Searching the Clouds:
Fourth Amendment Rights in the Age of Cloud Computing

June 10, 2019
11:20 a.m. – 12:20 p.m.

Connecticut Convention Center
Hartford, CT

CT Bar Institute Inc.
CT: 1.0 CLE Credits (General)
NY: 1.0 CLE Credits (AOP)

Seminar Materials Sponsored by

LexisNexis®

No representation or warranty is made as to the accuracy of these materials. Readers should check primary sources where appropriate and use the traditional legal research techniques to make sure that the information has not been affected or changed by recent developments.
As a lawyer I must strive to make our system of justice work fairly and efficiently. In order to carry out that responsibility, not only will I comply with the letter and spirit of the disciplinary standards applicable to all lawyers, but I will also conduct myself in accordance with the following Principles of Professionalism when dealing with my client, opposing parties, their counsel, the courts and the general public.

Civility and courtesy are the hallmarks of professionalism and should not be equated with weakness;

I will endeavor to be courteous and civil, both in oral and in written communications;

I will not knowingly make statements of fact or of law that are untrue;

I will agree to reasonable requests for extensions of time or for waiver of procedural formalities when the legitimate interests of my client will not be adversely affected;

I will refrain from causing unreasonable delays;

I will endeavor to consult with opposing counsel before scheduling depositions and meetings and before rescheduling hearings, and I will cooperate with opposing counsel when scheduling changes are requested;

When scheduled hearings or depositions have to be canceled, I will notify opposing counsel, and if appropriate, the court (or other tribunal) as early as possible;

Before dates for hearings or trials are set, or if that is not feasible, immediately after such dates have been set, I will attempt to verify the availability of key participants and witnesses so that I can promptly notify the court (or other tribunal) and opposing counsel of any likely problem in that regard;

I will refrain from utilizing litigation or any other course of conduct to harass the opposing party;

I will refrain from engaging in excessive and abusive discovery, and I will comply with all reasonable discovery requests;

In depositions and other proceedings, and in negotiations, I will conduct myself with dignity, avoid making groundless objections and refrain from engaging I acts of rudeness or disrespect;

I will not serve motions and pleadings on the other party or counsel at such time or in such manner as will unfairly limit the other party’s opportunity to respond;

In business transactions I will not quarrel over matters of form or style, but will concentrate on matters of substance and content;

I will be a vigorous and zealous advocate on behalf of my client, while recognizing, as an officer of the court, that excessive zeal may be detrimental to my client’s interests as well as to the proper functioning of our system of justice;

While I must consider my client’s decision concerning the objectives of the representation, I nevertheless will counsel my client that a willingness to initiate or engage in settlement discussions is consistent with zealous and effective representation;

Where consistent with my client’s interests, I will communicate with opposing counsel in an effort to avoid litigation and to resolve litigation that has actually commenced;

I will withdraw voluntarily claims or defense when it becomes apparent that they do not have merit or are superfluous;

I will not file frivolous motions;

I will make every effort to agree with other counsel, as early as possible, on a voluntary exchange of information and on a plan for discovery;

I will attempt to resolve, by agreement, my objections to matters contained in my opponent's pleadings and discovery requests;

In civil matters, I will stipulate to facts as to which there is no genuine dispute;

I will endeavor to be punctual in attending court hearings, conferences, meetings and depositions;

I will at all times be candid with the court and its personnel;

I will remember that, in addition to commitment to my client's cause, my responsibilities as a lawyer include a devotion to the public good;

I will endeavor to keep myself current in the areas in which I practice and when necessary, will associate with, or refer my client to, counsel knowledgeable in another field of practice;

I will be mindful of the fact that, as a member of a self-regulating profession, it is incumbent on me to report violations by fellow lawyers as required by the Rules of Professional Conduct;

I will be mindful of the need to protect the image of the legal profession in the eyes of the public and will be so guided when considering methods and content of advertising;

I will be mindful that the law is a learned profession and that among its desirable goals are devotion to public service, improvement of administration of justice, and the contribution of uncompensated time and civic influence on behalf of those persons who cannot afford adequate legal assistance;

I will endeavor to ensure that all persons, regardless of race, age, gender, disability, national origin, religion, sexual orientation, color, or creed receive fair and equal treatment under the law, and will always conduct myself in such a way as to promote equality and justice for all.

It is understood that nothing in these Principles shall be deemed to supersede, supplement or in any way amend the Rules of Professional Conduct, alter existing standards of conduct against which lawyer conduct might be judged or become a basis for the imposition of civil liability of any kind.

—Adopted by the Connecticut Bar Association House of Delegates on June 6, 1994
Cody N. Guarnieri, Esq. partner at Brown, Paindiris & Scott, LLP

Cody N. Guarnieri is a trial attorney at Brown, Paindiris & Scott. His litigation practice focuses on criminal defense and personal injury litigation. In his criminal defense practice, Cody defends both adults and juveniles who are being investigated by law enforcement or prosecuted by the state of Connecticut or the United States of America. Cody also counsels clients in dealing with administrative agencies for professional licensing issues, including with the Department of Public Health, Connecticut Medical Examining Board, Connecticut Board of Examiners for Nursing, Department of Developmental Services, Department of Consumer Protection, Department of Children and Families, and others. Cody regularly works with investigatory and disciplinary staff at the many boards, commissions and agencies of the State of Connecticut.

Cody is a Presidential Fellow Emeritus of the Connecticut Bar Association and is currently the vice-chair of the Criminal Justice Section of the Bar Association. Cody is also the co-chair of the Criminal Justice Section of the Hartford County Bar Association ("HCBA") and was recently nominated and elected as a fellow of the Connecticut Bar Foundation ("CBF"). Cody is also a member of the Connecticut Criminal Defense Lawyers Association ("CCDLA"), the American Bar Association ("ABA") Criminal Justice Section, the National Association of Criminal Defense Lawyers ("NACDL"), the Connecticut Trial Lawyers Association ("CTLA"), the American Association for Justice ("AAJ") and the Litigation Section, Membership Committee and Medical Marijuana Committees of the Connecticut Bar Association. Cody also serves as the president of the Catholic Lawyers Guild of the Archdiocese of Hartford.

