. No two individuals have influenced me and made me who I am today more than them. Their love and support can neither be measured nor quantified, but it is exemplified and personified by the product of these pages, and by every decision I will make in life going forward. They have taught me the value of working hard and the importance of family. They have never put me down, they have only lifted me up, they have been strict but fair, and above all else they have been the greatest parents any child could ever have. These words in this acknowledgment and in this thesis are the culmination of the year’s sacrifice, hard work, and love of my parents: I could not have done it without you.

Next I must thank Professor Fulco. She has spent hours from September till mid-May helping me craft this question, guide my research, and better my writing. Whether it was an email with a small stylistic question at 10:00PM on a Wednesday, or it was a scheduled hour long meeting in her office to go over her corrections on a draft of a chapter Professor Fulco has been my guiding light during this process. She always told me that there was a light at the end of the tunnel, and although I could not always see it, her tireless effort and endless help on this thesis is the only reason I can finally see that light. She has been my advisor since sophomore year, and I could not have had the success and academic fulfillment that I did during my time at Trinity without her. This small paragraph in no way could ever encapsulate the thanks and gratitude that she deserves for all of her hard work and continuous effort to push me to be a better student and write this thesis.
# Table of Contents

**Title Page** .................................................................................................................. 1
**Acknowledgements** ...................................................................................................... 2
**Table of Contents** .......................................................................................................... 3

## Chapter 1: The Evolution of Privacy ............................................................................. 5

I. Origins of the Right to Privacy ....................................................................................... 5
II. The Physical Trespass Doctrine ................................................................................... 7
III. Reasonable Expectation of Privacy ............................................................................. 9
IV. The Creation of the Third-Party Doctrine ................................................................. 11
V. Objections to the Third-Party Doctrine .................................................................... 14
VI. Legal Scholars’ Support to the Third-Party Doctrine ................................................ 16
VII. Legal Scholars’ Objections to the Third-Party Doctrine .......................................... 22
VIII. A World Without Privacy ....................................................................................... 25
IX. Modern Legal Applicability of the Third-Party Doctrine ......................................... 27

## Chapter 2: The Fourth Amendment and Modern Technology ..................................... 29

I. *Kyllo v. United States* ................................................................................................. 29
II. *United States v. Jones* .............................................................................................. 31
III. Judicial or Legislative Solution .................................................................................. 33
IV. *Riley v. California* .................................................................................................. 37
V. *Carpenter v. United States* ........................................................................................ 41
   A. Petitioner’s Brief in *Carpenter v. United States* ..................................................... 42
      1. Carpenter Has a Reasonable Expectation of Privacy ......................................... 43
      2. The Analogue Third-Party Doctrine is not Applicable in the Digital Era ........... 45
      3. CSLI Data is Considered the “Papers” of the Cellular Customer ....................... 46
   B. Brief for the Respondent ......................................................................................... 47
VI. Are the Courts the Correct Branch to Resolve this Issue? ....................................... 51

## Chapter 3: Legislation and the Third-Party Doctrine ................................................ 52

I. History of Congressional Electronic Privacy Statutes .................................................. 53
   A. Title I of the ECPA .................................................................................................. 55
   B. Title II of the ECPA ............................................................................................... 55
   C. Title III of the ECPA ............................................................................................. 57
II. Statutory Response to *Smith* and *Miller* ............................................................... 57
III. Additional Statutory Exceptions to the Third-Party Doctrine .................................. 59
IV. Telecommunications Act of 1996 .............................................................................. 60
V. Legal Scholars’ Support for a Legislative Solution .................................................... 63
VI. Legal Scholars’ Support for a Judicial Solution ....................................................... 67
VII. Additional Arguments for a Judicial Solution ........................................................... 68
Chapter 4: Carpenter Oral Argument Analysis and Opinion Predictions

I. Carpenter Oral Argument Analysis. ................................................................. 71
   A. Justice Neil Gorsuch.................................................................................. 72
   B. Justice Clarence Thomas......................................................................... 77
   C. Justice Elena Kagan................................................................................ 77
   D. Justice Sonia Sotomayor.......................................................................... 80
   E. Chief Justice John G. Roberts Jr.............................................................. 82
   F. Justice Stephen Breyer............................................................................. 84
   G. Justice Ruth Bader Ginsburg................................................................... 86
   H. Justice Samuel Alito Jr. .......................................................................... 87
   I. Justice Anthony Kennedy......................................................................... 89

II. “This is an Open Box. We Know Not Where We Go”.................................. 91
III. Expansive and Sweeping Privacy Decision v. Narrow and Cautious Decision..... 93
IV. Conclusion.................................................................................................. 99

Work Cited........................................................................................................ 103
Chapter 1: The Evolution of Privacy

It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is.¹

The Fourth Amendment of the United States Constitution states, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”² The Amendment’s original purpose was to protect the citizens of the new American republic from a replication of the abuses perpetrated by the British during the Colonial period. “The founding generation sought to cabin the new government’s authority to engage in searches and seizures and to limit the possibilities for abuses.”³

I. Origins of the Right to Privacy

From the early years of the republic through the Civil War, the Fourth Amendment achieved its goal of protecting citizens from physical unwarranted intrusions into their persons, houses, papers, and effects. However, in 1890, Samuel Warren and future Supreme Court Justice Louise Brandeis wrote what some consider to be the most influential law review article ever published: “The Right to Privacy.” When the article was published, the ideas of a penumbra of rights containing a right to privacy, or an expectation of privacy were not ones that had been considered in constitutional jurisprudence, let alone Fourth Amendment jurisprudence.

Warren and Brandeis’ article arose out of their recognition that certain conversations and topics that once were understood to be private in nature had become the staple of America’s ever-growing desire for gossip and tabloid media. “The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery.”

The invasion by the late nineteenth-century tabloids and newspapers into the previously private life of individuals dictated that there must be protections put in place to allow the people to exercise their “Right to be let alone.”

Brandeis and Warren realized that societal changes, society’s needs, and society’s expectations regarding privacy illustrated that the law must change and adapt to the times, and to society, not the other way around.

The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual.

The Brandeis and Warren article lay the foundation for the establishment of the right to privacy by demanding that law evolve along with the requirements and expectations of society:

Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society … Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term ‘property’ has grown to comprise every form of possession—intangible, as well as tangible.

The article describes people’s inherent right to privacy, and argues that the courts must address whether this right to privacy is one that the law is ready to recognize. “The question whether our

---

4 Warren and Brandeis, 196.  
5 Warren and Brandeis, 195.  
6 Warren and Brandeis, 195.  
7 Warren and Brandeis, 193.
law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration.”

II. The Physical Trespass Doctrine

The Supreme Court’s first major case in the nearly one hundred-year struggle over the right to privacy came in the 1928 case *Olmstead v. United States*. *Olmstead* involved bootleggers during prohibition who were convicted of “[u]nlawfully possessing, transporting, and importing intoxicating liquors and maintaining nuisances, and by selling intoxicating liquors.” Mr. Olmstead was the leader of the conspiracy, which involved eleven other men. Law enforcement intercepted communications between Mr. Olmstead and the other conspirators by having “[s]mall wires [that] were inserted along the ordinary telephone wires from the residences of four of the petitioners and those leading from the chief office.” The placement of these small wires, which were intended to overhear and intercept the messages of the conspirators, was done without a warrant, and the petitioners argued that the Prohibition officers wiretapping their conversations without a warrant had violated their right to privacy and their Fourth Amendment rights.

The Supreme Court jurisprudence at the time of *Olmstead* followed the long-established common law precedent that the only manner by which the government could violate the Fourth Amendment, in regards to searches, was by physically trespassing onto the property or into the home of the accused without a warrant. This common law doctrine was the main legal philosophy questioned in the Brandeis and Warren article. Did the law only protect people against physical invasion of their property? “The common law has always recognized a man's

---

8 Warren and Brandeis, 195.
10 *Id. at* 456-457.
house as his castle, impregnable, often, even to his own officers engaged in the execution of its command.” Alternatively, would the Court stop unwanted invasions of privacy even when a physical trespass had not occurred? Or as Brandeis and Warren noted, “Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?”

In *Olmstead*, the Court did not heed the warning of Brandeis and Warren regarding the capabilities of law enforcement becoming more advanced with each day.

The narrower [physical trespass] doctrine may have satisfied the demands of society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or a special confidence; but now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation.

Instead, ignoring this admonishment, the Court in *Olmstead* relied on the physical trespass doctrine of the Fourth Amendment. “The insertions were made without trespass upon any property of the defendants,” and as a result the Court decided,

Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house ‘or curtilage’ for the purpose of making a seizure. We think, therefore, that the wiretapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.

By the time the Court decided *Olmstead*, Brandeis was a Justice on the Supreme Court, and he reiterated the point he had made nearly forty years earlier in his law review article. He wrote in his *Olmstead* dissent that the physical trespass doctrine was a dangerous and outdated Fourth Amendment standard. He warned that both the days of required physical trespass by law

---

11 Warren and Brandeis, 220.
12 Warren and Brandeis, 220.
13 Warren and Brandeis, 210-211.
15 *Id.* at 466.
enforcement in order to obtain evidence, and the days of the physical trespass doctrine being sufficient protection for citizens were coming to a rapid end. In *Olmstead*, a law enforcement officer now possessed the technology to avoid a physical trespass or presence to overhear the planning of criminal activity, and instead could attach a few wires and overhear an entire criminal organization or any citizen of their choosing.

‘Time works changes, brings into existence new conditions and purposes.’ Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. Moreover, ‘in the application of a constitution, our contemplation cannot be only of what has, been but of what may be.’ The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. ‘That places the liberty of every man in the hands of every petty officer’ was said by James Otis of much lesser intrusions than these. To Lord Camden, a far slighter intrusion seemed ‘subversive of all the comforts of society.’ Can it be that the Constitution affords no protection against such invasions of individual security?16

It would not be until thirty-nine years later that the Court would begin to heed Brandeis’ warning from *Olmstead*, and his famous law review article.

**III. Reasonable Expectation of Privacy**

In 1967, the Supreme Court in *Katz v. United States*, forever changed Fourth Amendment jurisprudence. The case articulated a new standard for examining potential Fourth Amendment violations by the Government. The new test was meant not only to replace the strict physical trespass doctrine that the Court had used in *Olmstead* and in all other prior cases, but also to give new protections in a world of constant technological change and innovation. In *Katz* the Court realized that people needed greater protections from government intrusions, just as Brandeis had

---

16 *Id.* at 473-474, (Brandeis, J., dissenting).
warned in *Olmstead*. The case involved Charles Katz, who was charged with running an illegal gambling operation and was caught by FBI agents who “[a]ttached an electronic listening and recording device to the outside of the telephone booth from which calls were made.” Justice Stewart wrote the opinion for the Court, in which he brought the right of privacy into the discussion of the Fourth Amendment protections. His opinion discussed how technological changes, such as the telephone booth, became so vital to private communication and to society in general, that constitutional protections were required to adequately guard citizens against the prying ears of the government.

But what he sought to exclude when he entered the booth was not the intruding eye -- it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

Justice Stewart wrote, not only that there was a right to privacy from the “uninvited ear” when Katz closed the telephone booth door, but also that the days where the government could claim, that the absence of a physical trespass prevented a violation of Katz’s Fourth Amendment right, were over. “Thus, although a closely divided Court supposed in *Olmstead* that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested.”

The new scope of Fourth Amendment protections was embodied by the new standard articulated in Justice John Marshall Harlan II’s concurrence. “My understanding of the rule that

---

18 *Id.* at 352.
19 *Id.* at 353.
has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”\textsuperscript{20} This test was applied to the facts of \textit{Katz}:

The critical fact in this case is that ‘[o]ne who occupies it [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume’ that his conversation is not being intercepted. The point is not that the booth is ‘accessible to the public’ at other times, but that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable … That case established that interception of conversations reasonably intended to be private could constitute a ‘search and seizure.’ and that the examination or taking of physical property was not required.\textsuperscript{21}

The new two-prong standard of exhibiting an actual expectation of privacy, one that society is ready to recognize as reasonable, became the guiding Fourth Amendment test. The test has been applied to numerous cases, including those that involve the highly controversial third-party doctrine of the Fourth Amendment.

\textbf{IV. The Creation of the Third-Party Doctrine}

The third-party doctrine in constitutional law was conceived in the 1976 decision \textit{United States v. Miller}, a case that involved a man who was distilling and selling un-taxed whiskey. The police obtained copies of his bank records without a warrant. Miller argued that this violated his subjective expectation to privacy in his private financial transactions with the bank, and that this privacy expectation was one that society was ready to accept as reasonable. In \textit{Miller} the Court distinguished between a person’s private papers, which have robust Fourth Amendment protections, and papers used in a commercial transaction. “On their face, the documents… are not respondent’s ‘private papers.’ … Respondent can assert neither ownership nor possession.

\textsuperscript{20} \textit{Id.} at 361, (Harlan, J., concurring).
\textsuperscript{21} \textit{Id.} at 361, (Harlan, J., concurring).
Instead, these are the business records of the banks.”\textsuperscript{22} Miller argued that he “[h]as a Fourth Amendment interest in the records kept by the banks because they are merely copies of personal records that were made available to the banks for a limited purpose and in which he has a reasonable expectation of privacy.”\textsuperscript{23} This is where the Court first introduces the third-party doctrine, opening the door to the controversy that both Congress and the Supreme Court are still dealing with today.

We perceive no legitimate "expectation of privacy" in their contents. The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business … The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.\textsuperscript{24}

Simply stated, the third-party doctrine provides that when an individual disseminates information to a third party, he no longer has a reasonable expectation to privacy in that information, and, therefore, the individual loses all Fourth Amendment protection over this information. And as a critical corollary, the government no longer needs a warrant to obtain this information. Three years later, the Supreme Court in \textit{Smith v. Maryland}, would solidify the third-party doctrine’s place in constitutional jurisprudence; however, \textit{Smith} would also highlight the flaws of the third-party doctrine that continue in the modern-day interconnected and globalized world.

Decided in 1979, \textit{Smith v. Maryland} reinforced the view that information disseminated to a third party by an individual no longer satisfied the two-pronged test from \textit{Katz}. The question for

\textsuperscript{23} \textit{Id.} at 442.
\textsuperscript{24} \textit{Id.} at 442-443.
the Court to consider in *Smith* was, “Whether the installation and use of a pen register constitutes a ‘search’ within the meaning of the Fourth Amendment.”

This case again revolved around an individual disseminating information to a company in order to conduct a necessary function in society. Instead of conducting transactions with a bank, as in *Miller*, this time it was providing numbers to the telephone company in order to be able to call other people. Just as in *Miller*, the petitioner claimed that he had a subjective expectation of privacy that society was ready to accept as reasonable in the numbers that one dialed from one’s phone.

The Court’s opinion, written by Justice Blackmun, flat out rejects this argument, with a strong dismissal of the notion that people appropriately believe they have a real expectation to privacy in the telephone numbers that they dial.

This claim must be rejected. First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the telephone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.

Justice Blackmun reinforced the use of the third-party doctrine to dismiss the petitioner’s claims. His opinion argued that even if the Court did accept that Smith had a subjective expectation of privacy in the numbers dialed, his Fourth Amendment protection claim would still fall short of satisfying the second prong of the *Katz* test, because it is not an expectation of privacy that society is ready to accept as reasonable.

Even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not "one that society is prepared to recognize as `reasonable.'” This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.

---

27 *Id.* at 742.
28 *Id.* at 743-744.
This absolute rejection of any expectation of privacy in information voluntarily handed over to third parties, in this case phone numbers dialed, was not a unanimously held view of the *Miller* Court, nor is it a view held by all Fourth Amendment scholars, past or present.

**V. Objections to the Third-Party Doctrine**

The dissent, written by Justice Marshall, highlights many of the issues with the majority’s opinion, and the precedent it sets, not only in 1979, but also in its application to modern society, modern technology, and the modern workplace. Justice Marshall did not simply believe that because one gives up information to a business or any another third party for a specific purpose, such as conducting a bank transaction or making a phone call, that one forfeits all Fourth Amendment protections. “Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.”

His dissent explains how the “assumption of risk,” by which “[i]ndividuals who convey information to third parties have ‘assumed the risk,’ of disclosure to the government,” is “[m]isconceived in two critical areas.” First Marshall believes that the majority was misguided and incorrect in holding that, “Unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of ‘assuming’ risks in contexts where, as a practical matter, individuals have no realistic alternative.” The use of a telephone, or conducting transactions at a bank, is an indispensable and unavoidable practice of modern life. Every time an individual engages in one of these

---

29 *Id.* at 749 (Marshall, J., dissenting).
30 *Id.* at 749 (Marshall, J., dissenting).
31 *Id.* at 749 (Marshall, J., dissenting).
32 *Id.* at 750 (Marshall, J., dissenting).
practices they assume the risk of being surveyed by the government, no matter how necessary they are to function as a working contributing member of society.

Justice Marshall’s second objection to the majority opinion’s logic is that the Court expanded the new ability of the government to discern and interpret the scope of the Fourth Amendment and its protections for citizens in certain situations. In the majority opinion, the Court understands the new immense power it has bestowed upon the government. However, it failed to explain under what circumstances the Court would be able to, or be required to, step in and question the justification claimed by the government in any particular case about the expansion or contraction of police power under the Fourth Amendment.

More fundamentally, to make risk analysis dispositive in assessing the reasonableness of privacy expectations would allow the government to define the scope of Fourth Amendment protections. For example, law enforcement officials, simply by announcing their intent to monitor the content of random samples of first-class mail or private phone conversations, could put the public on notice of the risks they would thereafter assume in such communications. Although acknowledging this implication of its analysis, the Court is willing to concede only that, in some circumstances, a further ‘normative inquiry would be proper.’ No meaningful effort is made to explain what those circumstances might be, or why this case is not among them.

Justice Marshall believes that a subjective expectation of privacy exists, and that it is one that society is ready to recognize as legitimate even if the individual has disseminated information to a third party. This is especially true if the information being disseminated is required for the individual to be an active and positive contributor to modern society, or if the information must be given to a third party to conduct their normal daily life. Marshall, in his dissent, argues that he believes the judiciary must decide on a case-by-case basis whether an individual has a subjective expectation to privacy that society is ready to recognize as reasonable with respect to the specific information provided to a third party.

---

33 Id. at 750 (Marshall, J., dissenting).
In my view, whether privacy expectations are legitimate within the meaning of Katz depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society. By its terms, the constitutional prohibition of unreasonable searches and seizures assigns to the judiciary some prescriptive responsibility … courts must evaluate the “intrinsic character” of investigative practices with reference to the basic values underlying the Fourth Amendment. And for those “extensive intrusions that significantly jeopardize [individuals’] sense of security … more than self-restraint by law enforcement officials is required.”