Cody was named a "New Leader in the Law" by the Connecticut Law Tribune in 2016. He has been invited to speak at seminars and panels, including the annual meeting of the Connecticut Criminal Defense Lawyers Association and the Connecticut Bar Association’s Connecticut Legal Conference as well as at continuing legal education programs held by the CBA and other organizations. Cody has been featured in the Practice Tips series of the Connecticut Bar Association. Cody is the author of the definitive Outline of Pretrial Diversionary Programs in Connecticut, which is distributed to and relied on by many private criminal defense attorneys, public defenders and prosecutors throughout the State of Connecticut.
# Searching the Clouds: Fourth Amendment Rights in the Age of Cloud Computing (CLC-B09)

## Agenda

Speaker: **Cody Guarnieri**, Brown Paindiris & Scott LLP

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:20 – 11:25 a.m.</td>
<td>Introduction to the topic</td>
</tr>
<tr>
<td>11:25 – 11:35 a.m.</td>
<td>Katz to Jones: Expansion and Contraction of the Reasonable Expectation of Privacy Test</td>
</tr>
<tr>
<td>11:35 – 11:55 a.m.</td>
<td>Carpenter v. United States and the Several Ways to Skin the Cat</td>
</tr>
<tr>
<td>11:55 – 12:00 p.m.</td>
<td>Survey of Post-Carpenter Fourth Amendment Thought</td>
</tr>
<tr>
<td>12:00 – 12:10 p.m.</td>
<td>Carpenter in Connecticut and Conclusion</td>
</tr>
<tr>
<td>12:10 – 12:20 p.m.</td>
<td>Questions</td>
</tr>
</tbody>
</table>
SEARCHING THE CLOUDS: FOURTH AMENDMENT RIGHTS IN THE AGE OF CLOUD COMPUTING
By Cody N. Guarnieri, Esq.

I. Introduction

There was a time when the proscriptions of the Fourth Amendment may have been more straightforward. The Fourth Amendment states that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no 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.” Of course, the Fourth Amendment was a component of the Bill of Rights, ratified by the States in 1791, largely as a response to the anti-federalists’ claims that the Constitution, ratified between 1787 and 1789, failed to adequately address personal freedoms and limitations on governmental power.

It was much clearer after the ratification of the Bill of Rights in the late eighteenth century, and into the nineteenth century, how the Fourth Amendment applied than it is today. In 1791 a government intrusion on persons, houses, papers and effects was, necessarily, physical in nature. That is, if the Government could be alleged to have unlawfully searched or seized a person or his houses, papers or effects, it would necessarily have required Government agents to trespass on the person’s property, to take possession of his physical belongings, to intrude on his private correspondence.\(^1\) However, the development of jurisprudence under the Fourth Amendment, as it twists and bends to address (or avoid) technological advancements in Government investigation methods have sacrificed clarity in favor of a very slow incrementalism.

As is apparent, the world today is a vastly different place than it was in 1791. Today, it is estimated that there are 224.3 million smart phones in the United States, and that number is expected to pass 270 million by 2022.\(^2\) That would represent more than eighty percent of the population.\(^3\) And of course, “smart” phone is, itself, becoming a misnomer. Modern smart phones are said to be “supercomputers” in your pocket with substantially more computing power than all of NASA when it put men on the moon in 1969.\(^4\) With this seemingly unbounded capacity, smart phones are obviously no longer merely for making calls and are, in fact, a primary form in which modern Americans “cloud compute,” whether they realize it or not.

It stands to reason that many smart phone users have the Facebook App to utilize that platform, considering that in October of 2018 Facebook reported that it services 2.27 billion

---

\(^1\) See In re Jackson, 96 U.S. 727, 733 (1878) (asserting that a warrant based on probable cause was necessary to search a letter in the mail).


monthly users.\textsuperscript{5} Twitter recently reported 126 million daily active users on its platform (Facebook reports 1.2 billion daily active users).\textsuperscript{6} However, are general cell phone users, or those with Facebook, Twitter, Google, Apple or other accounts generally, aware that “[c]ompanies like Google, Apple, and Facebook host private files and photos in the ‘cloud’ while maintaining a frighteningly detailed log of user activity, both on and off their sites. Emailing, tweeting, instant messaging, surfing, searching, liking, and downloading all create an inescapable trail of third-party records.”\textsuperscript{7}

Keeping with the Facebook example, it is also notable that Facebook’s servers, the basis for its “cloud,” include data centers in the United States, Sweden and Ireland.\textsuperscript{8} To this point, Google maintains data centers in eight countries, including Chile, Taiwan, Singapore, Ireland, Finland and Belgium.\textsuperscript{9} Thus, not only are user data for these social media sites stored and maintained by these companies, but they are also “pinging around a globally distributed network.”\textsuperscript{10}

In terms of the privacy danger this presents to the public, consider that “Facebook received 32,716 requests for information from U.S. law enforcement between January 2017 and June 2017. These requests covered 52,280 user accounts and included 19,393 search warrants and 7632 subpoenas.”\textsuperscript{11} Thus, here is only one example of the proliferation of cloud computing, or mobile cloud computing, and the corollary effect on the Government’s investigative efforts. This also represents the general expansion of another mobile service issue that was addressed by the Supreme Court in 2018, that of Cell-Site Location Information (“CSLI”) and the implications for Fourth Amendment jurisprudence. As the Supreme Court notes in Carpenter v. United States, “a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner.”\textsuperscript{12} Moreover, the Court also draws a concern about what the CSLI actually means, in practical terms, when Chief Justice Roberts writes that “[w]hile individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.”\textsuperscript{13}

Thus, this introduction started with a hint of the uncertain future of the problem, the inevitability of the proliferation of cloud computing, perhaps even unwitting cloud computing for many users, and the need to address the same from the Fourth Amendment perspective. However,

\begin{itemize}
\item \textsuperscript{7} Michael Price, Carpenter Versus the United States and the Future of the Fourth Amendment, THE CHAMPION, June 2018, at 48.
\item \textsuperscript{8} Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance, 131 HARV. L. REV. 1722, 1733 (2018).
\item \textsuperscript{9} Id. at 1733.
\item \textsuperscript{10} Id.
\item \textsuperscript{11} Id. at 1722.
\item \textsuperscript{12} 138 S. Ct. 2206, 2218 (2018).
\item \textsuperscript{13} Id.
\end{itemize}
to better understand that issue, it is important to understand the underpinnings and development of Fourth Amendment jurisprudence leading up to Carpenter.