The third-party doctrine presents one of the most complex and important challenges facing the Supreme Court. Given the momentous changes in surveillance and data collection technology since the time of Olmstead, Katz, Miller, and Smith, the Court is now faced with the challenging task of determining which of these controversial precedents is still valid in our technologically connected and globalized modern world. The Court is not alone in this task, and many scholars have attempted to articulate how the third-party doctrine should be applied, if at all, by the courts or by the Congress. What follows is a brief description of the most influential theories regarding the role of third-party doctrine interpretations of Fourth Amendment protections today.

VI. Legal Scholars’ Support for the Third-Party Doctrine

In his article, “The Case for the Third-Party Doctrine,” legal scholar Orin Kerr recognizes the importance of technology in society, and the increasing role of the third-party doctrine currently and in the future. He says, “The topic is a timely one: Technological progress places more and more communications in the hands of third parties, and the growing importance of new technologies such as the internet has led to a renewal of the attacks on the third-party doctrine.”

Kerr is one of the leading legal scholars on the Fourth Amendment, and he is one of the few legal scholars who supports the principles of the third-party doctrine. He believes that, while it is not

---

34 Id. at 750-751 (Marshall, J., dissenting).
perfect, it remains solid law that should continue to evolve symbiotically with technological
advances. He acknowledges that the pro-third-party doctrine position is not popular with legal
scholars or with some state judges, who have strong and vehement opposition to the doctrine.

He argues,

The third-party doctrine is the Fourth Amendment rule scholars love to hate. It is the *Lochner*
of search and seizure law, widely criticized as profoundly misguided. Decisions applying the
doctrine ‘top the chart of [the] most-criticized fourth amendment cases. Wayne LaFave
asserts in his influential treatise that the Court's decisions applying it are ‘dead wrong’ and
‘make a mockery of the Fourth Amendment.’ The verdict among commentators has been
frequent and apparently unanimous: The third-party doctrine is not only wrong, but horribly
wrong.’ Even many state court judges have agreed. Over a dozen state Supreme Courts have
rejected the doctrine under parallel provisions of their state constitutions.36

Kerr understands he is arguing against the majority of scholars and even against some
members of the judicial branch, but his arguments present important and often overlooked
aspects of the third-party doctrine. These overlooked areas, Kerr believes, are crucial not only to
demonstrate the value of the third-party doctrine, but also to show the critical need for the third-
party doctrine during the current technologically driven and evolving era. Kerr identifies two
main reasons why he supports the third-party doctrine:

The first and most important purpose is to maintain the technological neutrality of Fourth
Amendment rules. Use of third parties has a substitution effect: It takes open and public
portions of crimes and hides them from public observation. Without the third-party doc-
trine, savvy wrongdoers could use third-party services in a tactical way to enshroud the
entirety of their crimes in zones of Fourth Amendment protection. The result would allow
technology to upset the Fourth Amendment's traditional balance between privacy and
security, weakening the deterrent and retributive goals of criminal punishment. The third-
party doctrine blocks this end-run around the traditional Fourth Amendment balance.37

According to Kerr, the third-party doctrine produces a precarious balancing act between
citizen’s privacy and the power of law enforcement, which has been and will continue to be
under great scrutiny as technology becomes more advanced and integrated into everyday life.

Kerr argues that this critical balance is achieved, during these times, thanks to the third-party doctrine’s ability to render technology as a neutral weapon for both law enforcement and criminals. Kerr continues by asserting that without the third-party doctrine being properly utilized by law enforcement, criminals would be able to use technology to skirt around the law, resulting in the inadmissibility of evidence against the accused, or law enforcement’s inability to acquire the evidence in the first place. It would upset the delicate balance between individual freedom and protection from unreasonable and unwarranted government intrusions, and giving law enforcement the tools and power necessary and to effectively gather evidence and convict criminals in a technology-driven society.

The second reason Kerr supports the application of the third-party doctrine is because it provides a bright line distinguishing what tools law enforcement may legally use. He argues, [t]o foster ex ante clarity in Fourth Amendment rules. The on/off switch of the suppression remedy demands clear Fourth Amendment rules on what police conduct triggers Fourth Amendment protection and what police conduct does not.' The third-party doctrine creates ex ante clarity by matching the Fourth Amendment rules for information with the Fourth Amendment rules for location. Under the doctrine, rights in information extinguish when the information arrives at its destination. This means that the present location of information defines the Fourth Amendment rules for collecting it, and the Fourth Amendment rules are constant within each location.\(^3\)

Kerr supports the third-party doctrine because it applies a clear-cut line, based upon where the information in question is stored, to determine whether the potential evidence is within the police power to obtain without a warrant. Consider the example of someone recording the numbers they have dialed on their home phone in a notebook beside the telephone when the police enter this person’s home, without a warrant, and take the notebook. This is a clear violation of the Fourth Amendment, and the third-party doctrine is not part of the discussion. However, if the police go to the telephone company and obtain a copy of the suspect’s telephone

---

records, Kerr says this demonstrates a correct and proper exercise of law enforcement power under the third-party doctrine. According to Kerr, the doctrine draws a clear and unambiguous line for Fourth Amendment cases: the location of the information obtained by law enforcement dictates unequivocally whether there has been a Fourth Amendment violation, and if the police lawfully exercised their power. The clarity provided by the third-party doctrine is one of the main aspects that makes it attractive and viable in application by the Court; however, Kerr understands that it is not perfect and it is not the only possible solution. In addition, it has been nearly impossible for the courts or legal scholars to develop a clear-cut and well-reasoned framework to replace the third-party doctrine, and this is another reason why Kerr supports the doctrine.

Without the third-party doctrine, courts would have to develop some alternative test, with the same ex ante clarity, for identifying when information is protected under the Fourth Amendment. This task may not be impossible, but it is quite difficult. Few critics of the third-party doctrine have tried. And the difficulty of devising a clear alternative to the third-party doctrine provides a second argument in its favor.39

Kerr is not arguing that the third-party doctrine is appropriate in all cases. When he considers a cost-benefit analysis of the doctrine in its application to Fourth Amendment law, the benefits outweigh the costs. The need for change in the third-party doctrine is not in question. Kerr understands that technology has changed since the time of Miller and Smith, but he contends that the solid legal principle of the third-party doctrine should not be abandoned, but, instead, should be carefully reworked. “The importance of third-party records in new technologies and the continuing criticisms of the Court's case law suggest that the time has come

for courts and commentators alike to develop a more sophisticated understanding of the third-party doctrine. The doctrine should be recast rather than cast aside."\(^{40}\)

In his article Kerr not only discusses the crucial advantages of the third-party doctrine, but he also examines two of the most relevant critiques of the doctrine. The first critique of the third-party doctrine is the doctrinal critique, which focuses on the legal arguments themselves. The doctrinal critique employs the Katz test:

According to, critics, individuals normally expect privacy in their bank records, phone records, and other third-party records. Such expectations of privacy are common and reasonable, and Justices who cannot see that are simply out of touch with society and are misapplying the Fourth Amendment. From this perspective, it ‘defies reality’ to say that a person ‘voluntarily’ surrenders information to third parties like banks or telephone companies. As Justice Marshall reasoned in his Smith dissent, ‘[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.’\(^{41}\)

The doctrinal critique emphasizes that simply because someone has handed over information to a third party does not mean that they lose all or any of ones expectation to privacy protections of the information. Some scholars and justices believe that this is a too narrow reading of the Fourth Amendment by the Court because in many instances the information given to a third party is not voluntarily conveyed. Nevertheless, giving this information to a third party is required for an individual to be a functional and productive member of society. This narrow reading may have held true for people using deposit slips at the bank in 1976, and phone numbers to make phone calls in 1979. But the real challenge to the third-party doctrine in the modern technology age comes in the form of emails, texts, phone calls, Facebook messages, and every other form of communication and interaction which are absolutely necessary not just in a modern social context, but also in nearly all modern workplaces. The use of the internet, email,


\(^{41}\) Kerr, “The Case for the Third-Party Doctrine,” 570-571.
text messages, and most other technology now requires information to be given to one or more third parties. According to this line of thinking, if the Court cannot realize that people do not assume a risk when they are simply performing the everyday tasks that are necessary to do their job and interact with other individuals in today’s society then their ability to answer the questions presented by technologies clash with the Fourth Amendment will be severely compromised. As a result, then the Court is truly out of touch with reality and must reconsider the application and intent of the third-party doctrine.

The doctrinal critique continues by challenging one of the parts of the doctrine Kerr supports, which is the ex-ante clarity. In his dissent in *Smith*, Justice Marshall was the first to warn about the Court’s adherence to an all-or-nothing policy regarding privacy, especially privacy surrounding information given to a third party. This warning has been heeded and accepted by many scholars and is one of the main critiques of the third-party doctrine.

A corollary to this claim is that the Justices supporting the third-party doctrine have misunderstood the concept of privacy. The Justices envision privacy as an on-off switch, equating disclosure to one with disclosure to all, and as a result they miss the many shades of gray. As Justice Marshall put the point in *Smith*, “privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.” Echoing Justice Marshall, Daniel Solove argues that the third-party doctrine is based on an incorrect “conception of privacy,” a conception of privacy as total secrecy. Along the same lines, Richard Posner argues that the Miller line of cases is “unrealistic.” “Informational privacy does not mean refusing to share information with everyone,” he maintains, for “[o]ne must not confuse solitude with secrecy.” Sherry Colb agrees, writing that “treating exposure to a limited audience as identical to exposure to the world' fails to recognize the degrees of privacy.”42

The other critique that Kerr examines is called the functional critique of the third-party doctrine. This critique examines how the government, under the third-party doctrine, is provided too much power over people, in order to allow them to fully participate in a free, honest, and

---

open society. Kerr uses Justice Harlan’s dissent in *United States v White* where he argued that allowing the government to use an undercover informant wearing a wire in an unregulated context would grant the government too much power, and take away too much privacy from the individual. Justice Harlan says,

> Were third party bugging a prevalent practice, it might well smother that spontaneity reflected in frivolous, impetuous, sacrilegious, and defiant discourse that liberates daily life. Much offhand exchange is easily forgotten and one may count on the obscurity of his remarks, protected by the very fact of a limited audience, and the likelihood that the listener will either overlook or forget what is said, as well as the listener's inability to reformulate a conversation without having to contend with a documented record. All these values are sacrificed by a rule of law that permits official monitoring of private discourse limited only by the need to locate a willing assistant.\(^{43}\)

Kerr cites Marshall’s dissent in *Smith* again to show that he also believed that unchecked power of the government due to unfettered access to information disseminated to a third-party would have a chilling effect on society.

> The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts. Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society.\(^{44}\)

### VII. Legal Scholars’ Objections to the Third-Party Doctrine

While Kerr presents one of the few arguments in support of the third-party doctrine, there are many different arguments against the doctrine, especially in the modern technology era.

Michael Price in his article, “Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine,” presents arguments for the inapplicability of many Fourth Amendment doctrines, in particular the third-party doctrine, to modern day society with its ever-expanding use of technology and communications involving third-party systems. “If the Supreme Court intends to


afford greater privacy protection to personal data stored electronically, as it seems inclined to do, then it may want to consider a new analytical framework for the job. Existing Fourth Amendment tests are not fit for the digital long haul.”

He recognizes that there is no need for an entire overhaul of Fourth Amendment tests and jurisprudence; rather, their needs to be adaptations made to recognize the immense and perpetually increasing role of technology in modern-day society. In Price’s view, “The framework is compatible with existing Fourth Amendment tests; there is no need to displace them entirely. But the proliferation of highly personal third-party data demands an avenue for Fourth Amendment analysis that is cognizant of its role in society.”

Price illustrates why the third-party doctrine simply cannot function in a society where nearly every action of a person going about ones daily life and work is recorded by a third party in some form or capacity. Allowing the government to access all this information about an individual’s information amounts to one of the most serious threats to privacy this country has ever witnessed.

Almost every aspect of online life now leaves a trail of digital breadcrumbs in the form of third-party records. Every phone call, every email, every search and click online can create a third-party record. Google, for example, keeps a copy of every search it is asked to make and, if possible, links each search to a particular user. There are even records of what people do not read and do not click. If courts take the third-party doctrine seriously, then police can lawfully obtain all of this information without a warrant or probable cause. It is no hyperbole to say that even a person’s mere curiosity could and would be monitored. As Daniel Solove observes, “[T]his state of affairs poses one of the most significant threats to privacy in the twenty-first century.”

Price next discusses, as Justice Marshall did in Smith, the inapplicability of the third-party doctrine as an all-or-nothing conceptualization of privacy. Again he points out how this doctrine

46 Price, 248-249.
47 Price, 268.
does not work in the current digital era and will not work in the future. He also echoes the worries that both Marshall and Harlan had, in *Smith* and *White* respectively, about how this all-or-nothing approach would create a world where police could request every utterance and every movement of a person. This would have the chilling effect of rendering American society less free and open as it once had been. As Price argues,

The third-party doctrine is especially problematic in the digital age because it treats privacy as a binary equation: either information is completely secret, or it is absolutely public. This principle is at odds with the way that people share information online. As with other types of personal interaction, sharing digital data is not an all-or-nothing endeavor; it is more like a sliding scale that users may control (although not always with success). Depending on the social media context, one may opt to comment anonymously, to send a message to just a few friends, or to post a public video on YouTube in search of worldwide Internet fame. The third-party doctrine disregards this nuance, treating everything as public. As more of life takes place online, the doctrine becomes more devastating to freedom of speech and association. Imagine a society where every thought, every utterance, every behavior conveyed through digital means is ‘public’ information, cataloged in a database, just waiting for the police to request it. The resulting chill to freedom of speech and association would cause an ice age.

With the problems of the third-party doctrine in the technology-driven twenty-first century well established, Price discusses how his solution to the third-party doctrine problem involves an expansion of the meaning of “papers,” from the language of the Fourth Amendment, to encompass a meaning consistent with current and future technology.

In this framework, the particular form or format of the data is not terribly important. The inquiry, in other words, should be technology-neutral. If ‘papers’ include private correspondence in the mail, then the same constitutional protection should carry forward to new and alternative modes of communication, whatever they may be. Phone calls, for example—sound waves transmitted over copper wire—are an essential form of private communication, deserving equal Fourth Amendment protection as parchment sealed with wax. Privacy should not become a casualty of technology. Letters, telegraphs, phone calls, emails, and text messages—they are all forms of private communication and would therefore be treated as ‘papers’ for Fourth Amendment purposes.

---

48 Price, 268.
49 Price, 273.
Redefining the definition of what a “paper” means under the Fourth Amendment would not be an easy task for the judiciary; however, it will provide a significantly more appropriate framework and guide to deal with current and future technology and its inevitable collision with the third-party doctrine.

VIII. A World Without Privacy

The next critique of the third-party doctrine does not just seek a reformulation of the doctrine, but a reformulation of the expectations of privacy in a society. Paul Ohm questions the very nature of whether privacy still exists in modern society due to the amount of information that is shared with third parties, with friends and family, and with private technology companies. Ohm questions that if there is no privacy left in the world, does the Fourth Amendment still hold any power, and if it does then what would be the constraints on the power of the government to acquire all these records given to third parties by individuals?

Does that amendment [‘s] “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures” survive once the police can request from the private sector the fruits of comprehensive, consensual private surveillance? Were we unthinkingly to extend current Fourth Amendment doctrine, the answer to these questions might be no. If we woke up tomorrow in a world without privacy, we might also find ourselves in a world without constitutional protection from new, invasive police powers. This bleak scenario is not science fiction, for tomorrow we will likely wake up in that world.50

Ohm is extremely concerned that the trend of individuals using devices and services through a third party that will track and store every aspect of one’s life. As a result under the current Fourth Amendment doctrines an Orwellian 1984-type society exists. In this society, law enforcement will be able to use warrantless searches to track people’s movements, and learn unlimited information on every American.

---

As the surveillance society expands, the police will learn to rely more on the products of private surveillance, and will shift their time, energy, and money away from traditional self-help policing, becoming passive consumers rather than active producers of surveillance. Private industry is destined to become the unwitting research and development arm of the FBI. If we continue to interpret the Fourth Amendment as we always have, we will find ourselves not only in a surveillance society, but also in a surveillance state.\(^{51}\)

Ohm notes that while many scholars have conflicting views about the third-party doctrine, none are willing to take the discussion to the place he is, a world where privacy no longer exists.

“...These authors have all recognized, to greater or lesser extent, that privacy is on the decline or has rapidly been redefined, but these middle-strength observations and predictions have given rise to proportionate half measures.”\(^{52}\) Ohm’s entire argument hinges upon changing the underpinnings of the Fourth Amendment thinking from an argument that is based upon balancing privacy and security, to one that centers around the dispersion of power between the state and the individuals. “Privacy has served as a useful proxy for deciding what the Fourth Amendment protects. As we witness the rapid decline of privacy, we should be prepared to rebuild the Fourth Amendment on a new foundation focused on the balance of power between the state and its citizens.”\(^{53}\)

Ohm argues that in order to achieve the desired balance in his privacy-less society a new test must be put into place. Under his formulation, the critical test of how high a burden should be placed on police before they may access and use this new technology must ask who will bear the more significant injury should errors in use of the new technology occur. Ohm believes that under the current third-party doctrine, society and the people bear the cost of the errors committed by law enforcement when the police use new technology involving a third party in order to conduct investigations or arrest an individual; however, in a society with diminished or

\(^{51}\) Ohm, 1311.
\(^{52}\) Ohm, 1330.
\(^{53}\) Ohm, 1336.
no privacy, the cost of errors should fall directly upon law enforcement, which should bear the burden in order to use a new device, a new database, or new surveillance technique.

The cost of errors should be borne first by the police. Whenever a private company enables a new form of surveillance, the police should be forced to assume that access to the fruits of the surveillance requires a warrant and probable cause until we know (with the assistance of metrics) that the new service benefits criminals more than it helps the police.\(^{54}\)

**IX. Modern Legal Applicability of the Third-Party Doctrine**

While all of these scholarly arguments for and against the third-party doctrine are well thought out and well constructed, they may have only limited impact on the doctrine’s direction. Justice Sonia Sotomayor, in *United States v. Jones*, provided the first insight into what the current Court—or at least one member of the Court—may be thinking about the third-party doctrine in today’s technologically advanced society. Justice Sotomayor, who harkens back Justice Marshall’s dissenting opinion in *Smith*, focuses on the problem that a large amount of information given to third parties by individuals today is not given voluntarily due to the need to be a functioning member in a free and open society. Furthermore, she believes that this information, even though it is given to a third party, absolutely garners a subjective expectation of privacy that society is willing to recognize as reasonable. As a result, she believes it may very well be time to reconsider the application of the third-party doctrine in this technology age.

More fundamentally, it 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. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the ‘tradeoff’ of privacy for convenience ‘worthwhile,’ or come to accept this ‘diminution of privacy’ as ‘inevitable,’ and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the

\(^{54}\) Ohm, 1351-1352.
societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. 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.\footnote{United States v. Jones 565 U.S. 400, 417-418 (2012) (Sotomayor, J., concurring).}

While this may only be the opinion of one Justice it is a strong rebuke of the third-party doctrine. Moreover, the concurring opinion by Justice Alito in \textit{Jones}, in which four other justices joined, though not nearly as strong, made some very conspicuous references to the possibility of the Court looking into the application of the third-party doctrine in the twenty-first century digital age.