II. *Katz* to *Jones*: Expansion and Contraction of the Reasonable Expectation of Privacy Test

Leading up to the mid-twentieth century, Fourth Amendment jurisprudence had been inextricably tied to common law property language and concepts.\(^{14}\)

The modern watershed case in Fourth Amendment Jurisprudence, which still reverberates through all of the Court’s Fourth Amendment decisions to this day, is the 1967 decision of *Katz v. United States*.\(^{15}\) Justice Potter Stewart wrote for the majority and the issue presented in that case is whether there was a Fourth Amendment violation where law enforcement placed a recording device in the *outside* of a public telephone booth that was used by the defendant (in the course of his alleged bookkeeping business).\(^{16}\) While the parties focused on whether the telephone booth was a “constitutionally protected place,” the court’s decision went in a different direction, indicating that “the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”\(^{17}\) Without putting a fine point on the test that this case would become known for, later jurisprudence would accept that in this case the Court generally divorced the Fourth Amendment inquiry from whether a *physical trespass* (i.e. trespass doctrine) was controlling.\(^{18}\)

Put another way, the *Katz* majority held that whether a physical trespass by the government occurred was not determinative,\(^{19}\) but that *Katz*, having occupied a telephone booth, shut the door behind him, and paid to make a call, entitled him, under the Fourth Amendment, to believe that his call would not be “broadcast to the world.”\(^{20}\) The *Katz* court concludes that “the Government’s activities in electronically listening to and recording the petitioner’s words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a ‘search and seizure’ within the meaning of the Fourth Amendment.”\(^{21}\)

Both interestingly, and as a source of conflict in later decisions, the standard espoused in *Katz* in further decisional law comes not from the majority decision, but from the concurrence authored by Justice John M. Harlan, II, when he writes “[m]y understanding of the rule that has


\(^{15}\) 88 S. Ct. 507 (1967).

\(^{16}\) Id. at 510.

\(^{17}\) Id. at 511.

\(^{18}\) Id. at 512.

\(^{19}\) Id. at 510 (“Once this much is acknowledged, and once it is recognized that the Fourth Amendment protects people—and not simply ‘areas’—against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.”).

\(^{20}\) Id. at 511-12 (“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… To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.”).

\(^{21}\) Id. at 512.
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.’”22 Justice Harlan goes on to note that while “[a] man’s home is, for most purposes, a place where he expects privacy, … objects, activities, or statements that he exposes to the ‘plain view’ of outsiders are not ‘protected’ because no intention to keep them to himself has been exhibited.”23 This implicates, in part, the third-party doctrine that the decisional law will return to.

It is also of note that the Supreme Court was not unanimous in its acceptance of a break of Fourth Amendment jurisprudence from property based understandings of trespass law. Justice Hugo Black’s dissent indicates themes that will be picked up by later Justices similarly uncomfortable with this perceived interpretation of the Fourth Amendment as creating a more general constitutional protection for broad “privacy” interests generally, untethered to the very terms of the Fourth Amendment.24

More recent developments in Fourth Amendment jurisprudence include *Kyllo v. United States*25 and *Jones v. United States*,26 both of which are decisions authored by Justice Antonin Scalia. In *Kyllo*, the issue presented was whether the Fourth Amendment was violated by government agents using a thermal-imaging device aimed at a private home from the street to detect heat within (as evidence of a marijuana growing operation).27 The Ninth Circuit affirmed the denial of Kyllo’s motion to suppress the evidence seized from his home, based in part on probable cause based on the thermal imaging information, holding that the defendant had no reasonable expectation of privacy in the heat escaping from his home, nor is such a privacy interest one that the public is prepared to accept as reasonable.28

The Supreme Court framed the issue by noting that it has “previously reserved judgment as to how much technological enhancement of ordinary perception from such a vantage point, if any, is too much.”29 Also by noting that “[t]he question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.”30

The Court ultimately concluded that the use of “sense-enhancing” technology to gather information about the interior of a home that would not otherwise be observable without a physical intrusion constitutes a search.31 Thus, in the light of technological advancement in *Kyllo*, the Court

22 Id. at 516 (Harlan, J., concurring) (emphasis added).
23 Id.
24 Id. at 523 (Black, J., dissenting) (“The Fourth Amendment protects privacy only to the extent that it prohibits unreasonable searches and seizures of ‘persons, houses, papers, and effects.’ No general right is created by the Amendment so as to give this Court the unlimited power to hold unconstitutional everything which affects privacy.”).
26 565 U.S. 400 (2012).
27 *Kyllo*, 121 S. Ct. at 2040-41 (“In order to determine whether an amount of heat was emanating from petitioner’s home consistent with the use of such lamps, at 3:20 a.m. on January 16, 1992, Agent Elliott and Dan Haas used an Agema Thermovision 210 thermal imager to scan the triplex.”)
28 Id. at 2041.
29 Id. at 2043.
30 Id. (internal quotation and citation omitted).
31 Id. (“We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area,’ constitutes a search—at least where (as here) the technology in question is not in general public use.”)
seeks to rein in or side-step Katz and, instead, ensure that the degree of privacy entitled to citizens is that which existed when the Fourth Amendment was adopted.\(^{32}\) Interestingly, however, the Court in Kyllo also specifically notes that its decision must take into account further technological advancement, in use or development, which could potentially discern human activity within the home.\(^{33}\) Thus, in a somewhat of a contradiction, the Court notes its farsightedness in addressing this developing area of technological advancement, but at the same time does so within a framework of what the Fourth Amendment would have meant at the time of its adoption, long before thermal-imaging technology.

Dissenting from the majority in Kyllo was Justice John Paul Stevens, who chides the majority for “taking the long view” by creating a rule that relates to the direct observations within a home, while that is not the circumstance before the Court.\(^{34}\) Nevertheless, while Justice Stevens is laudatory of the majority’s sensitivity to threats to privacy that will result from technological advancement, he does caution judicial restraint in light of these Fourth Amendment cases implicating new technologies and investigative techniques.\(^{35}\)

In United States v. Jones the issue presented was whether the Fourth Amendment was violated where law enforcement placed a global position system (“GPS”) unit on the defendant’s truck to monitor the vehicle’s movements on public streets.\(^{36}\) In Jones, law enforcement had used traditional forms of surveillance in order to develop probable cause to apply for a warrant authorizing the placement of a GPS unit on the Jeep Grand Cherokee registered to Jones’s wife.\(^{37}\) A warrant was issued allowing the placement of the GPS, which was placed and recorded the vehicle’s movements for the next twenty-eight days to within 100 feet of accuracy.\(^{38}\) Investigators exceeded the length of time they were permitted to use the GPS\(^ {39}\) as well as the geographical scope.\(^ {40}\)

The Supreme Court held that the Government’s installation of the GPS, outside of the constraints of the warrant, constituted a search.\(^ {41}\) However, declining to consider the larger

\(^{32}\) *Id.* ( “The Katz test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable.”).