This chapter has laid the foundation upon which the third-party doctrine is built, not only from a case law perspective, but also from the viewpoint of prominent Fourth Amendment scholars. The following chapters will dive much deeper into the legal, legislative, and scholarly debate surrounding technology and the Fourth Amendment, the balance between police power and individual privacy, and the third-party doctrine. Chapter Two will present the modern technology Fourth Amendment cases such as \textit{Kyllo}, \textit{Jones}, and \textit{Riley} and how they have culminated in the pending Supreme Court case of \textit{Carpenter v. United States}.  


Chapter 2: The Fourth Amendment and Modern Technology

More fundamentally, it 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 in 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.\(^5^6\)

The Supreme Court created the third-party doctrine in the late 1970s in Smith and Miller. In the 1970s, 1980s, and 1990s the doctrine was relatively uncontroversial; however, by the 2000s, the development of more sophisticated technology started to rapidly outpace the evolution of Fourth Amendment case law. The architects of the Fourth Amendment had no way of predicting how technology would advance, or to what degree, and at what pace technology would evolve. They created the amendment to protect themselves and their fellow citizens from the issue of the writs of assistance issued by the British government before and during the Revolutionary War. The framers had no way of conceiving the advent of automobiles, cell phones, emails, computers, or a tool as powerful as the Internet. This chapter will focus on the how the Court has dealt with the clash between digital era technology and analogue era doctrines and precedents.

1. Kyllo v. United States

The Court first considered the possible impact of new technology on the existing Fourth Amendment law in Kyllo v. United States. This case, decided in 2001, concerned police using a thermal imager to detect infrared radiation, the radiation emitted by most objects, which cannot be seen by the human eye. A thermal imaging scan shows heat signatures of the radiation. This is significant, because in order to grow marijuana indoors, one “typically requires high intensity lamps.”\(^5^7\) Agent William Elliot used a thermal imager to scan Danny Kyllo’s house to see if Mr.

Kyllo was using high intensity lamps. After explaining the basic facts of the case, and the foundational underpinnings of the Court’s technology-based jurisprudence, Justice Scalia states,

It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. For example, as the cases discussed above make clear, the technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private. See *Ciraolo, supra*, at 215. The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.\(^{58}\)

Implicit in Scalia’s statement is, no matter what a Justice’s philosophy about originalism or in a living evolving Constitution, it must be recognized that technological innovation is relevant to the Court’s Fourth Amendment decisions. Scalia continues his argument by discussing *Katz* and the reasonable expectation of privacy test. He understands that the use of technology by police in order to gather evidence against criminals will need a case-by-case interpretation; however, he will not accept that technology will require or allow for diminished privacy protections in the most revered and protected institution in Fourth Amendment jurisprudence, the home.

While it may be difficult to refine *Katz* when the search of areas such as telephone booths, automobiles, or even the curtilage and uncovered portions of residences is at issue, in the case of the search of the interior of homes the prototypical and hence most commonly litigated area of protected privacy there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment.\(^{59}\)

Scalia’s forward-looking opinion is not one that solely answers the question presented in *Kyllo*; but in addition he is doing what justices must often do, and that is consider how their current decision will impact future cases. Such opinions are especially important when technological innovation is occurring so rapidly.

---

\(^{58}\) *Id.* at 33-34.

\(^{59}\) *Id.* at 34.
We rejected such a mechanical interpretation of the Fourth Amendment in *Katz*, where the eavesdropping device picked up only sound waves that reached the exterior of the phone booth. Reversing that approach would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home. 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.60

Scalia imagined cases such as *United States v. Jones, Riley v. California*, and *Carpenter v. United States*, in which the Court is confronted with more complex and pressing questions about the Fourth Amendment’s application, including the application of the third-party doctrine to the modern, technology-driven society.

II. *United States v. Jones*

In *United States v. Jones*, the Court dealt with, “Whether the attachment of a Global-Positioning-System (GPS) tracking device to an individual’s vehicle, and subsequent use of that device to monitor the vehicle’s movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment."61 The police attached a GPS tracking device to the bottom of Mr. Jones’ car and recorded his whereabouts for twenty-eight days. The Supreme Court, in a unanimous opinion, ruled that the use of a GPS did in fact violate Mr. Jones’ Fourth Amendment rights. Justice Scalia’s majority opinion seemed to take a step back in time from his opinion in *Kyllo*. Scalia’s analysis applied the physical trespass doctrine highlighted in the *Olmstead* decision, while the concurring opinions by Alito and Sotomayor, drove at the heart of the growing incongruence between the digital age and the Court’s Fourth Amendment jurisprudence. “Yet, while the *Jones* majority did little to stop the erosion of Fourth Amendment protections because it focused exclusively on the government’s trespass on the defendant's vehicle, the two concurrences suggest future judicial evaluation of changing expectations of

60 Id. at 35-36.
privacy in the digital age.” While Alito and Sotomayor agree with the outcome of the case, Alito questioned the grounds and reasoning of the majority opinion, and Sotomayor focuses on the applicability of the third-party doctrine in the digital age. This does not mean that Alito completely ignores the third-party doctrine in the digital age. Rather, he just has a different approach to how the issue should be solved, which could impact how he and other members of the Court vote on the pending Carpenter case.

Justice Alito’s concurring opinion begins by echoing Justice Scalia’s majority opinion from Kyllo. He says, “This case requires us to apply the Fourth Amendment’s prohibition of unreasonable searches and seizures to a 21st-century surveillance technique.” Beyond that opening however, Alito diverges from Scalia’s analysis, by criticizing and questioning the entire base of the Scalia’s majority opinion. Alito believes the physical trespass doctrine utilized by the majority is not only outdated in the post-Katz line of cases, but also creates many future problems in cases involving technology and the Fourth Amendment:

The premise that property interests control the right of the Government to search and seize has been discredited… In sum, the majority is hard pressed to find support in post-Katz cases for its trespass-based theory. Disharmony with a substantial body of existing case law is only one of the problems with the Court’s approach in this case. Alito goes on to list the four additional problems that he believes the majority opinion will create for the Court in the future.

First, the Court’s reasoning largely disregards what is really important (the use of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car’s operation)… Second, the Court’s approach leads to incongruous results… Third, under the Court’s theory, the coverage of the Fourth

64 Id. at 423-424 (Alito, J., concurring).
Amendment may vary from State to State... Fourth, the Court’s reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked.65

III. Judicial or Legislative Solution

For all the problems that technology presents to the Fourth Amendment and citizen’s privacy, Alito believes that the solution lies not in opinions written by the Court but by legislation passed by Congress. The solution should come from Congress, not the nine justices on the Court, identifying and codifying privacy and privacy expectations in the twenty-first century. Alito understand and recognizes that the times have changed, and that the expectations of privacy in society have evolved due to technology, and will continue to evolve as the nature and sophistication of available technology changes. This will result in the need to have those changes reflected in the law, due to the actions and legislation by Congress, especially when it comes to the Fourth Amendment.

In addition, the Katz test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.66

Alito believes that it is well within the right, power, and capability of Congress to enact legislation to reflect the constantly changing expectation of privacy that the people of the United States have, and will continue to have. He wants Congress to use its enforcement power to codify privacy expectations in a way which the Court would never be able to do. In Alito’s view, Congress is far better suited to conduct research to understand what people hold as a

65 Id. at 424-426 (Alito, J., concurring).
66 Id. at 427 (Alito, J., concurring).
subjective expectation of privacy, what society is ready to accept as reasonable, and what trade-offs people are willing to make in terms of security and convenience, for privacy protections. Congress has shown the ability to accomplish this before with wiretapping when they passed the Electronic Communication Privacy Act of 1986 (ECPA). Although the ECPA does not account for the advanced level of technology used today, the ECPA still shows that Congress has used its power before to regulate the use of technology by the government when it comes to Fourth Amendment issues.

On the other hand, concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping. After Katz, Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute, see 18 U. S. C. §§2510–2522 (2006 ed. and Supp. IV), and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law. 67 Alito believes that a legislative solution would allow for the necessary clarity to be gained on the complex issue of government surveillance, and use of technology as it pertains to the Fourth Amendment rights of citizens in the technology era. Whether the legislature or the Court is the best vehicle to answer these questions will be discussed in the coming chapters.

By contrast, in her separate concurrence, Justice Sotomayor believes that it will be up to the Court to deal with the relationship between privacy and technology. Justice Sotomayor agrees with Justice Alito about the impact that technology will have in shaping the future of Fourth Amendment cases. She says, “As Justice Alito incisively observes, the same technological advances that have made possible non-trespassory surveillance techniques will also affect the Katz test by shaping the evolution of societal privacy expectations.” 68 Society’s changing expectations must be taken into account when applying not only the Katz test moving forward,

67 Id. at 427-428 (Alito, J., concurring).
68 Id. at 415 (Sotomayor, J., concurring).
but also, in the Court’s view of how technology and the Fourth Amendment work and function together. “Justice Sotomayor’s decision…went further than Justice Alito in emphasizing the importance of updating the Court’s evaluation of expectations of privacy.”

As Lauren Elena Smith showcases in her article, “Jonesing for a Test: Fourth Amendment Privacy in the Wake of United States v. Jones,” Justice Sotomayor states her belief that the Court must take action to update people’s expectations of privacy in the digital age by dealing with the outdated analogue third-party doctrine.

She took the critique one step further by examining more circumstances in which the Court should update its conception of what is reasonable given the norms to which society has adjusted. By highlighting several shortcomings of current judicial treatment of ‘voluntary’ communication of information, Justice Sotomayor brought attention to circumstances in which citizens do currently have an expectation of privacy that is not currently recognized by the Court.

Sotomayor analyzes the main issue of the third-party doctrine in the digital era from two different angles.

Justice Sotomayor focused on two primary circumstances in which voluntary communication of information [to a third party] enabled by technology leads to exploitation of citizens’ expectation of privacy that the Katz test should protect: first, the ability of third-party information collectors to pass information to the government and, second, the ability of law enforcement to easily and warrantlessly ascertain and aggregate the totality of a person’s movements.

The government’s ability to collect “voluntarily” surrendered information from third parties, such as Internet service providers or phone companies—information that contains an unprecedented degree of private and intimate information—is growing daily. Also, not only is the sheer volume of information increasing, but also the intimate and private nature of information available from third parties. However, though the amount and intimacy of the

69 Lauren Elena Smith, 1016.
70 Lauren Elena Smith, 1017.
71 Lauren Elena Smith, 1017.
information that the government can obtain from third parties has dramatically increased, at the same time the privacy protection afforded to the individual regarding that information has not.

This is the first issue that Sotomayor feels the Court must address going forward. People have an expectation of privacy in the information that they relay to third parties today, because it touches every aspect of their daily lives and work. “People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.”

Sotomayor notes how the government is able to aggregate such a massive amount of private and intimate information in a way in which they never were previously capable. Not only can the government obtain this information in massive quantities and depth as they never could before, but also they can do so more easily than at any other time in history.

The Government can store such records and efficiently mine them for information years into the future… I would ask whether people reasonably expect that their movement will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.

She discusses how these “voluntary” acts of giving information to a third party are not voluntary in today’s world, and yet the doctrine from years ago is still the controlling precedent.

More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. E.g., Smith, 442 U. S., at 742; United States v. Miller, 425 U. S. 435, 443 (1976). 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.

Although the concurring opinions of Justice Alito and Justice Sotomayor apply different analysis, it seems clear that within the Court there is a recognition that there is a need for broader

---

73 Id. at 415-416 (Sotomayor, J., concurring).
74 Id. at 417 (Sotomayor, J., concurring).
protections has increased from the enactment of the Fourth Amendment, to the time of the
Olmstead and Katz decisions, and finally to the time of the third-party doctrines creation in Smith
and Miller. However, the extent of this required increase in privacy and which branch of
government will implement this increase is still being debated and decided by the Court.

IV. Riley v. California

In Riley v. California the Court continued to rework the Fourth Amendment jurisprudence in
response to changing technology and an individual’s constant interaction with technology in ones
daily life. Although the decision in Riley does not directly implicate the Court’s third-party
doctrine, it holds a potentially key feature of the currently pending Cell Site Location
Information (CSLI) case, Carpenter v. United States. Mr. Riley had been stopped for a traffic
violation, which resulted in him being arrested on weapons charges. The arresting officer,
without a warrant, “accessed information on [Riley’s] phone and noticed the repeated use of a
term associated with a street gang.” Some hours later, a special agent, who was a gangs expert,
went through the digital contents of the phone, still without a warrant, and concluded:

Based in part on photographs and videos that the detective found, the State charged Riley in
connection with a shooting that had occurred a few weeks earlier and sought an enhanced
sentence based on Riley’s gang membership. Riley moved to suppress all evidence that the
police had obtained from his cell phone.

The issue presented in Riley was whether law enforcement needed a warrant to search the digital
contents of an arrested person’s cellphone. The Court, in a unanimous decision written by Chief
Justice Roberts, held that a warrant was required to search the contents of an arrested person’s

---

75 Riley v. California, No. 13-132, Slip op. at 1 (June. 25th, 2014).
76 Riley, slip op. at 1.
demonstrate how the evolution and advancement of technology requires Fourth Amendment case law to evolve in order to properly protect individual privacy rights.

Phones are based on technology nearly inconceivable just a few decades ago… Absent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement ‘by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.’

Chief Justice Roberts rejected the government’s argument that searching the millions of personal points of data available by searching a phone is “materially indistinguishable” from the search of physical persons or effects on a suspect at the time of an arrest. Roberts noted that the two concepts are entirely incompatible with the recognized privacy expectations under the Fourth Amendment in the modern digital age.

The United States asserts that a search of all data stored on a cell phone is “materially indistinguishable” from searches of these sorts of physical items. Brief for United States in No. 13–212, p. 26. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee’s pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.

The Chief Justice continues, explaining why cell phones, and in particular, the data that is stored on them must be treated differently as a matter of law. Not only is the device able to make calls, but it also has the capacity to perform countless other functions, and store countless amounts of data all within a person’s pocket, backpack, or purse.

Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee’s person. The term “cell phone” is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as

---

77 Riley, slip op. at 9.
78 Riley, slip op. at 16.
79 Riley, slip op. at 16-17.
a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.\textsuperscript{80}

The capabilities of a cell phone are undeniable, but what truly sets modern smart phones apart from devices or papers previous generations of suspects held on their person is the storage capacity and the details that the digitally stored content on a person’s phone can reveal about them.

One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. See Kerr, Foreword: Accounting for Technological Change, 36 Harv. J. L. & Pub. Pol’y 403, 404–405 (2013). Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in Chadwick, supra, rather than a container the size of the cigarette package in Robinson.\textsuperscript{81}

Chief Justice Roberts and other members of the Court understand that the current storage capacities of phones will not diminish or remain where they are; they will only grow as the technology becomes better. This will create and widen the gap between the amount of information one could physically have on them when arrested, and the amount of digital information stored on their phones. “We expect that the gulf between physical practicability and digital capacity will only continue to widen in the future.”\textsuperscript{82} The privacy interests of the information on a phone lie in four different compartments for the Court, and all of them factor into the Court’s unanimous decision that police need a warrant before searching the intimate and voluminous information stored on a arrestee’s cell phone.

The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any  

\textsuperscript{80} Riley, slip op. at 17.  
\textsuperscript{81} Riley, slip op. at 17.  
\textsuperscript{82} Riley, slip op. at 18.
isolated record. Second, a cell phone’s capacity allows even just one type of information to convey far more than previously possible. The sum of an individual’s private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.83

The final connection between the storage capacity of modern day cell phones and privacy leads perfectly into the issues presented in the Carpenter case: the “voluntary” nature of owning a smart phone in modern society.

Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower. See Harris Interactive, 2013 Mobile Consumer Habits Study (June 2013). A decade ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary… But those discoveries were likely to be few and far between. Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate… Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.84

Having a cell phone in modern society is not a voluntary act or a status symbol; it is a required tool for people’s jobs, social lives, and everything in between. The voluntary aspect of owning and using a cell phone, which interacts thousands of times a day with third parties, gives the government the opportunity to access millions of points of data on nearly every citizen, without a warrant, including the CSLI data at the center of the Carpenter case.

83 Riley, slip op. at 18.
84 Riley, slip op. at 19.
V. Carpenter v. United States

The progression of Fourth Amendment cases in *Kyllo, Jones,* and *Riley* all lead up to *Carpenter v. United States,* which was argued on November 19th, 2017. *Carpenter* presents the Court with the opportunity to decide how all of its Fourth Amendment precedents and doctrines discussed in this paper will be applied in the modern technology era. In *Carpenter* four men were suspected of committing a series of armed robberies in April 2011. One of the four men gave the FBI not only his cell phone number, but also the cell phone numbers of the other three suspects. With this information the FBI sought three orders, to obtain the “transactional records” of the alleged participants in the armed robberies. These orders, known as 2703(d) orders, were granted under provision 2703(d) of the Stored Communications Act,

That Act provides that the government may require the disclosure of certain telecommunications records when ‘specific and articulable facts show that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.’

In *Carpenter,* the transactional records that were requested included not only the date and time of calls, but also the location of the phone, and as a result the location of Mr. Carpenter, based upon the cell phone’s distance from cell phone tower sites. This is where the Cell Site Location Information (CSLI) occurs. Any time a cellphone automatically sends signals to a cell tower, pings the tower, in order to retrieve new emails, text messages, or refresh a web search, a new CSLI data point is created for that cell phone user. This pinging of cell site towers

---

by an individual’s cellphone in order to refresh applications and processes on a phone creates new
CSLI data points hundred if not thousands of times each day.

The private information available from cell phones is not limited to the data stored on the
phone itself. For a phone to receive and share much of that data—to be usable at all—it must
connect with a cell tower. Every time it does, it generates information, stored by the phone
company, about which tower the phone connected to—essentially where the phone was—on
a given date and time. These small bits of data—called cell site location information (CSLI)—are aggregated by providers and, like GPS data, they ‘generate a precise,
comprehensive record of a person’s public movements that reflects a wealth of detail about
her familial, political, professional, religious, and sexual associations.’

In Carpenter the Government obtained 127 days of Mr. Carpenter’s CSLI data. The case
presents numerous issues for the Court to grapple with, and many different doctrines and
precedents to adapt to the reality of the modern digital age. It presents a true test of how the
Court will deal with the Fourth Amendment’s expectations of privacy and the third-party
document in the era of ever growing-digital data and cell phone usage and capabilities.

A. Petitioner’s Brief in Carpenter v. United States

In the petitioner’s brief for Carpenter, the main argument is that CSLI should be covered
under the Katz test and receive the protection of requiring a warrant before the government can
obtain this information. In order to establish this point Carpenter puts forth three arguments, 1).
Showing that there is subjective expectation to privacy that society is ready to accept as
reasonable, 2). That the analogue era third-party doctrine, from Smith and Miller, does not apply
to this digital age, 3). Finally how under the Telecommunications Act § 222(c)(1)-(2), (h)(1)(A)
CSLI data is the property of the wireless customer, and therefore “papers” under the Fourth
Amendment in the digital age.