\(^{33}\) *Id.* at 2044 (“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.”).

\(^{34}\) *Id.* at 2048 (Stevens, J., dissenting) (“While the Court ‘take[s] the long view’ and decides this case based largely on the potential of yet-to-be-developed technology that might allow ‘through-the-wall surveillance,’ this case involves nothing more than off-the-wall surveillance by law enforcement officers to gather information exposed to the general public from the outside of petitioner’s home.”) (internal citation omitted).

\(^{35}\) *Id.* at 2052 (Stevens, J., dissenting) (“Although the Court is properly and commendably concerned about the threats to privacy that may flow from advances in the technology available to the law enforcement profession, it has unfortunately failed to heed the tried and true counsel of judicial restraint. Instead of concentrating on the rather mundane issue that is actually presented by the case before it, the Court has endeavored to craft an all-encompassing rule for the future. It would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issues rather than to shackle them with prematurely devised constitutional constraints.”).


\(^{37}\) *Id.* at 403.

\(^{38}\) See *id.* at 402-03 (Over that 28 day period, more than 2,000 pages of data related to the vehicle’s movements was related to investigators.).

\(^{39}\) See *id.* (The GPS was directed to be installed within ten days, and it was installed on the eleventh day.).

\(^{40}\) See *id.* (The warrant was issued in the D.D.C., and the device was installed while the car was in Maryland, and monitored outside of D.C. as well.).

\(^{41}\) *Id.* at 404.
implications of GPS technology with respect to the Fourth Amendment, the Court was very particular to describe the limitation of its decision: “It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information.” Thus, in another step away from the reasonable expectation of privacy test in *Katz*, the Court returned to foundational trespass principles. Thus, the Court notes that its Fourth Amendment jurisprudence, before the mid-twentieth century, was tied to common-law conceptions of trespass, and that the Court in deciding *Jones* was applying that “minimum degree of protection” the Fourth Amendment afforded when adopted in the 18th century.

Justice Sotomayor concurred in the Court’s result, but wrote separately to note that while *Katz* did not diminish pre-existing trespassory understandings of the Fourth Amendment, it augmented the Fourth Amendment’s protections. Both Justice Sotomayor, and Justice Alito (joined by Justices Breyer, Ginsberg and Kagan) in his concurrence, also raise concerns about the Court’s decision in relation to technological advancement. With regard to the *Katz* test, the concurring Justices note that technological advances will play a role in shaping the “evolution of societal privacy expectations.” As will be directly implicated in *Carpenter* only a few years later, Justice Sotomayor asks “[w]hether people reasonably expect that their movements 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.”

Justice Sotomayor’s concurrence asks, in part, whether the third-party doctrine, or the premise that individuals have no reasonable expectation of privacy in information they disclose to third parties, needs to be reconsidered in light of modern technological advancements. Justice Sotomayor concludes that she “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.”

Justice Alito’s concurrence generally seeks to analyze the case in accordance with *Katz* and the reasonable expectation of privacy test. Justice Alito is seemingly frustrated by the majority’s focus on the placement of a GPS unit on the Jeep, instead of the use of GPS for purposes of long-term tracking, what he deems the “really important” consideration of the case. Raising

---

42 *Id.* at 404.
43 *Id.* at 405 (“But we need not address the Government’s contentions, because Jones’s Fourth Amendment rights do not rise or fall with the *Katz* formulation.”).
44 *Id.* at 411 (“What we apply is an 18th-century guarantee against unreasonable searches, which we believe must provide at a minimum the degree of protection it afforded when it was adopted.”).
45 *Id.* at 414.
46 *Id.* at 415-18, 427-30.
47 *Id.* at 415.
48 *Id.* at 416.
49 *Id.* at 417 (“This approach [i.e. the third-party doctrine] 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.”).
50 *Id.* at 418.
51 *Id.* at 418-30 (Alito, J. concurring).
52 *Id.* at 424-25.
the same issue as Justice Sotomayor, Justice Alito describes his concern of how technological changes will impact popular attitudes and, therefore, affect the Katz determinations of the future.53

Thus, the Fourth Amendment jurisprudence over the half-century leading to the Carpenter decision includes an expansion from common-law trespass principles in the Katz reasonable expectation of privacy test, along with the rebound to avoid Katz by using common law trespassory principles in Kyllo and Jones. However, these cases also suggest the Court’s anticipation and unease regarding the Fourth Amendment implications relative to technological advancements of the future. While some Justices seek to re-define technological advancements in terms of corollary practices of the eighteenth century,54 others seem to want to return to original meanings of the Fourth Amendment and implications of trespassory property principles,55 while still others see the inherent conflict between third-party doctrine and modern technology.56

It is in this context that the prolific writer of the Kyllo and Jones decisions, Justice Scalia, passed away in February of 2016 and was replaced by Justice Neil Gorsuch, appointed by President Donald Trump and confirmed by the senate in April of 2017. With this single and meaningful change in the Court’s composition, the Court accepted to hear United States v. Carpenter in its 2017-2018 session, and which was decided in June of 2018.

III. Carpenter v. United States and the Several Ways to Skin the Cat

Chief Justice John Roberts authored the opinion of the Court in Carpenter v. United States.57 As briefly described above, Carpenter involves cellular-site location information, or CSLI, and considers whether the Fourth Amendment is violated by the Government obtaining these records from cell phone carriers without a warrant.58 CSLI are records of a cell phone communicating with a cell site, or cell tower, which generally occurs several times a minute whenever the phone signal is on, regardless of whether the phone is in active use.59 This information, which indicates where a phone is at a given point in time, and its movements over the course of time, is collected and stored by cell phone carriers for their own business purposes.60 Moreover, not only do carriers aggregate this information about their users, they also sell it to data brokers.61

53 Id. at 427 (“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. On the other hand, concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions.” (internal citation omitted).
54 See Katz v. United States, 88 S. Ct. 507, 519 (1967) (Black, J., dissenting) (“Wiretapping and recording by electronic devices is merely modern eavesdropping, an ancient practice the framers were aware of and could have written into the Fourth Amendment if they chose to include such conduct/evidence.”).
58 Id. at 2211.
59 Id.
60 Id. at 2212.
61 Id.
The investigation which led to Carpenter’s indictment began with four men suspected of robbing a series of T-Mobile and RadioShack stores in Detroit.62 Ultimately, the investigation of these four men led to investigators learning of a larger ring of robberies in Michigan and Ohio which implicated the defendant, Carpenter.63