88 Brief for Electronic Frontier Foundation, et al. as Amici Curiae Supporting Petitioner,
1. Carpenter Has a Reasonable Expectation of Privacy

In order to show that the government conducted a search, without a warrant, and therefore violated his Fourth Amendment rights, Carpenter must show that CSLI passes the *Katz* test from Justice Harlan’s concurrence.

Under this Court’s longstanding test, government agents engage in a Fourth Amendment search when they intrude on an expectation of privacy that society is prepared to recognize as reasonable. *Kyllo v. United States*, 533 U.S. 27, 33 (2001); *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). 89

The *Katz* framework was put into place, and must be applied to the technology available to the government today, in order to “‘assure preservation of that degree of privacy against government that existed’ prior to the advent of the new technology in question.” 90 The prime example of this is from the *Katz* case where the “Court held…that the Fourth Amendment applies to conversations transmitted over telephone lines because phones played a ‘vital role’ in conducting the type of communication previously treated as ‘private.’” *Katz*, 389 U.S. at 352-53. 91 Carpenter argues that just like the GPS device used to track Mr. Jones’ every movement, CSLI does the exact same thing, but on a more accurate, and detailed level.

Applying this framework in *United States v. Jones*, five Justices agreed that people have a reasonable expectation of privacy in ‘longer term GPS monitoring in investigations of most offenses.’ *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment). Because GPS monitoring of a car tracks ‘every movement’ a person makes in that vehicle, id. at 430 (Alito, J., concurring in the judgment), it generates extremely sensitive and private information that ‘enables the Government to ascertain, more or less at will, [people’s] political and religious beliefs, sexual habits, and so on,’ id. at 416 (Sotomayor, J., concurring). Prior to the digital age, this information would have been largely immune from search. Although historically the government could have tasked a team of agents with surreptitiously tailing a suspect, doing so ‘for any extended period of time was difficult and costly and therefore rarely undertaken.’ Id. at 429 (Alito, J., concurring in the judgment). Therefore, ‘society’s expectation has been that law enforcement agents and others would not— and indeed, in the main, simply could

---

90 Brief for Petitioner, 15.
91 Brief for Petitioner, 15.
not—secretly monitor and catalogue every single movement of an individual’s car for a very long period.’ Id. at 430.\textsuperscript{92}

CSLI does the same thing as long-term GPS monitoring, but can give a law enforcement individual an even more vivid depiction of the individual’s movements and associations during the collection of CSLI data. Relying on the result in\textit{Jones}, and the \textit{Katz} test, Carpenter argues, “These principles dictate that government agents conduct a search when they obtain longer-term historical cell phone location records from a person’s cellular service provider.”\textsuperscript{93}

Carpenter asserts that any ruling other than one that affords a reasonable expectation of privacy in CSLI is inconsistent with\textit{Jones} and with the principle laid down in\textit{Katz}.

For the same reason that five Justices concluded that there is a reasonable expectation of privacy in longer-term GPS monitoring of a car, there is a reasonable expectation of privacy in longer-term cell phone location records. Any other conclusion would allow the government to circumvent the principle accepted by five Justices in\textit{Jones} through the simple expedient of obtaining cell phone location records. People use their cell phones throughout the day—when they are at home, work, or school, when they are in the car or on public transportation, when they are shopping or eating, and when they are visiting the doctor, a lawyer, a political associate, or a friend. People even keep their phones nearby and turned on while they are asleep. Indeed, ‘nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.’ Riley, 134 S. Ct. at 2490. ‘[D]etails about the location of a cell phone can provide an intimate picture of one’s daily life.’ State v. Earls, 70 A.3d 630, 642 (N.J. 2013)…And to state the obvious, when people make a ‘visit to a gynecologist, a psychiatrist, a bookie, or a priest,’ they typically ‘assume that the visit is private.’ United States v. Davis, 754 F.3d 1205, 1216 (11th Cir. 2014) (Sentelle, J.), rev’d en banc, 785 F.3d 498 (11th Cir. 2015).\textsuperscript{94}

The type of detail and infallible computer generated data that the CSLI provides law enforcement is far beyond anything the government has ever had the power to obtain.

Indeed, prior to the digital age, the only way for the government conceivably to have obtained anything close to [CSLI]…would have been to ask the suspect to recall his past movements and divulge them to police. But that exercise would be severely limited by the vagaries of human memory and the Fifth Amendment’s privilege against self-

\textsuperscript{92} Brief for Petitioner, 16.
\textsuperscript{93} Brief for Petitioner, 16.
\textsuperscript{94} Brief for Petitioner, 16-17.
Carpenter continues by again illustrating how the CSLI will only become more precise and revealing as the number of cell sites increase, and as the cell phone technology becomes more advanced. In order to preserve the expectation of privacy adopted by the framers about a person’s location history and whereabouts, Carpenter concludes that the only thing the Court can do is bring the Katz test into the twenty-first century and protect citizens from unlimited government access to their CSLI. “Drawing a line that protects against collection of longer-term location records is crucial to preserving the privacy that Americans enjoyed from the Framing to the dawn of the digital age.”

2. The Analogue Third-Party Doctrine is not Applicable in the Digital Era

The second prong of Carpenter’s case is to show that the decisions of Smith and Miller upon which the Sixth Circuit based its decision are incorrect. Carpenter believes that this approach is incorrect, and incompatible with CSLI in two major ways.

The Sixth Circuit believed that two cases from the pre-digital age—Smith v. Maryland, 442 U.S. 735 (1979), and United States v. Miller, 425 U.S. 435 (1976)—constituted ‘binding precedent’ precluding application of the Fourth Amendment to the records at issue. Pet. App. 12a-14a; see also BIO 14. They do not. There is no basis in this Court’s jurisprudence for extending Smith and Miller to CSLI, both because the information is more sensitive, and because it is not voluntarily shared with a third party in any meaningful way.

Not only does Carpenter believe that Smith and Miller are not workable in the digital age, the lawyer who argued and won for Maryland, in Smith v. Maryland, believes that the third-party doctrine should not apply to the modern digital era, especially to CSLI.

---

95 Brief for Petitioner, 18-19.
96 Brief for Petitioner, 31.
97 Brief for Petitioner, 35.
The facts in *Carpenter* are markedly different — and so is the technology…A majority of the U.S. Court of Appeals for the 6th Circuit held that the phone-based logic of *Smith* was also applicable to cell-tower communications and affirmed Carpenter’s convictions…This is taking the *Smith* precedent way too far, in a vastly different technological age. When the Supreme Court decided *Smith*, in the pre-dawn of the digital age…no one involved in the case could foresee the digital revolution that was to come.\(^{98}\)

Carpenter is not asking for the Court to overturn *Smith* and *Miller*. Instead, Carpenter is asking the Court to distinguish these decisions by virtue of the nature of the information available to the police in the digital age.

This Court need not disturb the holdings of *Smith* and *Miller* to conclude that they do not apply in this context. The particular records at issue here are far more sensitive and personal than those in *Smith* and *Miller*, and are not conveyed in a meaningfully voluntary way. Indeed, the typical user is not even aware that the cellular service provider has this compendium of sensitive information.\(^{99}\)

3. CSLI Data is Considered the “Papers” of the Cellular Customer

The final element of Carpenter’s argument is found in a provision of the Telecommunication Act, specifically § 222(c)(1)-(2), (h)(1)(A). This provision,

> [d]esignates cell phone location information as “customer proprietary network information” (“CPNI”)—a category of records that the service provider cannot disclose absent “approval of the customer.” 47 U.S.C. § 222(c)(1)-(2), (h)(1)(A). As the Federal Communications Commission explains, location information “clearly qualifies as CPNI,” and therefore subjects service providers to “a duty to protect [its] confidentiality.”\(^{100}\)

As a result of this, and the intent behind the act to clearly include location data, Mr. Carpenter’s CSLI data would clearly become his “papers,” which are explicitly stated as being protected under the Fourth Amendment. “The proprietary interest created by statute makes clear that CSLI is the “paper”—of the customer. ‘[T]o the extent CPNI is property, . . . it is better understood as


\(^{99}\) Brief for Petitioner, 36.

\(^{100}\) Brief for Petitioner, 33.
belonging to the customer, not the carrier.” Carpenter concludes that his aim is not to have
Smith and Miller and the third-party doctrine overturned, but instead find a necessary and
appropriate balance between privacy and police powers,

In sum, clarifying that a warrant is required will ensure that law enforcement officers can acquire particular spans of location records where there is probable cause that they will provide evidence of criminal conduct. And it will protect records that are not pertinent to the investigation but that can reveal much private information about a person’s life. This Court should provide a ‘simple’ answer to the question presented: ‘get a warrant.’ Riley, 134 S. Ct. at 2495.

B. Brief for the Respondent

The government’s position in Carpenter was succinctly summarized in the oral argument of the case, where Mr. Dreeben, speaking for the government said,

The technology here is new, but the legal principles that this Court has articulated under the Fourth Amendment are not… They [the cell phone companies] choose to make their own business records… They make decisions based on their business needs about what there going to retain. And when the government comes and asks them to produce it, it is doing the same thing that it did in Smith. It is doing the same thing that it did in Miller. It is asking a business to provide information about the business’s own transactions with a customer. And under the third-party doctrine, that does not implicate the Fourth Amendment rights of the customer.

In its brief the United States attempts to refute the claim that obtaining the CSLI information of an individual from a wireless carrier is a search under the Fourth Amendment. It is not a search because the third-party doctrine created in Smith and Miller gave the government the right to obtain information from a third party, and it would not be considered a search. “In its decisions in Miller and Smith v. Maryland, 442 U.S. 735 (1979), this Court further concluded that the acquisition of a business’s records does not constitute a Fourth Amendment ‘search’ of an

101 Brief for Petitioner, 34.
102 Brief for Petitioner, 58.
individual customer even when the records reflect information pertaining to that customer." Even though the technology of CSLI and cellphones is new, the United States is arguing that the Court should decide the case under the same precedents that have been in place for nearly four decades. “The principles set forth in *Miller* and *Smith* resolve this case.” Specifically, one of the main principles from *Smith* and *Miller* that should carry through and apply to this case is articulated below:

Any subjective expectation of privacy in information transmitted to a cellular-service provider by engaging its cellular network would not be objectively reasonable because ‘a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.’ *Smith*, 442 U.S. at 743-744… a cell-phone user must reveal his general location to a cell tower in order for the cellular service provider to connect a call. And a cell phone user thus ‘takes the risk, in revealing his affairs to [the cellular-service provider], that the information’ he transmits in engaging the cellular network ‘will be conveyed by [the cellular-service provider] to the Government.’ *Miller*, 425 U.S. at 443. Because petitioner ‘voluntarily conveyed to [his cellular-service providers] information that [they] had facilities for recording and that [they] w[ere] free to record,’ he ‘assumed the risk that the information would be divulged to police.’ *Smith*, 442 U.S. at 745.

Under this line of thinking, the government concluded that the Sixth Circuit “correctly concluded that the government’s acquisition of the historical cell-site data did not constitute a Fourth Amendment search.” The United States recognizes that there is new technology present in this case, and that Carpenter utilizes *Jones* and *Riley* to make his argument. However the United States attempts to distinguish these two cases from *Carpenter*, noting they only relate to *Carpenter* because of their use of new technology, not because of their relation to the third-party doctrine and its applicability to the modern digital age.

Petitioner suggests (Pet. 16-18, 27-28) that the Fourth Amendment principles recognized in *Smith* and *Miller* should not apply to new technologies. Although petitioner relies (Pet. 16-

---

104 Brief For The United States In Opposition at 11-12, *Carpenter v. United States* (2017) (No. 16-402).
105 Brief For The United States In Opposition, 14.
106 Brief For The United States In Opposition,15-16.
107 Brief For The United States In Opposition,16.
18) on Jones and Riley v. California, 134 S. Ct. 2473 (2014), those decisions did not address—much less disavow—this Court’s precedents recognizing that an individual does not have a Fourth Amendment interest in a third party’s records pertaining to him or in information that he voluntarily conveys to third parties.\textsuperscript{108}

The brief also addresses Carpenter’s claim that having a cell-phone and creating CSLI is not voluntary at the modern day and age. The government’s brief contends that,

Petitioner chose to carry a cell phone for the purpose of having his wireless provider route calls to and from him whenever he was in range of a cell tower. By ‘expect[ing] his phone to work,’ he ‘permit[ed]—indeed, request[ed]—his service provider to establish a connection between his phone and a nearby cell tower,’ and he thus ‘voluntarily convey[ed] the information necessary for his service provider to identify the [historical cell-site data] for his calls.’\textsuperscript{109}

Since people understand that in order for their phone to send and receive calls, emails, text messages, and use the internet, the phone must connect to the carrier’s cell towers and receive a cell signal, they are properly viewed as voluntarily conveying this information to the cell phone company, a third party. In addition, the United States argues for the continuing applicability of the third-party doctrine, and it also rejects that the sensitivity and intimacy of the information CSLI can reveal about a person garners any legal standing or precedent case law.

Petitioner also errs in suggesting (Pet. 29) that Smith and Miller are inapplicable because the records at issue in this case are ‘exceedingly sensitive and private in ways that were not at issue in [those decisions].’ Petitioner provides no support for his contention that records of the cell towers to which a phone connected when placing or receiving a call are more private than, for example, the financial information contained in the ‘checks, deposit slips, * * * financial statements, and * * * monthly statements’ the government acquired in Miller. 425 U.S. at 438… That analysis applies with even greater force here because, unlike in Miller, the records at issue here are not even copies of documents that petitioner submitted to the cellular-service providers, and the government did not require the providers to keep those records. See \textit{ibid}. Petitioner’s argument also overlooks the ‘core distinction’ between ‘the content of personal communications’ and ‘the information necessary to get those communications from point A to point B.’ ‘The business records here fall on the unprotected side of this line’ because they ‘say nothing about the content of any calls’ but instead contain only ‘routing information.’\textsuperscript{110}

\textsuperscript{108} Brief For The United States In Opposition,19.
\textsuperscript{109} Brief For The United States In Opposition,16.
\textsuperscript{110} Brief For The United States In Opposition,17-18.
Finally, the United States seeks to apply a balancing test for the Fourth Amendment. Under this argument, even were the Court, incorrectly, to grant privacy protection to the CSLI records of Mr. Carpenter, the government still would have committed a reasonable search under the Fourth Amendment.

“As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is ‘reasonableness.’” Maryland v. King, 133 S. Ct. 1958, 1969 (2013) (citation omitted). A “warrant is not required to establish the reasonableness of all government searches; and when a warrant is not required (and the Warrant Clause therefore not applicable), probable cause is not invariably required either.” Vernonia Sch. Dist. 47 v. Acton, 515 U.S. 646, 653 (1995).\footnote{111}

When Fourth Amendment cases arise which do not possess much if any guidance from the framers about the reasonableness of warrantless search the Court usually proceeds, “[b]y assessing, on the one hand, the degree to which it intrudes upon the individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interest.”\footnote{112}

Under traditional Fourth Amendment standards, petitioner had no legitimate expectation of privacy in the third-party business records at issue here. But even if this Court were to depart from that settled framework and hold that an individual can assert a Fourth Amendment interest in records created by a third party… petitioner could at most assert only a diminished expectation of privacy in those records. That is a factor that this Court has said ‘may render a warrantless search or seizure reasonable.’… And any invasion of petitioner’s assumed privacy interest was minimal, given the imprecise nature of the location information that could be inferred from the historical cell-site records at issue here… On the other side of the reasonableness balance, the government has a compelling interest… like other investigative techniques that involve seeking information from third parties about a crime, this evidence is ‘particularly valuable during the early stages of an investigation, when the police [may] lack probable cause and are confronted with multiple suspects… Society has a strong interest in both promptly apprehending criminals and exonerating innocent suspects as early as possible during an investigation.”\footnote{113}

\footnote{111} Brief For The United States In Opposition, 23. \footnote{112} Riley, slip op. at 9. \footnote{113} Brief For The United States In Opposition, 25.
VI. Are the Courts the Correct Branch to Resolve this Issue?

The case presented by both sides of Carpenter v. United States relies heavily on affirming, distinguishing, or refuting long-standing and recently decided cases issued by the Court. Both sides make compelling arguments about why the Court should decide this case in their favor; however, these are not the only two parties who are considering this important issue at the moment. As has been noted, some justices and legal scholars are not sure if the courts are the correct vehicle for deciding privacy of third-party records in the modern digital age. Many believe that it should be up to legislatures to conduct research and find out what Americans truly believe should be protected by privacy claims and what should not. The next chapter will focus on the legislative history of electronic privacy, mainly at the federal level, and will take a look at some of the proposals that are being considered by Congress in order to give adequate privacy protections to citizens in the modern technology age.
Chapter 3: Legislation and the Third-Party Doctrine

Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens.\textsuperscript{114}

There is no doubt among the Supreme Court Justices that times have changed, and the digital era requires updated privacy protections from the analogue generation; however, among the Justices it is not clear how this should be accomplished, or even which branch of government is best suited to provide a solution to this complex and constantly-evolving issue. Justice Alito in his concurring opinion in \textit{United States v. Jones} recognized that there many important issues presented by the clash of modern technologies and the Fourth Amendment. It is his position that the issues should not be resolved first by the Supreme Court, but rather that the legislature must perform the necessary research, in order to arrive at the required solution to this problem.

Justice Alito is not the only critic of today’s reliance upon the Court to resolve these thorny privacy matters. Many Fourth Amendment scholars believe that Alito’s call for a legislative solution is correct. On the other side of this issue, Justice Sotomayor made it clear in her separate concurring opinion in \textit{Jones} that it was time for the Court to reconsider its jurisprudence concerning the Fourth Amendment and its interaction with modern technology. Justice Sotomayor believes that it is up to the Court to reconsider the third-party doctrine and other interpretations of the Fourth Amendment and its applicability to cases involving technology. Her position is that the Court must reengineer its analogue jurisprudence to adapt to the modern digital era first \textit{before} Congress should attempt to address the inequality between police power

and citizen privacy. The change and adaptation of the Court’s precedents to modern times needs to come from the nine members of the Court and not the elected representatives in Congress.

I. History of Congressional Electronic Privacy Statutes

The previous chapters explained how the Court has arrived at its current case, Carpenter v. United States, and the potential privacy implications it presents. However, to understand all of the implications of this case one must understand the congressional legislation they produced that coincide with the Court decisions. This chapter will focus on the congressional legislation that has been enacted, from the analogue protections of the Electronic Communications Privacy Act (ECPA) to the many updates and amendments to the ECPA, such as the Telecommunication Act of 1996. The chapter will also discuss the competing arguments about whether the Court or Congress can best resolve the issue. The positions of both legal scholars and Justices Alito and Sotomayor will be carefully analyzed.

Before turning to this discussion relevant congressional legislation will be considered. The first Act of Congress that must be understood is the combined Electronic Communications Privacy Act and the Stored Communications Act, which are commonly grouped together as the ECPA. The ECPA was passed in 1986, and was an update of the 1968 Federal Wiretap Act. The Federal Wiretap Act of 1968 dealt with intercepted conversations that occurred using “hard” telephone lines. The updated ECPA was Congress’ first attempt to provide protections not only for wire and oral conversations, but also for new (at the time) electronic communications such as email and stored electronic data. Congress understood in 1986 that there needed to be greater privacy protections for citizens than just from “hard” communications.

\[\text{115} \text{ Electronic Communications Privacy Act, 18 U.S.C. § 2510-22.}\]
\[\text{116} \text{ Stored Communications Act, 18 U.S.C. § 201-12.}\]
\[\text{117} \text{ The Federal Wiretap Act, 18 U.S.C. § 2510-22.}\]
via the telephone. Changing technology dictated to Congress that there needed to be changes to
the privacy protections citizens had, but at the same time the protections could not be so all-
encompassing that they would hinder the ability of law enforcement officers to use the new
technology to do their jobs in the most effective manner possible. “By enacting ECPA, Congress
weighed different public interests. The House report noted that the ECPA measure ‘represents a
fair balance between the privacy expectations of citizens and the legitimate needs of law
enforcement.’”

The ECPA represents an extremely challenging issue for Congress, and one that has only
become harder as technology has become more and more advanced. On the one hand, Congress
must grant citizens their required expectation of privacy that was laid out in the Katz test. On the
other hand, Congress must give law enforcement the procedures and tools that will allow them to
do their jobs in the most efficient and proper way possible. When the only way to communicate
with people was through written messages, telephone communications, and face-to-face
conversations, the Wiretap Act of 1968 was perfectly suited for that analogue era of technology.
Now with new forms of technology appearing seemingly daily, and new platforms for
communication being utilized every hour, it is clear that the Wiretap Act of 1968 is no longer
sufficient. Consequently, the original ECPA of 1986 must be constantly reviewed and amended
to suit modern times. However, questions remain regarding how should Congress update the
ECPA to make sure it will pass the balancing test laid out above. Another question is whether
Congress is the most appropriate governmental branch to maintain the constantly changing
equilibrium between privacy and police power in the digital age?

118 Kevin V. Ryan and Mark L. Krotoski, “Caution Advised: Avoid Undermining the Legitimate
Needs of Law Enforcement to Solve Crimes Involving the Internet in Amending the Electronic
Communications Privacy Act,” University of San Francisco Law Review 47, no. 2, (Fall 2012):
A. Title I of the ECPA

The ECPA is broken up into three distinct sections, referred to as “Titles.” Title I is most commonly known as the Wiretap Act, and--is the amended as of 1986 version--of the Wiretap Act of 1968. Title I “prohibits the intentional actual or attempted interception, use, disclosure, or ‘procure[ment] [of] any other person to intercept or endeavor to intercept and wire, oral, or electronic communication,’”119 except when a proper order from a magistrate has been given to law enforcement. Title I does not say that a warrant, backed by probable cause, is required to obtain this information. Rather, it stipulates that a court order from a judge must be obtained in order for this information to be obtained or attempted to be obtained. Here Congress is seeking to prevent law enforcement from going on a “witch hunt” and surveying all calls and conversations made by each individual. Instead, Congress is simply requiring law enforcement officers to have sufficient evidence to convince a judge that compromising the privacy of a certain citizen or citizens is likely to yield evidence of criminal activity. This balances the need of law enforcement to obtain this information with the citizen’s privacy interest by having the protection of a third-party magistrate, who ensures that the law enforcement officers are looking with some degree of likelihood of finding evidence. Although a warrant backed by probable cause is not required by Title I of the ECPA, Congress still requires that a judge approve the information and order.

B. Title II of the ECPA

Title II of the ECPA is called the Stored Communications Act (SCA). Title II “protects the privacy of the contents of files stored by service providers and of records held about the

It is not limited to information such as a subscriber’s name, billing records, or IP addresses, and it covers issues such as Cell Site Location Information (CSLI), and the thousands of data points that come from that form of data stored by a third party. This type of CSLI data, obtained by the government with a 2703(d) order, is the data in question in the Carpenter case. Just as with Title I of the ECPA, the government must obtain a magistrate’s order, but is not required to obtain a warrant backed by probable cause, to be able to obtain stored records that fall under the purview of the SCA. Again, this plays into the balancing test that Congress required when considering the privacy of citizens, and the ability of law enforcement to effectively do their jobs. The absence of a warrant requirement is one of the main issues that the Court will have to either address themselves or hold appropriate for a legislative solution.

The SCA is becoming increasingly crucial as a result of the massive and constantly growing amounts of information third parties such as cellphone providers, television providers, internet search engines, and social media websites maintain and store about each individual’s preferences, browsing and user history. All of this information is available to the government, without a warrant backed by probable cause what is required is to merely show a judge there is enough reasonable suspicion for a subpoena. Nearly every person gives information to a third party in some capacity in the digital age. That information is then being stored and used by companies in ways never before possible. This depth of information, such as the 127 days of CSLI data in Carpenter that can be obtained by the government without a warrant, brings into

---

question the balance between citizen’s privacy and the ability of law enforcement to do their jobs under the ECPA.

C. Title III of the ECPA

Title III of the ECPA was created to address the issue of “pen registers,” like the one used in Smith v. Maryland, and tap and trace devices. This last Title of the ECPA “requires government entities to obtain a court order authorizing the installation and use of a pen register… and/or a trap and trace… The order can be issued on the basis of certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation.”\(^{121}\) This part of the ECPA clearly shows how the legislature can play a critical role in solving this problem of technology in the digital era, especially when data and information is given to third parties in an involuntary manner, required by society. Title III was enacted as part of the ECPA as a direct result of Congress’ disagreement with the decision in Smith. The objective was to mandate additional protections when it comes the government’s use of trap trace devices, and more specifically pen registers.

For example, in response to Smith, Congress enacted the Pen Register and Trap and Trace Devices Statute… However, the Pen Register statute makes it a crime to install a pen register without a court order, subject to some exceptions. Obtaining a court order is quite easy under the statute: Investigators need only certify that ‘the information likely to be obtained ... is relevant to an ongoing criminal investigation.’ But this still imposes a good faith test: The law requires an actual ongoing investigation and a good faith belief in the likelihood that evidence to be obtained is relevant to that investigation.\(^{122}\)

II. Statutory Response to Smith and Miller

This legislative response to the Smith decision, which held that individuals had no reasonable expectation of privacy in information given to third parties—specifically the phone numbers they


\(^{122}\) Kerr, “The Case for the Third-Party Doctrine,” 596.
dialed—was one that does not place a significant burden on law enforcement to obtain the information. Meanwhile Congress put in a reasonable safeguard to ensure that law enforcement was not simply fishing in random people’s phone records. The ECPA, and more specifically Title III, are not the only measures that Congress has taken to ensure that people have more protections in private information they give to a third party.

Congress also enacted the Right to Financial Privacy Act (RFPA) in response to the Miller case. In Miller the Court held that once financial information or any information had been given to a third party such as a bank, the customer or individual lost all expectations to privacy, and all privacy protections. Congress limited the scope of the Miller decision when it passed the RFPA.

RFPA responds to Miller by limiting government access to ‘the information contained in the financial records of any customer from a financial institution’ where the Fourth Amendment, thanks to Miller, does not. Under RFPA, the government can obtain such financial records with a subpoena only if the government has ‘reason to believe that the records sought are relevant to a legitimate law enforcement inquiry’ and the government first provides the suspect with prior notice of the planned action that gives him an opportunity to move to quash the subpoena.\(^{123}\)

Congressional response to Miller provides citizens with a stronger privacy protection in their financial information than in their phone numbers they have dialed. With respect to phone numbers, all the government must do is have a court issue an order that is backed by the likelihood that the information obtained will lead to evidence of crime. In the case of financial information held by a third-party, under the RFPA, the government not only must get a subpoena, but also must notify the individual that they are attempting to obtain the subpoena. This allows the individual time to file a motion to quash the subpoena before the records demanded by the order are ever handed over to the government. While both of these responses to the third-party doctrine’s foundation cases are strong indicators that Congress is capable of

vehicle for solving the issue of third-party information and law enforcement’s access to it in the
digital age, neither of these acts provide that the government must satisfy the higher standard
required for a warrant before obtaining third party information.

III. Additional Statutory Exceptions to the Third-Party Doctrine

Congress has not only enacted statutory privacy protections for citizens’ information given to
third parties (in the case of phone numbers dialed or financial transactions); it has also enacted
many other restrictions on the government attempting to collect certain types of information
from specific third party information collectors and holders.

The Health Insurance Portability and Accountability Act ("HIPAA") protects medical
records; the Privacy Protection Act restricts government access to third-party records held by
newsgathering organizations; the Video Privacy Protection Act provides special privacy
protections for video rental records; the Stored Communications Act restricts access to email
account records; and the Cable Act restricts access to cable account records. These laws all
impose statutory restrictions on access to records that the third-party doctrine leaves
unprotected under the Fourth Amendment.124

These are just a few of the examples where Congress has intervened legislatively and has raised
the privacy bar from unfettered government access to information voluntarily given to a third
party, to that of requiring a Court order or subpoena. Although most of the time these statutes
grant less privacy protections than a probable cause warrant required in other Fourth Amendment
cases, they still establish a higher privacy standard for individuals and their information given to
certain third parties than is required by the third-party doctrine.125 Many scholars agree with
Justice Alito that the legislature should decide, with statutes, on the privacy expectations of
society when it comes to the technology era and the third-party doctrine.

One of these scholars is Orin Kerr who believes, like Justice Alito, that these statutory
protections granted to citizens offer a strong remedy for the current issues presented by third-

party information in the technology age. Kerr also believes that the fact that most of these provisions provide for less privacy protection than a probable cause warrant. While at the same time maintaining an appropriate balance that Congress and or the Court must find, between an individual’s expectation of privacy in the digital age, and the restrictions to place on law enforcement trying to do their jobs as effectively as possible in the technology era. Kerr says,

In many (but not all) of these cases, the statutory privacy laws provide less protection than would the analogous Fourth Amendment standard of a probable cause warrant. But that is a good thing rather than a bad one. The fact that standards are low prevents the end-run around the balance of Fourth Amendment rules that outsourcing can permit. At the same time, the standards are substantial enough to make it quite unlikely that the police would use the investigative powers solely to harass innocent suspects. In the case of financial records, a suspect could move to quash the subpoena, which would provide a court audience to hear his complaint of government overreaching. And in the case of pen registers, the government must first go to a judge and seek an order, certifying under oath that an ongoing investigation exists and that the information collected is likely to be relevant. These intermediate standards deter wrongful abuse while permitting legitimate investigations. They strike a middle ground not possible under the Fourth Amendment. 126

In other words, Fourth Amendment case law could not achieve the required delicate balance as effectively as the statutory protections Congress is able to prescribe. The required middle ground can be reached, between the third-party doctrine giving the government free reign and unrestricted access to all third parties records, and a probable cause warrant as prescribed by the Fourth Amendment placing a substantial burden of proof on law enforcement trying to gather and obtain evidence for a case. This middle ground, according to Kerr, can be found by statutory protections and regulations implemented by Congress as new technology develops.

IV. The Telecommunications Act of 1996

The final piece of legislation that plays a role in the Carpenter case, and in the future of third-party doctrine, is the Telecommunication Act of 1996. The original Telecommunications

---

Act was passed in 1934. As can readily be imagined, it is not adequate either in terms of the privacy protections it provides or technology and scope of the laws it covered. The 1996 Telecommunications Act did not have as its primary purpose the updating of privacy protections for individuals or the third-party doctrine and its application to modern technology and society. Instead, its intent was “to let anyone enter any communications business—to let any communications business compete in any market against any other.”¹²⁷ The Act, however, has two sections that could play a crucial role in the decision in the Carpenter case, and how Congress will deal with the evolution of technology and privacy law in the coming years. The two sections, 47 U.S.C. §§ 222(c)(1)-(2) and (f), provide that information given to a telecommunications company such as an internet, cellphone, or television provider, is proprietary to the customer, and will require the explicit consent of the customer before it can be given to anyone, including the government.¹²⁸ This may seem as though there is no question left by section 222 that the information belongs to the customer to decide who may have it, when they may have it, and how much information they may have. In fact, the sections comes with a caveat which says, “Except as required by law,….”¹²⁹ This exception is the crux of the Telecommunications Act argument in Carpenter. As it stands now, the 2703(d) Order used by the government to require cell phone companies to turn over certain types of information, including CSLI data, is required by law. This is being challenged by Mr. Carpenter, who argues that section 222 means that information such as CSLI data, which is collected by cell phone carriers, is in fact his personal property and therefore is part of his private papers. As a result of

this property-based approach, the same approach used by the majorities in *Olmstead* and *Jones*,
the information protected by sections 222 of the Telecommunications Act is the papers of the
customer. Therefore these records are subject to Fourth Amendment protections, meaning a
warrant backed by probable cause is required, regardless of what the reasonable expectations of
privacy analysis would dictate. And even more importantly, since the information is property
belonging to the customer and is not simply information given to a third party, the third-party
doctrine is not relevant and cannot be used.

In addition, obtaining CSLI records invades an individual’s Fourth Amendment right to
security in his private ‘papers.’ Federal law grants individuals a proprietary interest in their
CSLI records by prohibiting service providers from disclosing that information without
‘express prior authorization of the customer.’ 47 U.S.C. § 222(f). Wholly apart from the
reasonable-expectation-of-privacy analysis, the government’s impingement on that interest
for the purposes of gather-information constitutes a search.130

The Telecommunications Act of 1996 adds an entirely new concept into the mix of the
*Carpenter* case, because it is addition by subtraction. As a result of removing ownership of the
CSLI data from the cell phone carrier, and giving it back to the customer, the third-party doctrine
and the entirety of the government’s argument that the case should be decided on the same
grounds as *Smith* and *Miller* becomes moot and no longer relevant. Whether only Justice
Gorsuch is interested in this argument offered by Carpenter remains to be seen, but this small
part of the Telecommunications Act of 1996 could play a huge role in swinging how the Court
votes on the important third-party doctrine case *Carpenter*. This property-based approach that is
employed by originalists such as Justices Gorsuch and Thomas could provide two additional
votes in favor of Mr. Carpenter. As will be discussed in the next chapter, Mr. Carpenter appears
to have a majority of the Court willing to rule in his favor, but for many different reasons.

---

130 Brief for Petitioner, 11.
Of course, Congress has enacted additional legislation that has raised or lowered the privacy standard for different types of law enforcement requests, but the ECPA of 1986 and the Telecommunications Act of 1996 are the major pieces of legislation not only in Carpenter, but also in the larger future of identifying that critical balance between a citizen’s expectations of privacy and the needs of law enforcement. Whether or not these acts are sufficient to solve the problems presented by technology in the digital era, and more specifically the questions that technology raises regarding the third-party doctrine, has been hotly debated among scholars.

Opponents of the view espoused by Professor Kerr believe that it is up to the Court to resolve these issues. He argues that because the Court created the third-party doctrine, and since Congress does not currently seem to able to pass legislation, the Court must be proactive and take cases that will help settle this issue as quickly as possible. Some theories also include the Court taking cues from the legislation passed by Congress in order to better reflect the expectations of society as a whole when it comes to privacy in the digital era. The following part of the chapter will discuss the reasons why scholars believe that the Court alone, or Congress alone, or some amalgamation of the two decide what to do about privacy standards, and more specifically the third-party doctrine, in the current technology era.

V. Legal Scholars’ Support for a Legislative Solution

Professor Kerr is one of the only scholars who champions the third-party doctrine in the digital age, and he supports a legislative solution. Kerr believes that the legislature is best equipped to handle the constant change in technology and the scope of the privacy protections that should be given to citizens, and the restrictions that should be placed on law enforcement’s use of the new technology. “Enthusiasm for judicial solutions overlooks significant institutional limitations of judicial rulemaking. Courts tend to be poorly suited to generate effective rules
regulating criminal investigations involving new technologies. In contrast, legislatures possess significant institutional advantages in this area over courts.” Kerr argues that legislation is the best option when it comes to being able to adapt, research, and produce the most balanced and thorough approach to the privacy issues raised by new technology, and its intersection with analogue precedents such as the third-party doctrine. The differences between the capabilities of the legislature and of the courts inform Orin Kerr’s belief that Congress is the appropriate arbiter of the clash between the new technology and individual privacy rights. However, other scholars such as Charles Maclean, agree with Kerr that in the modern technology age Congress is the more appropriate vehicle to settle this dispute, but present a distinct rationale.

In his article, “Katz on a Hot Tin Roof,” Maclean lays out why he believes that in an era of constant technological change the legislature is the best vehicle to reset the privacy bar to the appropriate height. While he acknowledges that the Court played a critical and positive role in the analogue era, he believes that the pace of technological change makes the Court less able to respond than Congress.

When technological change moved glacially before the digital age, it was sufficient for courts to serve as the line of defense for privacy rights. But in the digital age, technological advancement moves like the hare, and courts move like the tortoise, so we must now look to legislature, and particular Congress, to reset the privacy bar. Maclean harkens back to Justice Brandeis’ dissent in Olmstead, in which he pointed to “an ongoing need for such Congressional interventions lest technology diminish privacy to the

---


vanishing point.” He continues by using the ECPA as an example of congressional
recognition of the need to update the Act from 1986 and bring it into the twenty-first century.
The ECPA of 1986 has been unable to provide the necessary protections for the unforeseen shift
in the foundation of society created by the exponential expansion of the use and capabilities of
the internet. As a result, Congress saw the need to update the Act in order for it to maintain the
critical balance between citizen’s privacy and law enforcement powers. “By 2000, Congress had
witnessed more technological revolution, necessitating, in its view, the ECPA, adding electronic
communications to the oral and wire communications addressed in Title III, among other
changes necessitated predominantly by the Internet explosion.” This demonstrates that
Congress is capable of drawing the necessary lines, at the required times, to facilitate the proper
privacy protections for people, while the Court is only able to set the minimum standard of
acceptable privacy protections for citizens. “Courts can set, perhaps, the absolute floor as
constitutionally required, but Congress must decide where, above that floor, the privacy line
must be drawn.” Maclean continues with his ECPA example by demonstrating how Congress
updated the protections due to changes in society’s use of technology in 2013, verses its use of
technology in 2000,

Congressional intervention continued, as exemplified in the 2013 amendments to the ECPA. Congress expressed the need for additional safeguards in the digital age:

The Committee recognizes that most Americans regularly use email in their professional and personal lives for confidential communications of a business or personal nature. The Committee also recognizes that there is growing uncertainty about the constitutionality of the provisions in ECPA that allow the Government to obtain certain email content without a search warrant. The absence of a clear legal standard for access to electronic communications content not only endangers privacy rights, but also endangers the admissibility of evidence in criminal and other legal proceedings. Accordingly, the Committee has determined that the law must be updated to keep pace with the advances

133 Maclean, 74.
134 Maclean, 74.
135 Maclean, 74.
in technology in order to ensure the continued vitality of the Fourth Amendment protections for email and other electronic communications content.\textsuperscript{136}

Maclean then lays out why the institutional limits on the Court, such as having to look back at precedent, while Congress can look forward to solve issues presented by current technology, makes Congress the correct body in order to solve these issues.