Based on their investigations, investigators obtained warrants under the Stored Communication Act (“SCA”)64 for cell records of Carpenter and others.65 The warrants were approved by a magistrate for all “cell/site sector [information] for [Carpenter’s] telephone[] at call origination and at call termination for incoming and outgoing calls” from his cell carriers during the four-month period when the string of robberies occurred.66 Through this SCA process, investigators obtained 12,898 location points cataloguing Carpenter’s movements, which amounted to an average of 101 data points, or location points, each day.67

Carpenter was indicted for six counts of robbery and six counts of carrying a firearm during a federal crime.68 Carpenter moved to suppress the CSLI records, which was denied, and that evidence was introduced through an FBI agent, offered as an expert, who testified about the movements of the defendant the CSLI showed, along with demonstrative maps.69 According to the agent, the CSLI evidence showed that Carpenter’s phone was in the area of four of the robberies around the time the robberies had occurred.70 Carpenter was convicted of five counts and sentenced to over 100 years, which was affirmed by the Sixth Circuit.71

The issue presented before the Supreme Court was Fourth Amendment implications of investigator’s collection of the CSLI used against Carpenter. The Court began by surveying its Fourth Amendment jurisprudence, noting the historic connection of the Fourth Amendment with common-law trespass doctrine and the development of the reasonable expectation of privacy test of Katz.72 Under the Katz paradigm, the Court turns to considerations of what constitutes privacy expectations that are entitled to protection.73

Chief Justice Roberts begins his analysis by noting that this kind of digital information or data which is collected and maintained by a third party “does not fit neatly under existing precedents.”74 Instead, he continues, this CSLI falls at the nexus of two lines of cases, that of the

---

62 Id.
63 Id.
64 18 U.S.C. § 2703(d). See Carpenter, 138 S. Ct. at 2212 (“[The Stored Communications Act], as amended in 1994, permits the Government to compel the disclosure of certain telecommunications records when it ‘offers specific and articulable facts showing that there are reasonable grounds to believe’ that the records sought ‘are relevant and material to an ongoing criminal investigation.’”). The Stored Communications Act, or “SCA” has been widely criticized in response to technological advancements that have postdated its passage. This will be briefly described infra.
65 Carpenter, 138 S. Ct. at 2212.
66 Id.
67 Id.
68 Id. at 2212. See 18 U.S.C. § 924(c) (robbery); 18 U.S.C. § 1951(a) (carrying a firearm during a federal crime).
70 Id.
71 Id. at 2213.
72 Id. at 2213.
73 Id. at 2213-14.
74 Id. at 2214-15.
Katz reasonable expectation of privacy doctrine and that of third-party doctrine jurisprudence. With regard to third-party doctrine, the Court noted that it “has drawn a line between what a person keeps to himself and what he shares with others. [The Court] ha[s] previously held that ‘a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.’” The Court points to United States v. Miller, where there was found to be no Fourth Amendment protection for bank records, such as checks and other commercial documents, which are exposed to bank employees in the normal course of business. The Court also pointed to Smith v. Maryland, where no Fourth Amendment protection was found for the use of a pen register, which records phone numbers dialed, as individuals have no reasonable expectation of privacy in the numbers they dial, nor is society prepared to recognize such a privacy interest as reasonable.

However, despite the apparent parallels between Miller, Smith and the circumstance before the Court in Carpenter, the Court declined to extend those cases and the third-party doctrine:

We decline to extend Smith and Miller to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user’s claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in Jones or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter’s wireless carriers was the product of a search.

To reach this conclusion, the Court relies heavily on the interest at stake, if not the Court’s actual reasoning, in Jones. As opposed to the physical intrusion on the vehicle that was determinative in Jones, the Court in Carpenter recognized instead the interest at stake in Jones as a person’s reasonable expectation of privacy in “the whole of their physical movements.” Moreover, the Court holds that the mere fact that these records are generated for commercial purposes “does not negate Carpenter’s anticipation of privacy in his physical location.”

Also like Jones, the Court’s decision specifically references its concerns for CSLI specifically in the future, as the precision of this location information will likely improve further.

---

75 Id. at 2215-16.
76 Id. at 2216 (quoting Smith v. Maryland, 442 U.S. 735, 743-44 (1979)).
79 Carpenter, 138 S. Ct. at 2217.
80 Id. at 2217.
81 Id.
82 Id. at 2219 (“While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision. As the number of cell sites has proliferated, the geographic area covered by each cell sector has shrunk, particularly in urban areas. In addition, with new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone’s location within 50 meters.”).
Also drawing a parallel to Kyllo in a sense, the Court notes its concern about the retrospective nature of this CSLI, where the timeframe is limited only by the cell carrier’s respective retention policies and, therefore, results in the defendant essentially having been “tailed” every day for years. Thus, where the Court in Kyllo noted a concern regarding how thermal imaging devices expand what is knowable by traditional investigative techniques, so too is that concern noted by the Court in Carpenter.

In further describing why the third-party doctrine does not apply in this case, the Court goes on to reference the “seismic shifts in digital technology that made possible the tracking of not only Carpenter’s location but also everyone else’s, not for a short period but for years and years.” Thus, in reference to Smith and Miller, the Court draws distinctions between the quantum of information acquired by the government and the nature of the documents and what it reflects about the defendant’s expectation of privacy. The Court explains this distinction about the “nature” of the document by indicating that “[c]ell phone location information is not truly ‘shared’ as one normally understands the term.” This is true because of the pervasiveness of cell phones to daily life, and how the CSLI collection is entirely passive on the part of the user (i.e., requires no affirmative act).