Left to their own devices, courts are compelled to look back at precedent to resolve the disputes of tomorrow. Congress, on the other hand, looks forward to reset the privacy bar in the digital age. The paradigm is set; society must look to Congress to redefine what should and shall be private in the future, rather than waiting for courts to force-fit new technologies into outmoded precedential analogies.\textsuperscript{137}

Although his reasons are different, Maclean fundamentally agrees with Kerr that Congress is the correct arbiter of privacy protections and law enforcement restrictions when it comes to technology, and obtaining data from a third party in the digital era.

The amount of information now stored with third party Internet companies have produced a qualitative change in the nature of communications and, accordingly, in the nature and amount of the information that may be exposed to interception by the government. In light of these developments, existing statutes should be updated to appropriately balance the concerns of law enforcement—namely, the concern that they have sufficient authority to obtain the information they need in order to keep the public safe—with individuals’ concerns that a sufficient degree of privacy and the integrity of personal information are maintained in an age of modern communications and information storage.\textsuperscript{138}

Justice Alito, along with many scholars, shares the position that Congress is the correct institution to remedy the wrongs of current privacy law. In addition, Alito believes that Congress can best set standards for electronic privacy, including data collected and given to third parties in the future. Justice Alito in Jones understood and acknowledged that technological innovation has dictated that change to privacy laws must be made, but he said that Congress was the branch of government that had to do this.

\textsuperscript{136} Maclean, 75.
\textsuperscript{137} Maclean, 76.
\textsuperscript{138} Maclean, 75.
VI. Legal Scholars’ Support for a Judicial Solution

Although she sided with the other eight members of the Court in *Jones*, Justice Sotomayor believes that the Court has to be the governmental branch that begins solving the issues that technology raises in terms of citizen privacy and law enforcement efficiency. In her concurring opinion, she argues,

More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties…I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.139

Legal scholar Paul Ohm, believes that in order for the issue of technology and privacy to be solved, the Court must reshape the way in which it thinks about Fourth Amendment cases. Ohm’s belief is based upon the fact that privacy is diminishing, if not dying, within society, and, as a result, the Court must switch thinking about the Fourth Amendment from the *Katz* reasonable expectation of privacy test to the balance of power between police power and individual’s privacy interests. “The end of privacy disrupts the rules we use to give action to the amendment, and we must shift away from *Katz*’s reasonable expectation of privacy to rules that focus instead on the balance of power between the police and the people.”140 Achieving this equilibrium between police power and citizen privacy can only be accomplished through changing the way the Court approaches Fourth Amendment precedents and future cases. Ohm believes that the effective utilization of warrants based upon probable cause is an aspect of the equilibrium adjustment equation; however, it is by no means a solid solution that will keep the precarious balance between police power and citizen privacy stable. He contends,

139 United States v. Jones 565 U.S. 400,417-418 (2012), (Sotomayor, J., Concurring)
140 Ohm, 1334-1335.
Equilibrium adjustment can help judges determine whether to turn the Fourth Amendment’s tuning knobs to restore the level playing field. But it will not do enough to safeguard liberty from undue governmental power unless we also add a few new tuning knobs. A new Fourth Amendment designed to enforce the level playing field must address the misconception that the warrant and probable cause requirements represent the high water mark, the most onerous and liberty-protective things that may be imposed on the government. The very development that brought us to this point, the rise of the surveillance society, instead reveals that the warrant and probable cause requirements are often quite toothless requirements that the government will be able to meet with ease.\(^\text{141}\)

According to Ohm, the equilibrium that has to be achieved in the modern digital era will require the Court to reconstruct the foundation upon which privacy protection is built. The analogue precedents that the Court relies upon, such as *Katz*, *Smith*, and *Miller*, are neither compatible with modern technology, nor are they the foundation of Fourth Amendment protections. The Fourth Amendment must be given an upgrade, a modernization, and this requires laying a new foundation upon which technology and privacy can be kept in equilibrium. The Court must balance police power and citizen privacy by establishing this new foundation on new footings, not based on analogue era precedents of reasonable expectations of privacy, or whether information has been given to a third-party.

For nearly fifty years, privacy has served as a useful proxy for deciding what the Fourth Amendment protects. As we witness the rapid decline of privacy, we should be prepared to rebuild the Fourth Amendment on a new foundation focused on the balance of power between the state and its citizens.\(^\text{142}\)

**VII. Additional Arguments for a Judicial Solution**

There are two remaining arguments that favor the Court taking control of this issue and making sure that citizens have adequate privacy protections while still allowing the law enforcement officers to do their job to the best of their ability. The first argument is that the past decade Congress has become increasingly polarized, and as a result has become less productive

\(^{141}\) Ohm, 1347.
\(^{142}\) Ohm, 1353.
and able to reach much needed compromise on nearly every issue. This lack of productivity comes at a critical time when more and more aspects of individuals’ lives are online in the form of shopping, social interactions, and work. And in many of these aspects of their lives they have no choice but to interact with, rely upon, and give information to a third party. All of this information is going to third parties and can be accessed by the government without a warrant. Congress has not stepped in to address this issue because they cannot compromise and find the right balance. Congress’ inability to do their job has left people more exposed and vulnerable to abuses of law enforcement power through their information stored by third parties.

Given Congress’ recent lack of productivity, it seems unlikely that the legislative branch will step in to reshape the third party exception any time soon. At the same time, consumers are doing an increasing amount of business online, making more information available to third parties than ever before. Particularly as companies and individuals increasingly turn to cloud computing, putting even more information into the hands of third parties, the judiciary should revisit the third party exception sooner rather than later.143

The second part of the argument is that, even if Congress were able to pass legislation dealing with the third-party doctrine or new technology and privacy concerns, it would not be all-encompassing. This inability to reform this statutory area with any meaningful and fully comprehensive laws and procedures not only leaves citizens’ privacy unprotected, but also forces the Court to use the Fourth Amendment as both a constitutional measure and as a privacy safeguard to ensure the equilibrium is achieved and maintained. This part of the argument does not view the Court as the ideal vehicle to solve this problem; rather it views the Court and the Fourth Amendment as the only current way any change and protections will be added as a result of constant congressional stalemate.

---

In an ideal world, government information gathering would be regulated by a comprehensive statutory regime. Courts would analyze whether the rules in this statutory regime met basic Fourth Amendment principles rather than craft the rules themselves. A pronouncement as short and vague as the Fourth Amendment best serves as a guidepost to evaluate rules, rather than as a source of those rules. But a comprehensive statutory regime to regulate government information gathering does not yet exist. Statutes regulate government information gathering in isolated areas, but there is no all-inclusive regime. For better or worse, the Fourth Amendment has been thrust into the role of the primary regulatory system of government information gathering. Until there is a substitute, we should treat the Fourth Amendment as the regulatory system it has been tasked with being. If legislatures respond with rules of their own, courts should shift from crafting the rules to evaluating the rules made by legislatures.144

The legislative history of technology and privacy reveals that Congress reacts to the changes in society far too late, and not nearly often enough in order to provide the proper privacy protections for citizens, while at the same time balancing the ability of the police to do their jobs as effectively as possible. The final chapter will show how privacy doctrine in this area has evolved from the law review article written by Samuel Warren and Justice Brandeis, to the third-party doctrine cases of Smith and Miller, the ECPA, and the modern technology cases of Riley and Jones, culminating in Carpenter v. United States. This case should demonstrate how the Court is going to handle the issues of not only new technology and privacy rights, but also how the Court is going to apply the third-party doctrine in the digital age. The solution must make sure that law enforcement has the tools needed to do their jobs, but at the same time grant citizens the required digital protections, not subject them to analogue doctrines, in a digital age.

Chapter 4: Carpenter Oral Argument Analysis and Opinion Predictions

The Court remains the interpreter of the Fourth Amendment in our modern age. The government’s practice of obtaining cell phone location data without a warrant is out of step with the Court’s recent opinions. The Court can and should leave the work of ‘impos[ing] detailed restrictions on electronic surveillance’ to Congress, as it has done before... But the Court should first establish that the Fourth Amendment applies to cell phone location data.\(^{145}\)

The final chapter of this paper will provide an in-depth discussion of the oral argument in Carpenter v. United States, and will combine that analysis with the precedents discussed in this paper such as Olmstead, Katz, Smith, Miller, Jones, and Riley, in order to attempt to decipher how the Court will decide the case. The discussion will seek to deduce how each justice is thinking about the case based upon the questions and hypotheticals they posed to counsel for Mr. Carpenter (Nathan Wessler) and for the United States (Michael Dreeben) during oral argument.

I. Carpenter Oral Argument Analysis

While predicting how a case before the Court will be decided based solely upon oral argument can be a difficult task, the long line of precedents, combined with the questions asked by the justices, provide a strong indication of how each justice will vote, and how this case will be decided. Finally, based on the predicted outcome of Carpenter, the chapter will conclude with an analysis of how the Court and Congress need to work together in order to provide the proper legal and statutory solution to the issue of individual privacy, especially in information provided to third parties, in the modern technology era. Combining each justice’s positions and opinions from previous cases with their questions from oral argument gives a pretty clear picture

\(^{145}\) Brief for Electronic Privacy Information Center (Epic) et al. as Amici Curiae Supporting Petitioner, Carpenter v. United States (August 14, 2017) (No. 16-402) 38-39.
that “plainly the Court is much more concerned about the privacy implications of new technology today than it was five years ago.”

A. Justice Neil Gorsuch

Consider Justices Gorsuch and Thomas, who could not have taken more different approaches during oral argument. As usual, Justice Clarence Thomas was silent during oral argument. By contrast, Justice Gorsuch was an active and insistent inquisitor of counsel. While he has not authored many opinions on the Supreme Court, due to his short tenure, his opinion in the Tenth Circuit Court of Appeals case of United States v. Ackerman reveals how Gorsuch views and understands the government’s argument in Carpenter. In Ackerman, emails in transit that carried the electronic signature of possible child pornography were sent to and opened by the National Center for Missing and Exploited Children (NCMEC), without a warrant. In delivering the opinion for a three-judge panel on the Tenth Circuit, Judge Gorsuch first found that the NCMEC was a governmental entity, which therefore subjected it to the Fourth Amendment. He further stated that there could be no greater analogy between the physical papers the Framers sought to protect with the Fourth Amendment and the emails in the digital era. “Of course, the framers were concerned with the protection of physical rather than virtual correspondence. But a more obvious analogy from principle to new technology is hard to imagine and, indeed, many courts have already applied the common law’s ancient trespass…doctrine to electronic, not just written, communications.”


147 United States v. Ackerman, 14-3265, 33, (10th Cir. 2017). (The questions presented in Ackerman were, First does NCMEC qualify as a governmental entity or agent? And second did NCMEC simply repeat or did it exceed the scope of AOL’s investigation?)
In order to strengthen the comparison between the sealed letters and private papers the Framers sought to protect and modern electronic mail, Gorsuch applied the 1878 case *Ex Parte Jackson*, noting:

The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household.\textsuperscript{148}

When a letter is in transit to wherever its destination may be, the government must have a warrant in order to open the letter or package. In *Ackerman* the Court used *United States v. Jones*’ physical trespass doctrine, taken from the *Olmstead* case, in order to come to the conclusion that emails in transit were considered papers under the Fourth Amendment. Just like the protected physical sealed mail in *Ex Parte Jackson*, emails now garner the same privacy protection under the Fourth Amendment as their handwritten predecessors.

The Tenth Circuit continued analyzing the issue at hand by applying the trespass theory under *Jones*, analogizing unopened email attachments to sealed letters sent through postal services. The Court invoked a familiar analogy between physical mail and electronic mail, thereby easing the issue into a ‘papers and effects’ argument from the Fourth Amendment. The Court found that the warrantless opening and searching of private correspondence in the email was ‘exactly the type of trespass to chattels that the Framers sought to prevent when they adopted the Fourth Amendment.’\textsuperscript{149}

Justice Gorsuch’s opinion requiring the same Fourth Amendment protections for emails as physical papers, under the physical property trespass rule established in *Olmstead*, and applied in *Jones*, provides a strong indication that he may side with Carpenter under a property-based approach.

\textsuperscript{148} *Ex Parte Jackson*, 96 U.S. 727 (1878).

Further support for this conclusion can be found from Justice Gorsuch’s questioning during the oral argument in *Carpenter* during which he pressed both lawyers on the property-based approach aspects of the *Carpenter* case. He began his questioning of Mr. Dreeben, counsel for the United States, by stating, “You know, the facts here wind up looking a lot like *Jones*. One thing *Jones* taught us is -- and reminded us, really, is that the property-based approach to privacy also has to be considered, not just the reasonable expectation approach.”

After establishing this, Gorsuch moves on to use Section 222 of the Telecommunications Act, which provides that the customer has the right, because the information is the customer’s property, to decide to whom and when the information is given.

JUSTICE GORSUCH: Well, what does Section 222 do, other than declare this customer proprietary network information --

MR. DREEBEN: So that --

JUSTICE GORSUCH: -- that the carrier cannot disclose?

MR. DREEBEN: It -- it does that in conjunction with a provision that it shall be disclosed as required by law.

JUSTICE GORSUCH: So -- so, let me ask you that. So -- so the government can acknowledge a property right but then strip it of any Fourth Amendment protection. Is that the government's position? After establishing this, Justice Gorsuch asks Mr. Dreeben if Section 222 of the Telecommunications Act says that if this information is the property of the customer and they have the right disclose to whom they want, when they want it, then how can the Government confer a property right and then take away all Fourth Amendment protection that comes with it? Mr. Dreeben’s response is that the exception to the created property right is when, as required by law, the carrier must release this

---


information. In *Carpenter* the “as required by law” provision is the 2703(d) order for Mr. Carpenter’s CSLI information. Gorsuch continues to question Mr. Dreeben about the relationship between Section 222 and the Fourth Amendment.

JUSTICE GORSUCH: So the Fourth Amendment controls, not -- not what the statute says --

MR. DREEBEN: Well --

JUSTICE GORSUCH: -- with respect to the disclosure of the information?

MR. DREEBEN: -- the Fourth Amendment applies once the Court has identified what interest the statute creates.

JUSTICE GORSUCH: Right. The statute creates customer proprietary information--

MR. DREEBEN: Well, it --

JUSTICE GORSUCH: -- in Section 222 and then the Fourth Amendment will determine when it can be revealed. Right?

MR. DREEBEN: No. The statute actually creates --

JUSTICE GORSUCH: Why does the statute control the Constitution? I think you are saying the statute controls the Constitution.152

Justice Gorsuch and Mr. Dreeben have a final exchange about the Framers protecting against third parties searching anything in a colonist’s home under writs of assistance, and how that is analogous to what the government is doing in *Carpenter*. They are searching through the property—in this case, the CSLI data of the customers—with the only restriction on the government being the requirement that it obtain a court order based on less evidence than a warrant backed by probable cause.

JUSTICE GORSUCH: Mr. Dreeben, it seems like your whole argument boils down to if we get it from a third party we're okay, regardless of property interest, regardless of anything else. But how does that fit with the original understanding of the Constitution and writs of assistance? You know, John Adams said one of the reasons for the war was the use by the

government of third parties to obtain information forced them to help as their snitches and snoops. Why -- why isn't this argument exactly what the framers were concerned about?

MR. DREEBEN: Well, I think that those -- those were writs that allowed people acting under governmental power to enter any place they wanted to search for anything that they wanted.

JUSTICE GORSUCH: Isn't that exactly your argument here, that so long as a third party's involved, we can get anything we want?

MR. DREEBEN: Well, I think the search is being carried out under a writ of assistance by a government agent, operating under government authority; whereas here, we -- the -- if there's a search in the acquisition cell site information, then it's the cell site company that is acquiring that information without governmental instigation, without --

JUSTICE GORSUCH: The subpoena --

MR. DREEBEN: -- governmental agency --

JUSTICE GORSUCH: -- being, though, the equivalent of a writ of assistance?

MR. DREEBEN: Oh, I don't think a subpoena is an equivalent of a writ of assistance. A writ of assistance allowed the agent to go into any house, to rip open anything looking for contraband, no limitations.

JUSTICE GORSUCH: Yeah. And you can subpoena anything that any company has anywhere in the globe regardless of any property rights, regardless of any privacy interests, simply because it's a third-party?

MR. DREEBEN: So I -- I think that, as Justice Alito was explaining, there is a traditional understanding that dates back to the time of the founding that subpoenas stand on a different footing from search warrants. And they do that because they are less intrusive, since they do not require the government going into private property and searching itself.153

It is clear from his decision in *Ackerman* and his questioning at oral argument that Justice Gorsuch understands not only modern technology, but also the privacy concerns that new technology raises. He takes a keen interest in the property-based approach that finds its roots in *Olmstead* and *Jones*, and in Section 222 of the Telecommunications Act in this particular case. Gorsuch is not the only justice on the Court who may take a property-based approach to the

---

"Carpenter" case. Justice Clarence Thomas could also decide this case under the same line of thinking, but may not extend the potentially expansive privacy rights that Justice Gorsuch maybe inclined to.

**B. Justice Clarence Thomas**

Justice Clarence Thomas has a well-known, extremely judicially conservative philosophy: "Thomas is a great deal more conservative than his colleagues, and arguably the most conservative Justice to serve on the Supreme Court since the nineteen-thirties." This philosophy Justice Thomas often shared only with the late Justice Scalia; however, with Justice Gorsuch now on the Court, Thomas may have gained a new partner on the far right. Due to this philosophy, Justice Thomas often writes separately or is dissenting. His conservative judicial philosophy, combined with his support for the majority opinion in *Jones*, which was based upon the physical trespass doctrine, indicates that he may take the same property-based approach in this case as Gorsuch may. With no hints, as always, from Justice Thomas during oral argument, his voting record and judicial philosophy are the only clues to how Justice Thomas will vote. Although Justice Gorsuch seems willing to extend great privacy protection to new technology under the property-based approach, Justice Thomas’ voting history and judicial philosophy make it unlikely he will extend privacy protections as far as Justice Gorsuch may.

**C. Justice Elena Kagan**

Moving away from the property-based approach, to one based on the sensitivity and intimacy of the information gleaned from the CSLI data, Justice Elena Kagan pressed Mr. Dreeben multiple times about how *Carpenter* is different than *Jones*. Justice Kagan, who signed onto

---

Justice Alito’s opinion in *Jones*, appears to side firmly with Mr. Carpenter for multiple reasons that stem from the rationale of *Jones*. Justice Kagan asks Mr. Dreeben how he can differentiate *Jones*, where the surveillance was held to be a violation of the Fourth Amendment, from the facts in Carpenter: they both involved collecting long-term 24/7 data on an individual, albeit employing differing means to obtain this information.

JUSTICE KAGAN: Mr. Dreeben, how is this different from *Jones*? You know, in *Jones*, there were a couple of different opinions, but five justices, as -- as I count it, said this -- this is from Justice Alito's opinion: ‘Society's expectation has been that law enforcement and others would not, and indeed in the main simply cannot, monitor and catalogue every single movement of an individual's’ -- there it was a car -- ‘for a long period.’ So how is it different from that?

MR. DREEBEN: I think it's fundamentally different, Justice Kagan, because this involves acquiring the business records of a provider which has determined to keep these records of the cell site information. *Jones* involved government surveillance. It involved attaching a GPS device to the car. Five members of the Court regarded that as a trespassory search. Five other members of the Court were prepared to analyze that under reasonable expectations of privacy. But in both cases, it was direct surveillance of the suspect in the crime.

JUSTICE KAGAN: So the question is why that should make more of a difference than the obvious similarity between this case and *Jones*? And the obvious similarity is that, in both cases, you have reliance on a new technology that allows for 24/7 tracking. Now, you're exactly right, there were different means, but in both cases, you have a new technology that allows for 24/7 tracking and a conclusion by a number of justices in *Jones* that that was an altogether new and different thing that did intrude on people's expectations of who would be watching them when.\(^{155}\)

Justice Kagan concedes that the means of collection in *Carpenter* is different but will not concede that the manner, detail, and length of time of the surveillance do not fall under the location protections established in *Jones*. Despite this concession Justice Kagan is not willing to concede that since the information is obtained from a third party that that means the privacy protections established in *Jones* no longer matter or carry any weight at all. In fact, she sees quite the opposite situation. She continues to push Mr. Dreeben about the length of time, and the

intimacy of the information that can be obtained currently and in the future should the Court rule in the United States’ favor.

JUSTICE KAGAN: Right. But, Mr. Dreeben, that could go away tomorrow. The question here is the constitutional question, not the statutory one. So can I take you back to what, it seems to me, is the essential identity between the factual circumstances here and in Jones, which is that the government is getting 24/7 information. I mean, in some ways, you could say this is more. Jones was just about a car; this is about every place that you are, whether you're in a car or not. And you said to me that what makes it different is that you've given the information to another person. But I recall that when you were here in the Jones case, your theory for why that was permissible was essentially that you had given that information to the entire public; in other words, just by being in the world, everybody sees you, everybody watches you, and you've lost your expectation of privacy in that way. Now, we pretty conclusively rejected that argument. Why is it different when it's giving it to one person, the same information, this 24/7 tracking, than we said it was when you give it to the entire world?

MR. DREEBEN: So I think that it is fundamentally different in the means that we chose to employ in Jones versus this case, and it's also different in what information we're acquiring. We did not acquire, in this case, 24/7 tracking of the precise movements of an individual everywhere he went. We acquired information of the cell tower where a call started –

JUSTICE KAGAN: But let's assume you could. Let's assume Mr. Wessler is right that the -- the technology keeps on getting better and better, more and more precise, it's not 10 football fields anymore; it's half of this courtroom. Next month, it may be an eighth of this courtroom. You know, so let's assume that we're looking ahead just a little bit and it's pretty precision-targeting.

MR. DREEBEN: So I would say that the third-party doctrine doesn't change. I also think that this Court could disagree and draw a line on more precise information that involves 24/7 tracking. This information is just simply far more similar to what was going on in the Smith case, where we got dialed phone numbers that would reveal a much more precise location where the dialed phone number came from and the person that was being spoken to. This case does not present the Court with the opportunity to decide the kind of granularity that Petitioner posits may happen in the future.156

The last exchange between Mr. Dreeben and Justice Kagan shows where she might come down in Carpenter. In addition, this last exchange hints at her position on the third-party doctrine in the digital age. She questions whether the United States feels as though simply because it

obtained a subpoena to acquire the CSLI data from a third party, the sensitivity and intimacy of the information CSLI data reveals should be inconsequential to the justices when deciding this case.

JUSTICE KAGAN: But -- but, Mr. Dreeben, that line of cases was developed in a period in which third parties did not have this kind of information, valid --

MR. DREEBEN: Not this kind specifically, Justice Kagan, but in the dissenting opinion in Smith, Justice Stewart warned that you're getting incredibly intimate information when you get the phone numbers of people who you have called. And I would submit that if the Court thinks about it, the information you get if you know who you are calling and the inferences you can draw about what kinds of conversations people are having are extremely sensitive with --

JUSTICE KAGAN: Yeah, but if --

MR. DREEBEN: -- dialed phone numbers.

JUSTICE KAGAN: -- I understand what you're saying, you're basically saying, well, because the government is going to a third-party here and doing it by subpoena, it doesn't matter how sensitive the information is. It doesn't matter whether there's really a lack of voluntariness on the individual's part in terms of conveying that information to the third-party. And we could go on and we could give, you know, other factors that you might think in a sensible world would matter to this question. And you're saying that all of that is trumped by the fact that the government is doing this by subpoena, rather than by setting up its own cell towers.157

Justice Kagan is hinting that in her mind the third-party doctrine is not applicable in the digital age, and she is looking not just at Carpenter, but the cases the Court knows will come in the years that follow regarding digital privacy.

D. Justice Sonia Sotomayor

Justice Sotomayor could not have been clearer where she stands about the third-party doctrine in the digital age in Jones, and she reiterated her desire for an expansive privacy protection ruling during oral argument.

Justice Sotomayor in *Jones* wrote:

More fundamentally, it 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 in 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.\(^{158}\)

As her opinion in *Jones* highlights, and as can be gleaned from her questions at oral argument in *Carpenter*, Justice Sotomayor strongly believes that it is time to overturn the third-party doctrine completely. For her, the analogue standard does not work in the digital era. The amount and depth of information people must give a third party to be a functioning member of society is far greater than anything that could have been imagined by the Court at the time of *Smith* and *Miller*.

The precision and wealth of information that third parties obtain from citizens, is an extremely pressing concern for Sotomayor that she drives home to Mr. Wessler during the *Carpenter* oral argument:

> Because right now we're only talking about the cell site records, but as I understand it, a cell phone can be pinged in your bedroom. It can be pinged at your doctor's office. It can ping you in the most intimate details of your life. Presumably at some point even in a dressing room as you're undressing. So I am not beyond the belief that someday a provider could turn on my cell phone and listen to my conversations.\(^{159}\)

Then when questioning Mr. Dreeben, she turns to her next concern about this third-party information, and its exponentially increasing role in technological development. How can the Court best prepare for future cases involving privacy concerns and its inevitable clash with ever-evolving technology? She addresses the future of the third-party doctrine and of technology and the Fourth Amendment, again by giving a small nod to the precision and intimacy of information that can and will be available to third parties when she discusses the individual’s cell phone usage habits, and in particular young people:


JUSTICE SOTOMAYOR: Mr. Dreeben, why is it not okay, in the way we said about beepers, to plant a beeper in somebody's bedroom, but it's okay to get the cell phone records of someone who I -- I don't, but I know that most young people have the phones in the bed with them…

JUSTICE SOTOMAYOR: All right? I know people who take phones into public restrooms. They take them with them everywhere. It's an appendage now for some people. If it's not okay to put a beeper into someone's bedroom, why is it okay to use the signals that phone is using from that person's bedroom, made accessible to law enforcement without probable cause?

MR. DREEBEN: So, Justice Sotomayor, I will answer the question about cell phone location in a house, but I think it's important that the Court understand that this case involves very generalized cell sector information –

JUSTICE SOTOMAYOR: That's today, Mr. Dreeben, but we need to look at this with respect to how the technology is developing.160

Justice Sotomayor is ready and willing to overturn the third-party doctrine in a more expansive ruling, or at least begin to carve out exceptions, to the third-party doctrine as technology and privacy concerns evolve.

E. Chief Justice John Roberts Jr.

Chief Justice Roberts authored the Court’s decision in Riley, which held that the police needed a warrant to search the contents of a cellphone incident to an arrest. However, even more important than the holding itself in Riley, the Chief Justice declared that cellphones were not voluntary in modern life: “These cases require us to decide how the search incident to arrest doctrine applies to modern cellphones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.”161

161 Riley, slip op. at 8-9.
The *Riley* decision, although it does not deal directly with the third-party doctrine, carries weight in how the Court may view *Carpenter*. The Chief Justice understands the privacy implications of this case; however, he does not understand why Mr. Wessler would have the Court draw a line stating that twenty-four hours of CSLI data would be permissible. The Chief Justice views this case as having to deal with the clash between the analogue third-party doctrine precedent and the realities of the digital technology age.

CHIEF JUSTICE ROBERTS: I want to understand the -- the basis for the 24-hour, or however long you want it to be, exception. It seems to me if there's going to be protection extended to the information, it has to involve some compromise of the third-party doctrine, and if that is altered, I don't see why it wouldn't also apply to, you know, one day of information.

MR. WESSLER: So the -- the only other court to address this question is the Supreme Judicial Court of Massachusetts, which drew the line at six hours. We have suggested 24 hours because we--

CHIEF JUSTICE ROBERTS: Well, I don't understand. What is the line we're drawing? It seems to me the line is between information to which the authorities have access and information to which they don't. I don't know why we're bothering about a line between six hours, three weeks, whatever.\[162\]

Chief Justice Roberts believes that this is going to be a case where the Court may not be able to make a narrow ruling; rather, it is going to have to be pronounced and emphatic simply due to the facts and timing of the case. For the Chief Justice, it appears as though changes to the doctrines of the Court must be the result of *Carpenter*. Based on his ruling in *Riley* and his questions to Mr. Wessler, it appears that the Chief Justice believes that the third-party doctrine must be altered in some manner or overruled because the privacy concerns raised by the new technology outweigh the importance of the *Smith* and *Miller* precedents. Another major concern for Roberts is whether a warrant is required for the government to obtain this information from a cellphone, and this concern, too, stems from his opinion in *Riley*. He continues with his

discussion about the application of the third-party doctrine in the technology age when Mr. Dreeben states that individuals voluntarily give CSLI data and other information to third parties, fully knowing all this information can be kept and shared with the government.

MR. DREEBEN: I don't think I did say that, Justice Kagan, because there is an element here of voluntariness in deciding to contract with a cell company, just like there's an element of voluntariness in getting a landline phone and making calls, and there's an element of voluntariness in signing up for a bank account and using a debit card to purchase --

CHIEF JUSTICE ROBERTS: That --

MR. DREEBEN: -- everything in your life.

CHIEF JUSTICE ROBERTS: -- that sounds inconsistent with our decision in Riley, though, which emphasized that you really don't have a choice these days if you want to have a cell phone.163

Roberts is clear that the Riley decision holds considerable importance, in light of the Smith and Miller decisions, which held there is no reasonable expectation of privacy in information given voluntarily to third parties. While Roberts does not believe that this CSLI information is given voluntarily in any sense, it is not clear how far he is willing to go in terms of extending privacy protections remains to be seen.

F. Justice Stephen Breyer

Justice Breyer was somewhat enigmatic during oral argument. While his questions present few clues as to how he might write the opinion of this case, they did clearly show his understanding and appreciation for how technology has dictated a need for change to the Fourth Amendment privacy protections.

Justice Breyer has not written a major decision concerning privacy and new technology in the digital era, and his questions at oral argument were telling, but only to a certain extent.

They not only suggested his personal positions, but also offered details about the Court’s predicament in this situation. One quotation demonstrates the new territory that the Court must now cover as technology evolves: “This is an open box. We know not where we go.”\textsuperscript{164} The Court as Breyer sees it must adapt to the new technology because the technology has dictated that it must.

Justice Breyer appears to be on Mr. Carpenter’s side, but he is thinking ahead, as Justice Scalia did in \textit{Kyllo}, and Justice Sotomayor did in \textit{Jones}. Breyer details the difficult questions the Court is grappling with in trying to write the opinion in a case like \textit{Carpenter} that will have such a tremendous impact on numerous Fourth Amendment cases to come to the Court. “So where are we going? Is this the right line? How do we, in fact, write it? Not, you see, for location. I have less trouble with that. But where is it going? Can you say -- it’s a very open question, but I’m very interested in your reactions.”\textsuperscript{165} He understands that the CSLI data should be protected in this case, but he is trying to gauge what the decision would mean for the future privacy and technology cases. Does the Court have to overturn the third-party doctrine completely? Can it just carve out an exception for CSLI data? Or is there another solution that the Court should employ? Breyer is speaking to the complex and ever-changing nature of the technology that is at play in this case and that will be at play in future cases. While he appears to be on Mr. Carpenter’s side in this case, if he were to write the majority opinion or a concurrence, it will most likely be on far narrower grounds than some of his colleagues. He seems to want to have more cases come up, and more technology develop to see exactly how the Court should handle these situations. In addition, Breyer might establish this exception, then allow Congress to


implement a statutory framework. Then lower courts could deal with subsequent challenges in order to allow the Court more time to consider the issues raised by advancing technologies clash with police power.

**G. Justice Ruth Bader Ginsburg**

Another Justice who showcased the difficulty that the Court would have with drawing a bright line regarding when or how long 24/7 surveillance of a citizen would become a Fourth Amendment violation was Justice Ruth Bader Ginsburg. While she, too, has not written a major decision in this line of cases, she did seem to be firmly on the side of Mr. Carpenter and baffled, just as was Chief Justice Roberts, by the standard that Mr. Wessler was suggesting.

JUSTICE GINSBURG: Now, suppose what was sought here was the CSLI information for the day of each robbery, just one day, the day of each robbery. Does that qualify as short term in your view that would not violate the Fourth Amendment?

MR. WESSLER: So the -- Your Honor, the -- the rule we proposed would be a single 24-hour period, contiguous 24-hour period... So we don't think the Court needs to -- to draw a bright line here, to define exactly where the line between short and long term is, but as we -- as we pointed out in our reply brief.

Justice Ginsburg is trying to see what standard Mr. Wessler would like the Court to apply since, as was discussed in *Jones*, longer-term surveillance was a violation under the Fourth Amendment. Ginsburg is attempting to ascertain what is considered longer term and therefore an intrusion on Mr. Carpenter’s Fourth Amendment protections. The standard that Mr. Wessler produces, one single twenty-four hour period of CSLI data, highlights how difficult this decision could be if the Court attempts to find a bright line rule for the number of hours the government can obtain CSLI data without a warrant. It may have to be a sweeping “all-or-nothing” ruling in this case due to the nature of the technology and the 2703(d) order that are at odds here. This expansive type of decision is where Justice Ginsburg may land, since, as noted above, she was unsatisfied with Mr. Wessler’s attempt to draw the time line for CSLI data. She highlights one
of the main flaws with the single 24-hour standard that Mr. Wessler has put forth before the Court:

JUSTICE GINSBURG: Mr. Wessler, could we go back to my question? You said 24 hours roughly. So, if there were only one robbery, we could get that information, but now there are how many, eight? So we can't get it for eight, but we can get it for the one?

MR. WESSLER: So, Your Honor, we've suggested 24 hours. I think that the most administrable line, if the Court wishes to draw a bright line, would be a single 24-hour period. But this Court could -- could craft other reasonable ways to -- to draw that intentional line.

JUSTICE GINSBURG: Well, what if it's reasonable for one robbery one day, why wouldn't it be reasonable -- equally reasonable for each other robbery?\textsuperscript{166}

Although it appears that Ginsburg is firmly on the side of Mr. Carpenter, she is also strongly opposed to the rule of one continuous twenty-four hour period of permitted warrantless CSLI data gathering by the government. She does not see how that is applicable to many cases, even the one in carpenter where the different robberies occurred on different days.

\textbf{H. Justice Samuel Alito Jr.}

The final two Justices on the Court, Justice Kennedy and Justice Alito, are the only two who do not appear to at least lean in the direction of Mr. Carpenter; however, they may do so for different reasons. There are a few separate reasons why Justice Kennedy and Justice Alito may not decide the case in Mr. Carpenter’s favor. First, they both believe legislation, like the statutory frameworks discussed in chapter three, provide a better solution to the balancing problem of police power and individual privacy. The second reason is that neither justice seemed convinced by Mr. Wessler’s arguments that the information obtained from CSLI data is any more sensitive or intimate than the information obtained by the government in \textit{Smith} and \textit{Miller}. In addition, Justice Alito, who acknowledged in his concurrence in \textit{Jones}, that

technology has changed how and what privacy means in the digital age did so again at oral argument in Carpenter. However this is where his agreement with Mr. Wessler ends; he understands that technology has changed, but is not sure if that requires the Court to overturn in part or in full the third-party doctrine.

JUSTICE ALITO: Well, you know, Mr. Wessler, I -- I agree with you that this new technology is raising very serious privacy concerns, but I need to know how much of existing precedent you want us to overrule or declare obsolete. And if I could, I'd just like to take you back briefly to -- to Miller and ask on what grounds that can be distinguished. You don't say we should overrule it, and you had - you said the information here is more sensitive. We maybe could agree to disagree about that. I don't know. But what else? What -- on what other ground can Miller possibly be distinguished?

Justice Alito wants to know why, even though the technology in the cases is extremely different, the third-party doctrine, established in Smith and Miller, should not be used to decide this case.

One of the ways that Mr. Wessler attempts to do this is by distinguishing the level of sensitivity and intimacy in the information extracted from the CSLI data in Carpenter and the financial information obtained in Miller.

JUSTICE ALITO: How would you distinguish Miller?

MR. WESSLER: Miller involved more limited records, certainly they could reveal some sensitive information, but more limited records and, as this Court held, they were voluntarily conveyed in that they were created by the passing of negotiable instruments into the stream of commerce to transfer funds. What we have here is both more sensitive and less voluntary.

JUSTICE ALITO: Why is it more -- why is it more sensitive? Why is cell site location information more sensitive than bank records, which particularly today, when a lot of people don't use cash much, if at all, a bank record will disclose purchases? It will not only disclose -- everything that the person buys, it will not only disclose locations, but it will disclose things that can be very sensitive.

MR. WESSLER: I absolutely agree, Justice Alito, that the information in bank records can be quite sensitive, but what it cannot do is chart a minute-by-minute account of a person's locations and movements and associations over a long period regardless of what the person is doing at any given moment.

JUSTICE ALITO: Yeah, I understand that. But why is that more sensitive than bank records that show, for example, periodicals to which a person subscribes or hotels where a person has stayed or entertainment establishments -- establishments that a person has visited.\footnote{Oral Argument at 1:24 Carpenter v. United States, No. 16-402, (2017), https://www.oyez.org/cases/2017/16-402.}

Justice Alito is not sold on the idea that simply because the technology is more advanced, that means that the information revealed by it will be more sensitive than the information disclosed in \textit{Miller}.