Notwithstanding the sweeping nature of the decision in Carpenter, as it relates to the function of third-party doctrine in relation to new technology and the Fourth Amendment jurisprudence generally, the Court seeks to narrow its decision to only the issue of the case before it. Thus, the Court’s decision is limited to the fact that the Fourth Amendment requires a warrant, or valid exception to the warrant requirement, to obtain CSLI under circumstances similar to those presented in Carpenter. “We hold only that a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party.” The Court concludes by quoting Justice Brandeis in Olmstead v. United States, where he writes “the Court is obligated—as ‘[s]ubtler and more far-reaching means of invading privacy have become available

83 Id. at 2218.
84 Id. at 2219.
85 Id.
86 Id. at 2220.
87 Id. (“In the first place, cell phones and the services they provide are ‘such a pervasive and insistent part of daily life’ that carrying one is indispensable to participation in modern society.”).
88 Id. (“Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.”).
89 Id. at 2220 (“Our decision today is a narrow one. We do not express a view on matters not before … We do not disturb the application of Smith and Miller or call into question conventional surveillance techniques and tools, such as security cameras. … As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not ‘embarrass the future.’”) (quoting Northwest Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).
90 Id. at 2221. Thus a “reasonable grounds” showing for believing that information “relevant and material” to an ongoing investigation for a magistrate’s warrant under the SCA is insufficient.
91 Id. at 2222.
to the Government’—to ensure that the ‘progress of science’ does not erode Fourth Amendment protections.”93

The Court’s decision drew a number of dissents, including from Justice Kennedy (joined by Justices Thomas and Alito), from Justice Thomas, from Justice Alito (joined by Justice Thomas) and from Justice Gorsuch.94 First, Justice Kennedy essentially chastises the majority from “unhing[ing] Fourth Amendment doctrine from the property-based concepts that have long grounded the analytic framework that pertains in these cases.”95 Justice Kennedy describes how the majority tailors an unworkable line between CSLI and bank (Miller) and telephone (Smith) records, which is inherently unworkable.96 Kennedy explains how Miller and Smith represent a necessary limitation on the Katz framework, requiring that a property interest in the searched or seized items by the defendant.97 Moreover, Justice Kennedy states that the compulsory process required by the SCA is sufficient where no Fourth Amendment interest exists due to the third-party doctrine.98

Compellingly, Justice Kennedy also describes how the contents of banking records or outgoing phone numbers can be as telling about an individual as can CSLI.99 In this sense, Justice Kennedy disagrees with the majority’s having treated CSLI as a “distinct category of information” from other forms of business records as unsupported.100

In his dissent, Justice Thomas describes how the majority’s decision misses the determinative issue: that the property searched was that of MetroPCS and Sprint, the defendant’s cell carriers, and not the defendant’s for Fourth Amendment purposes.101 Also raising the perceived misapplication of the third-party doctrine, Justice Thomas notes that Carpenter did not create the records, did not maintain them, did not control them and does not have the authority to destroy them, either by contract or operation of law.102

However, unlike Kennedy, Justice Thomas takes his criticism deeper, by arguing that Katz and the reasonable expectation of privacy test is, itself, is a distortion of Fourth Amendment jurisprudence.103 Justice Thomas argues that Katz has no basis in text or history of the Fourth Amendment and represents policy-making by the court which continues to distort Fourth

93 Id. at 2223.
94 Id. at 2224-72.
95 Id. at 2224 (Kennedy, J. dissenting).
96 Id. at 2226-27.
97 Id. at 2227 (“The defendants could make no argument that the records were their own papers or effects.”); Id. at 2229 (“As in Miller, Carpenter can ‘assert neither ownership nor possession’ of the records and has no control over them.”).
98 Id. at 2229-31 (“Cases like this one, where the Government uses court-approved compulsory process to obtain records owned and controlled by a third party, are governed by the two majority opinions in Miller and Smith.”).
99 Id. at 2232 (“What persons purchase and to whom they talk might disclose how much money they make; the political and religious organizations to which they donate; whether they have visited a psychiatrist, plastic surgeon, abortion clinic, or AIDS treatment center; whether they go to gay bars or straight ones; and who are their closest friends and family members. The troves of intimate information the Government can and does obtain using financial records and telephone records dwarfs what can be gathered from cell-site records.”).
100 Id. at 2234.
101 Id. at 2235 (Thomas, J., dissenting).
102 Id.
103 Id. at 2235-39.
Amendment jurisprudence. Justice Thomas indicates that the *Katz* focus on an amorphous concept of “privacy” inherently reads “persons, houses, papers, and effects” entirely out of the Fourth Amendment, clearly opposed to the intent of the founders whose very terms identified four categories of objects for which they intended Constitutional protections to extend. Justice Thomas also argues that *Katz* reads out the possessive component of the Fourth Amendment (i.e., “their” persons, etc.), in that a reasonable expectation of privacy can extend to another’s property. Thus, Justice Thomas’s dissent fundamentally argues that *Katz* itself is unsupportable as a matter of law and unworkable in practice, suggesting that the Court should return Fourth Amendment jurisprudence to the pre-*Katz* understanding, tied to property doctrines.

Justice Alito’s dissent also argues that the majority decision writes the possessory interest out of the Fourth Amendment by its corruption of third-party doctrine. However, unlike Justices Thomas or Kennedy, Justice Alito focuses on the compulsory aspect of the SCA that was implicated in this case vis-a-vis the requirements of the Fourth Amendment. In tracing the historical development of *subpoena duces tecum*, Justice Alito argues that where the compulsory production of documents is provided for, the Fourth Amendment cannot apply. Said another way, Justice Alito argues that production of documents under a compulsory process inherently does not implicate a “physical intrusion into a private space, nor any taking of property by agents of the state,” precursors to a Fourth Amendment claim.

In his dissent, Justice Alito also describes his concern that the majority decision creates a slippery slope for Fourth Amendment jurisprudence in the future. He writes that “[a]lthough the majority announces its holding in the context of the Stored Communications Act, nothing stops its logic from sweeping much further. The Court has offered no meaningful limiting principle, and none is apparent.” Finally, Justice Alito argues that while the majority frames its position as declining to extend the third-party doctrine of *Miller* and *Smith* when, in reality, the majority fails to understand that *Miller* and *Smith* merely rejected an argument that would have been at odds with the clear meaning of the Fourth Amendment (i.e., that one can assert a Fourth Amendment claim over papers or effects that are not theirs.)

Arguably the most interesting dissenting opinion is the final dissent, that of Justice Gorsuch. Justice Gorsuch’s dissent begins with a sweeping soliloquy about the state of the Fourth Amendment.

---

104 *Id.* at 2236.
105 *Id.* at 2241.
106 *Id.* at 2241-42.
107 *Id.* at 2244.
108 *Id.* at 2247 (Alito, J., dissenting).
109 *Id.* at 2247-61.
110 *Id.* at 2251 (“Talk of kings and common-law writs may seem out of place in a case about cell-site records and the protections afforded by the Fourth Amendment in the modern age. But this history matters, not least because it tells us what was on the minds of those who ratified the Fourth Amendment and how they understood its scope. That history makes it abundantly clear that the Fourth Amendment, as originally understood, did not apply to the compulsory production of documents at all. The Fourth Amendment does not regulate all methods by which the Government obtains documents. Rather, it prohibits only those ‘searches and seizures’ of ‘persons, houses, papers, and effects’ that are ‘unreasonable.’”)
111 *Id.* at 2251.
112 *Id.* at 2256.
113 *Id.*
114 *Id.* at 2260.
Amendment in light of modern American dependence on the internet and his perception of the options of how to address the same:

What’s left of the Fourth Amendment? Today we use the Internet to do most everything. Smartphones make it easy to keep a calendar, correspond with friends, make calls, conduct banking, and even watch the game. Countless Internet companies maintain records about us and, increasingly, for us. Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. Smith and Miller teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did. What to do? It seems to me we could respond in at least three ways. The first is to ignore the problem, maintain Smith and Miller, and live with the consequences. If the confluence of these decisions and modern technology means our Fourth Amendment rights are reduced to nearly nothing, so be it. The second choice is to set Smith and Miller aside and try again using the Katz ‘reasonable expectation of privacy’ jurisprudence that produced them. The third is to look for answers elsewhere.115

Justice Gorsuch goes on to take issue with the third-party doctrine of Smith and Miller, akin to the majority.116 Like Justice Thomas, Justice Gorsuch would see the end of the Katz inquiry, also finding it to be insufficiently justified.117 Justice Gorsuch poses the question of whether the Katz test is “supposed to pose an empirical question (what privacy expectations do people actually have) or a normative one (what expectations should they have)? Either way brings problems. If the test is supposed to be an empirical one, it’s unclear why judges rather than legislators should conduct it… [if a normative one] why (again) do judges, rather than legislators, get to determine whether society should be prepared to recognize an expectation of privacy as legitimate?”118

Justice Gorsuch goes on to comment on how the frailties of the Katz test have “yielded an often unpredictable—and sometimes unbelievable—jurisprudence.”119 Justice Gorsuch criticizes how little guidance the majority provides lower courts in imposing the more amorphous Katz

115 Id. 2262 (Gorsuch, J., dissenting).
116 Id. 2262 (“The problem isn’t with the Sixth Circuit’s application of Smith and Miller but with the cases themselves. Can the government demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights? Can it secure your DNA from 23andMe without a warrant or probable cause? Smith and Miller say yes it can—at least without running afoul of Katz. But that result strikes most lawyers and judges today—me included—as pretty unlikely.”).
117 Id. at 2265.
118 Id.
119 Id. at 2266 (“Take Florida v. Riley, 488 U.S. 445, 109 S.Ct. 693, 102 L.Ed.2d 835 (1989), which says that a police helicopter hovering 400 feet above a person’s property invades no reasonable expectation of privacy. Try that one out on your neighbors. Or California v. Greenwood, 486 U.S. 35, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988), which holds that a person has no reasonable expectation of privacy in the garbage he puts out for collection.”).
standard it has adopted. Justice Gorsuch continues that “[i]n the end, our lower court colleagues are left with two amorphous balancing tests, a series of weighty and incommensurable principles to consider in them, and a few illustrative examples that seem little more than the product of judicial intuition. In the Court’s defense, though, we have arrived at this strange place not because the Court has misunderstood Katz. Far from it. We have arrived here because this is where Katz inevitably leads.”

In addressing how he would envision a Fourth Amendment analysis in a post-Katz paradigm, Gorsuch offers a return to, and expansion of, the property-based considerations in this case. First, Justice Gorsuch suggests that one can have a property-based interest in papers or effects held by a third-party, when it is the basis of a bailment at common law. Justice Gorsuch thus argues that an individual entrusting his or her data, such as emails on a cloud-based email server, is a modern day bailment in which the owner “retains a vital and protected legal interest.”

Justice Gorsuch next argues that complete ownership or exclusive control is not a necessary condition for Fourth Amendment protection, and therefore Fourth Amendment protections can exist for property not in the owner’s possession and control when seized or searched.

Next, Justice Gorsuch posits that positive law, or the law of the state or federal government can create rights in tangible and intangible things, which may create Fourth Amendment protections in a given property, or which law could be designed to not defeat a Fourth Amendment claim. Finally, Justice Gorsuch breaks with Justice Alito by noting that the mere use of a compulsory process cannot be used to frustrate the protections of the Fourth Amendment. Justice Gorsuch concludes his dissent in summing up his preferred approach to Fourth Amendment analysis for the technological era: “I would look to a more traditional Fourth Amendment approach. Even if Katz may still supply one way to prove a Fourth Amendment interest, it has never been the only way. Neglecting more traditional approaches may mean failing to vindicate the full protections of the Fourth Amendment.”

---

120 Id. at 2266 (“Lower courts should be sure to add two special principles to their Katz calculus: the need to avoid ‘arbitrary power’ and the importance of ‘plac[ing] obstacles in the way of a too permeating police surveillance.’ Ante, at 2214 (internal quotation marks omitted). While surely laudable, these principles don’t offer lower courts much guidance. The Court does not tell us, for example, how far to carry either principle or how to weigh them against the legitimate needs of law enforcement. At what point does access to electronic data amount to ‘arbitrary’ authority? When does police surveillance become ‘too permeating’? And what sort of ‘obstacles’ should judges ‘place’ in law enforcement’s path when it does? We simply do not know.”).

121 Id. at 2267.

122 Id. at 2268-71.

123 Id. at 2268 (“Ever hand a private document to a friend to be returned? Toss your keys to a valet at a restaurant? Ask your neighbor to look after your dog while you travel? You would not expect the friend to share the document with others; the valet to lend your car to his buddy; or the neighbor to put Fido up for adoption. Entrusting your stuff to others is a bailment.”)

124 Id. at 2269.

125 Id. at 2270 (“Think of the finder of lost goods or the policeman who impounds a car. The law recognizes that the goods and the car still belong to their true owners.”).

126 Id. at 2270.

127 Id. at 2271. (“No one thinks the government can evade Jackson’s prohibition on opening sealed letters without a warrant simply by issuing a subpoena to a postmaster for ‘all letters sent by John Smith’ or, worse, ‘all letters sent by John Smith concerning a particular transaction.’ So the question courts will confront will be this: What other kinds of records are sufficiently similar to letters in the mail that the same rule should apply?”)