\textbf{I. Justice Anthony Kennedy}

Immediately following this questioning from Justice Alito, Justice Kennedy enters the argument, clearly showing that he, too, is not accepting the argument that the information is more sensitive than that in \textit{Miller} simply because the technology is more advanced.

JUSTICE KENNEDY: Particularly because the information in the bank records that Justice Alito referred to are not publicly known. Your whereabouts are publicly known. People can see you. Surveillance officers can follow you. It seems to me that this is much less private than -- than the case that Justice Alito is discussing.\footnote{Oral Argument at 2:47 Carpenter v. United States, No. 16-402, (2017), https://www.oyez.org/cases/2017/16-402.}

Neither Justice Kennedy nor Justice Alito sees the distinguishing factor between the sensitivity of the information disclosed in \textit{Miller} and the sensitivity of the information disclosed in \textit{Carpenter}.

The next part of their questioning of Mr. Wessler is rooted in Justice Alito’s concurrence in \textit{Jones}, where he said that deciding cases like \textit{Carpenter}, where new technology collides with privacy interests, should be left to Congress to decide, not the Court. In \textit{Jones} Justice Alito said, “In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to
draw detailed lines, and to balance privacy and public safety in a comprehensive way.\(^{170}\)

Justice Kennedy used this idea to question Mr. Wessler about whether the Court should defer to the judgment of Congress, since Congress has passed many statutes regulating law enforcement’s use of new technology due to citizens’ privacy concerns.

**JUSTICE KENNEDY:** But your argument, as I understood it from the brief and I'm hearing it today, makes the Stored Communications Act and the 2703(d) order irrelevant. You don't even talk about it. In an area where we're searching for a compromise, where it's difficult to draw a line, why shouldn't we give very significant weight to the Congress's determination that there should be and will be some judicial supervision over this -- over -- over these investigations?

**MR. WESSLER:** Justice Kennedy, Congress enacted the Stored Communications Act in 1986 and amended it in relevant part in 1994. Three-tenths of 1 percent of Americans had cell phones in 1986, only 9 percent in 1994. There were about 18,000 cell towers in 1994. Today there are over 300,000. And --

**JUSTICE KENNEDY:** Well, you mean -- you mean the Act was more necessary when there were fewer cell phones?

**MR. WESSLER:** No, not -- not --

**JUSTICE KENNEDY:** It seems to me just the opposite.

**MR. WESSLER:** Not at all, Your Honor. My point is that Congress quite clearly was not thinking about the existence of and certainly not law enforcement interest in historical cell site location information. There is nothing in the historical legislative record for -- for the members of the Court who would look there to indicate any cognizance of these kinds of records. So --

**JUSTICE KENNEDY:** Well, again, my question is, you give zero weight in your arguments to the fact that there is some protection?\(^{171}\)

Thus, it appears that both Kennedy and Alito do not agree that the information at issue in *Carpenter* is any more sensitive than that at issue in the third-party doctrine foundation cases.

Nor do they appear to acknowledge that the Court is the proper venue for deciding the complex

---


issue of what to do with the third-party doctrine, and its relationship to the battle between the citizens’ privacy and law enforcement ability to do its job effectively and properly.

II. “This is an Open Box. We Know not Where We Go.”

Based on existing precedent and the questioning at oral argument, it seems clear that the Court is extremely concerned about the digital privacy implications involved in Carpenter; however, what those implications are, what actions needs to be taken, and by what governmental body remain uncertain. The final part of this paper will discuss the best solution that the Court should put forward in its opinion in Carpenter, not only as a solution to CSLI data, but also as a foundation for deciding future technology cases. In addition, Congress’ role in developing a complementary statutory framework with the Supreme Court decision will be addressed.

New technology presents both the Court and Congress with new privacy concerns daily, and this is why the solution to these issues must come from the Court and Congress working together. As was stated early in the chapter, Justice Breyer said at oral argument in Carpenter, “This is an open box. We know not where we go.” This quote provides a solid summary of where the Court is in dealing with the privacy concerns that technology presents, and where Congress is in terms of aiding members of the Court to find the balance between privacy interests of citizens and law enforcement’s ability to do their jobs in the most effective manner possible. The “open box” that Justice Breyer is referring to is technology and the issues it presents to the Court and to Congress in Carpenter. However, his statement

---

is not solely concerned with the technology -- the CSLI data – at issue in *Carpenter*. Rather it is looking beyond and into the ever-advancing technology, and the privacy cases that the new technology will bring before the Court.

Breyer is also pointing out that the Court has not dealt with modern technology and privacy concerns, such as those raised by CSLI data being obtained through the simple use of a court order, and, therefore, this is new territory that raises a completely new set of issues that neither the Framers nor the Court that decided *Smith* and *Miller* could have imagined. This one quote from oral argument encapsulates the grounds upon which this decision needs to occur. However, while *Carpenter* represents extremely valid and important privacy concerns, is not the correct vehicle for a sweeping and expansive Fourth Amendment ruling.

The technology is changing so fast, and the Court’s precedents are too far behind, for the Court to make a sweeping and expansive ruling without allowing time for Congress to play the critical fact-finding and research role. The Court understands that these questions must be dealt with now, because as Justice Roberts noted in *Riley*, “We expect that the gulf between physical practicability and digital capacity will only continue to widen in the future.”

Roberts is making the point that the Court understands that technology is only going to advance with each passing day.

Consistent with Justice Breyer’s concern, the Justices appear to understand the crossroads at which they stand when it comes to technology and privacy, and there are two options. Option number one is to rule expansively for Mr. Carpenter, by overturning *Smith* and *Miller*, and requiring a warrant backed by probable cause to obtain CSLI data. This type of ruling is ill-advised because it does not fully consider the future. This paper has discussed how the justices

---

174 *Riley*, slip op. at 18.
have, for the most part, been extremely forward-thinking about the technology that would be coming, beginning with Justice Brandeis in Olmstead:

The progress of science in furnishing the Government with means of espionage is not likely to stop at wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enable to expose to a jury the most intimate occurrences of the home.\textsuperscript{175}

Similarly, Justice Scalia’s opinion in Kyllo, discussing the use of a thermal imager to determine the heat signature of rooms inside of a man’s house, wrote, “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.”\textsuperscript{176}

\textbf{III. Expansive and Sweeping Privacy Decision v. Narrow and Cautious Decision}

All of these earlier technology decisions have considered the future, and allowed for the development of case law as the technology required, but overturning the third-party doctrine, and requiring a warrant for the obtaining of CSLI data would not allow for this. It would allow for the Court to override its own established practice in this area, and this type of preclusion has backfired on the Court before. In Miller and Smith, the Court took broad and expansive steps in the opposite direction by allowing government unfettered access to any information given voluntarily to a third party. Granted, the Justices deciding those cases could not have predicted CSLI data, but they could have taken a more cautious and narrowly drawn position when crafting the third-party doctrine. However, as a result of these decisions, Congress realized that the Court had made too sweeping and expansive a ruling. “In response to Smith, Congress enacted the Pen Register and Trap and Trace Devices Statute,”\textsuperscript{177} which required a Court order to install a pen register to obtain the numbers a suspect has dialed, and “In response to Miller, Congress enacted

\textsuperscript{175} Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting)
\textsuperscript{177} Kerr, “The Case for the Third-Party Doctrine,” 596.
the Right to Financial Privacy Act (‘RFPA’),”\textsuperscript{178} which limited government access to “The information contained in the financial records of any customer from a financial institution’ where the Fourth Amendment, thanks to Miller, does not.”\textsuperscript{179} The RFPA set forth standards and requirements in order to obtain financial information. When the Court has made expansive and sweeping decisions about the use of technology and the privacy interests that surround them, Congress has been able to limit the scope of the decisions through the legislative process, whereby, unlike the Court, it can conduct research and better understand the impact that technology is having on citizens in this country and their privacy interests.

This ability of Congress to react to the expansive and consequential decisions handed down by the Court in previous technology and privacy-based cases is the reason why the second option below is the correct answer. Not only is it the right answer to the questions presented in Carpenter but also in all of the technology based cases requiring the Court to balance Fourth Amendment privacy protections against law enforcement’s use of new technology to do its job.

The second option, and the one that the Court should adopt, will be one that has the Court rightfully outline the privacy parameters that the Fourth Amendment provides for, and will give Congress ample room to perform its legislative function. Chief Justice Roberts alludes to the fact that cases dealing with modern technology will require the balancing of privacy rights and the security that police are able to provide, and that some sacrifices have to made by citizens in order to obtain new, or retain old privacy rights as technology advances.

We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.\textsuperscript{180}

\textsuperscript{178} Kerr, “The Case for the Third-Party Doctrine,” 596.
\textsuperscript{179} Kerr, “The Case for the Third-Party Doctrine,” 596.
\textsuperscript{180} Riley, slip op. at 25.
This sentiment that there will have to be a trade-off between privacy and security was echoed by Justice Alito in *Jones*.

But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.\(^{181}\)

However, in *Jones*, Justice Alito made the opposite argument that new technology that can provide for better security from law enforcement will have to come at the expense of privacy instead of privacy coming at the cost of security, as Roberts said in *Riley*. The trade-off between security and privacy will require the input of the Court and Congress in order to balance these potentially competing interests in the most effective, fair and constitutionally sound way possible.

Under the second option, the Court should require law enforcement to obtain a warrant in order to acquire CSLI data, no matter how long the tracking period. No longer will a 2703(d) order be the standard; instead, a warrant backed by probable cause should be required, and as a result, *Carpenter* should result in another exception to, and not the overturning of, the third-party doctrine. This exception is based on several factors. First, the third-party doctrine is premised on individuals losing all expectations of privacy when information is voluntarily given to a third party.\(^{182}\) However, as a result of *Riley*, owning a cell phone is no longer viewed as voluntary in modern society. Chief Justice Roberts made it abundantly clear in that opinion that owning and using a cell phone was no longer a luxury or an option, but instead has become a requirement of everyday life. A standard whereby information voluntarily given to a third party loses all


privacy protections is no longer satisfied, since Riley states that owning a cell phone is no longer voluntary. “Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.”183 The location information in Carpenter, produced by a cell phone and retained by a third party, no longer should be accessible by government with a simple 2703(d) order.

The second reason why CSLI data should require a warrant is that the information obtained from CSLI data is far more revealing and intimate in nature than anything the Court could have imagined when the Smith and Miller decisions were written. The contents of modern cellphones, especially modern smart phones, will show every facet of a person’s life, from medical records, financial records, and information about the interior of their home. However, while the issue in Carpenter is simply the location information that the phone gives off when it pings cell site towers, this information is more intimate and revealing than the location information obtained in the Jones case. In Jones all the government could track was the whereabouts of Mr. Jones’ car, not his physical person. By contrast, in Carpenter, the CSLI data shows every place he has been, and not only his location, but even what floor of a building a person is on. Justice Sotomayor made the point at oral argument—people take their phones into public restrooms, dressing rooms, and even in the case of most young people, in bed with them at night.184 This CSLI data is infallible and incorruptible; and it is not at the mercy of human memory, or determined by the location of a suspect’s car. It is a detailed map of every movement a person has made inside and outside of his home. The intimacy of this information is in no way, shape, or form comparable to

---

183 Riley, slip op. at 19.
the information that was obtained in *Smith* and *Miller*. The technology involved in those cases simply obtained the numbers a person dialed, and the deposit slips from bank transactions. Those analogue era pieces of information do not in any way reveal what time one leaves one’s house for work every morning, what time one goes to lunch at the office, or where one eats, and they especially do not reveal what room one is in in one’s home.

The modern digital era location information showing every place a person has been, cannot be held to the same standard that the analogue third-party doctrine, intended for phone numbers and deposit slips from over four decades ago: “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.”¹⁸⁵ Cellphones are not a voluntary part of being a functional member of society in the digital age, and the information the CSLI data reveals about an individual cannot be compared to the miniscule amount of information that could be gleaned by the government in the original third-party doctrine cases. For these reasons the Court must carve out an exception to the third-party doctrine for CSLI information, and require that a warrant backed by probable cause be obtained by the government before it can obtain CSLI data, for any length of time on an individual.

While some may object and say that the statutory framework provided in the Telecommunications Act and Stored Communications Act clearly states that only a 2703(d) order is required to obtain this information, Congress is not the arbiter and interpreter of the Constitution. It is one of the oldest principles in America that the Supreme Court is the interpreter of the Constitution and, therefore, the Fourth Amendment. “It is emphatically the

province and duty of the judicial department to say what the law is." It is the duty of the Court to set the privacy standards that are required by the Fourth Amendment. Once the Court has set this standard, the second part of the solution to the questions raised by new technology, such as determining the actual societal expectations of privacy, and the trade-offs individuals are willing to make between security and personal privacy, can begin to be answered by a statutory framework created by Congress.

But Congress should follow the lead of the Court as new conflicts between law enforcement practices, emerging technology, and Fourth Amendment privacy protections emerge… (‘Privacy protection under the Fourth Amendment is first and foremost the responsibility of the courts.’). With the Court’s constitutional guidance, Congress can take its turn and enact privacy legislation “that draws reasonable distinctions based on categories of information or [] other variables.”

Congress will no doubt play an important role in finding the right balance between personal privacy and law enforcement needs. It can build upon the constitutional groundwork that the Court provides in *Carpenter* and the cases it will decide in the future. Congress is far better suited to deal with these questions, once the Court has decided the constitutional question, because is has a wide range of resources at its disposal that the Court simply does not.

Legislatures can call and conduct hearings, selecting the number and types of witnesses and experts who testify before them. Legislatures act in an overly prospective manner, not bound to the facts of circumstances of any particular case or controversy. Legislatures can hear from dozens, hundreds, or even thousands of ‘parties’ in the form of live testimony and submitted written comments. And legislatures can amend their earlier enactments whenever they like, and whenever circumstances change. Courts, on the other hand, are constrained by the evidence, witnesses, and experts proffered by the parties. Courts act retrospectively, seeking primarily to resolve the disputes before the.

More specifically, Congress is not limited by cases that are granted certiorari. Congress can identify a problem, research it, and try to find a solution, and it does not have to wait for an issue

---

188 MacLean, 71.
to come to it, as does the Court. The only restriction placed on Congress is the Constitution, and once the Court has decided the constitutional question, it is up to Congress to use its resources and capabilities to fix the remaining imbalance between personal privacy and law enforcement powers.

Congress has the capability to interview experts, and hear from citizens and other interested parties about what they expect in terms of privacy, and balance that with what law enforcement officials tell Congress they need in order to effectively do their job. This combination of a narrow opinion by the Court in *Carpenter* and Congress’ implementation of a statutory framework provides the most comprehensive and workable solution to the questions presented by modern technology in the digital age.

**IV. Conclusion**

This paper has detailed the case law, the scholarly frameworks, and the legislation leading up to one of the most important cases of the 2017-2018 Supreme Court term, and one of the most important modern Fourth Amendment decisions. If the Court should rule on expansive and sweeping grounds, overruling the third-party doctrine and requiring a warrant for CSLI data, that solution will be hailed as a great decision for citizens’ privacy, but it may come at the cost of citizens’ security. Congress may also decide that doing so would tip the scale too far in the direction of citizen privacy, and it may enact statutes designed to restore balance between police power and individual privacy. If the Court takes the proper, narrower approach, then it will give Congress and the Court sufficient time within which to evaluate, adapt, and apply the new Fourth Amendment laws to the changing technology.

The Court’s jurisprudence has come a long way from the time of *Olmstead* and the physical trespass doctrine, the time of *Katz* and the reasonable expectation of privacy test, the time of
Smith and Miller and the creation of the unfettered third-party doctrine, and the time of the statutory protections of the ECPA and the Telecommunications Act. The Court has arrived at the time of Jones, Riley, and now Carpenter. The Carpenter case presents, just as Riley did, a chance for the Chief Justice to write a unanimous decision even though some justices are likely to write concurrences. Chief Justice Roberts authored one of the most important cases decided during his tenure in the Riley decision, which revolved around cell phone privacy laws. The Chief Justice understands the real-world impact of the Fourth Amendment technology cases, and he is keenly aware of power that unanimous vote in Carpenter would carry.

From the analysis in this chapter it is clear that the Chief Justice may not have trouble reaching that unanimous decision for Mr. Carpenter, but his real challenge lies in the different approaches the Justices will take. If the Chief Justice keeps this opinion for himself or he gives the opinion to Justice Breyer he will most likely see multiple concurrences like the opinion from Jones. The approach the Chief Justice will take based upon the oral argument and past decisions will be one that Justice Breyer, Ginsburg, and Kagan will fully sign onto and endorse. In addition, depending on whether he requires the government to get a warrant before obtaining the CSLI data, he may receive the vote of Sotomayor in agreement with his judgment in the case, but not with his reasoning.

The same situation would play out if the opinion were handed to Justice Breyer. Should the Chief or Justice Breyer write the majority opinion there will be at least three separate and defined concurrences. The first will be written by Justice Gorsuch and will agree in the judgment for Mr. Carpenter, but he will base his reasoning on the property-centered approach to the Fourth Amendment. Justice Thomas would most likely sign onto at least part of Justice Gorsuch’s opinion, depending on how expansive the privacy protection granted by Justice Gorsuch will be.
The second concurrence would come from Justice Alito who would have Justice Kennedy sign on, most likely, in full to his concurrence. Justice Alito would write an opinion that would be extremely close to the one he wrote in Jones. While it would declare Mr. Carpenter had a reasonable expectation to privacy in his information, it would not go any further than this, because Justice Alito would write that this issue should be solved by a statutory framework put forth by Congress. The final concurrence would come from Justice Sotomayor who would agree with the outcome in favor of Mr. Carpenter, but would not agree in terms of the limited privacy protections granted to Mr. Carpenter. Justice Sotomayor suggests the third-party doctrine needs to be overturned because it is an analogue precedent that is still alive in the digital era. In addition, this analogue precedent will only become more and more inapplicable to modern society as technology becomes more invasive into people’s lives.

The Carpenter case sets the stage for the Chief Justice to build upon his digital privacy jurisprudence that he began in Riley. He understands the importance, the implications, and the consequences of digital privacy decisions, and he also understands he could play a defining role in laying the foundations in an area of constitutional law, digital privacy, that could last decades after he is no longer Chief Justice. In this respect, he is like Chief Justice Taft in Olmstead. The Court knows that technology will continue to change, evolve, and adapt to modern times, as will society’s expectations of privacy, and its willingness to make certain trade-offs, such as security in the name of personal privacy. Nevertheless as long as technology continues to evolve, and questions about how best to balance personal privacy and police power continue to be raised, it will be the Court’s “[p]urpose to consider whether the existing law affords a principle which can
properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is.”189

---

189 Warren and Brandeis, 197.
Work Cited

Cases

*Ex Parte Jackson*, 96 U.S. 727 (1878).


Law Review and Scholar Articles


Carpenter v. United States: Background, Briefs, and Oral Argument


Legislative Sources