128 Id. at 2272.
IV. Survey of Post-Carpenter Fourth Amendment Thought

The nuance and various approaches proposed in Carpenter have led to innumerable interpretations and lines of thought regarding the strengths, shortcomings and predictive interpretations of the case in the academic and professional literature. For some, Carpenter is seen as the beginning of a significant changes to Fourth Amendment jurisprudence to come.129

A significant focus of legal thought regarding the implications of the Fourth Amendment post-Carpenter has been with an eye towards other forms of third-party data that permeate modern American life.130 Naturally, while the discreet question of CSLI in Carpenter is affirmatively decided, the myriad of other forms of cloud computing and remote data storage is fertile ground for Fourth Amendment speculation.

A related question that has been considered is the role that technology companies may play in endeavoring to comply, or resist, governmental forces.131 In this regard, legal scholars have looked at some of the cases in which “surveillance intermediaries” (i.e. technology companies which maintain user data) have dealt with government requests for information over time.132 There is a strong argument in favor of some body or institution outside of the tech companies themselves making the strategic decision about how to address government intrusion into the data of consumers.133

Others in legal scholarship have considered how the technical aspects of cloud computing impact questions of access and governmental incursion.134 There is a general frustration with how legislative efforts, such as the Stored Communications Act (“SCA”), perhaps right-minded or forward thinking at the time, have become inadequate as they have become technologically outdated.135

Part of what these questions of technological advancement and the interests of the tech companies are part of the bigger issue with Carpenter, in the many questions which remain unanswered about how the paradigm will develop and be imposed in the future. Some of the questions that have been described, which are even relatively akin to the issue in Carpenter, have been how the decision would apply to real time CSLI, monitoring of historic CSLI for less than

130 Michael Price, Carpenter Versus the United States and the Future of the Fourth Amendment, THE CHAMPION, June 2018, at ___ (“Today, third-party service providers keep records detailing cellphone use, web browsing history, and most online activities. Online retailers keep track of what a user has purchased or merely perused. App makers log how users interact with their programs, and often much more.”).
132 Id.
133 Id. at 1729 (“Do technology companies facilitate or frustrate government surveillance? The answer is that they do both, and this fluctuation should give one pause. Reasonable minds may differ as to what the ideal balance between cooperation and resistance might be, but it seems unlikely that this balance should be left to the judgment of a private corporation. Whatever the appropriate amount of cooperation—or resistance—is, this is an important public policy issue, and it should be decided with regard to the public’s best interests and wishes. When creating regulations, it is critical to understand why surveillance intermediaries make the decision to resist or cooperate, and to attempt to align those incentive structures with a balanced approach to security and privacy.”)
135 Id. at 1671.
the seven days at issue in Carpenter, wholesale dumps of cell site or cell tower information, or data accumulated from other kinds of cellular transactions, such as online banking apps, for example. For that matter, how will Carpenter’s holding apply to the whole wide universe of non-location information and data that is inherent in cloud computing? Ultimately, the academic literature wrestles with these issues and ultimately adds more and more questions.

V. Carpenter in Connecticut

In the very recently issued decision State v. Brown, the State of Connecticut appealed the trial court’s order dismissing the case against the defendant where law enforcement obtained six days of CSLI tracking his movements and they did so through three ex-parte orders under Conn. Gen. Stat. Section 54-47aa. This case ultimately tracked the issue in Carpenter, requiring the Connecticut Supreme Court to consider whether a compulsory process based on reasonable and articulable suspicion, under Section 54-47aa, was legally sufficient to obtain the Defendant’s CSLI. Given the close factual parallel with Carpenter, the Connecticut Supreme Court stayed the appeal to await the decision in Carpenter. Following the issuance of the Carpenter decision, the Court had the parties submit briefs on the application of Carpenter, and ultimately ruled that Carpenter was controlling authority and did require the trial court to suppress the CSLI obtained in violation of the Defendant’s Fourth Amendment rights.

In deciding Brown, the Connecticut Supreme Court was able to side step much of the uncertainty and thorny considerations that the Carpenter dissents and legal commentators have registered concerns about. Because Brown was so factually consistent with Carpenter, the application was relatively straightforward, and the Government’s attempts to distinguish Carpenter unavailing.

Another case, which is currently under consideration by the Connecticut Appellate Court, is State v. Montanez. Montanez, again, is specific to the use of CSLI, which was used in the State’s case against Montanez; however, the focus of that matter is more geared towards the application of Carpenter when the CSLI was not subject to a suppression hearing on Fourth Amendment grounds and the issue was not otherwise argued or, perhaps, preserved for appeal. Moreover, given the briefing on Montanez, it appears unclear whether a warrant was issued by investigators to obtain the CSLI that was ultimately used in the state’s case in chief.

---

137 331 Conn. 258 (2019).
138 Appellant’s Brief 14.
139 Brown, 331 Conn. 258.
140 Id.
141 Id. at 723 n.8 (“We believe that a fair reading of the decision is that accessing CSLI for seven days or more is clearly a search for purposes of the fourth amendment. What the court left unsettled is whether accessing CSLI for fewer than seven days constitutes a search. At best, therefore, Carpenter leaves unanswered the question of whether an order targeting a very short time frame would be permitted under the fourth amendment.”)
142 State v. Montanez, Docket No. AC40359.
143 Id.
144 Defendant’s Motion for Reconsideration En Banc, dated March 25, 2019, p. 9, FN4.
To date, it is unclear whether there are any cases currently before the appellate courts of Connecticut which seek to implicate Carpenter in a context other than CSLI.

VI. Conclusion

The Supreme Court’s decision in Carpenter is considered a “watershed” opinion, and for good reason. The Carpenter case will have long lasting implications not only for all that it says, but also because of what it does not say. While the Carpenter court definitively answers a discreet question regarding the Fourth Amendment implications for CSLI, in doing so the Court gives the world a glimpse into the possible applications of the Fourth Amendment in future cases involving other various technological advancements as they relate to investigative techniques and methods. Moreover, at the time of this writing two Supreme Court Justices are over eighty years old, one approaching ninety.\textsuperscript{145} As such, Supreme Court appointments in coming years may also lead to important changes in the Court’s dynamics regarding how the Fourth Amendment is addressed in the future.

The stakes in Carpenter were momentous for the Defendant, but also for the American people. CSLI is merely a drop in the bucket of the forms and kinds of electronic data that is collected every second of every day in modern America. CSLI is but one piece of a puzzle that law enforcement may seek to gain a better understanding of their target, how he spends his time, the places he goes, the people he consorts with and all of the implications that follow. As the era of cloud computing continues to be at its dawn, we can anticipate the various frameworks, considerations, concerns and disagreements on display in Carpenter to be repeated themes in the development of Fourth Amendment jurisprudence.