YOUR SPYING SMARTPHONE: INDIVIDUAL PRIVACY IS NARROWLY STRENGTHENED IN *CARPENTER V. UNITED STATES*, THE U.S. SUPREME COURT'S MOST RECENT FOURTH AMENDMENT RULING

Vania Mia Chaker, Esq.[*]

Abstract

Recently, the United States Supreme Court wrestled with the profoundly complex and bedeviling issue of individual privacy in the landmark case of *Carpenter v. United States*.[1] It is the most recent in a long line of Fourth Amendment cases that examine an individual's reasonable expectation of privacy. In *Carpenter*, the Supreme Court revisited and expanded upon this query from *Riley v. California*[2] and *United States v. Jones*[3]—both progeny of *Katz v. United States*,[4] the leading case in this area.

The *Carpenter* Court ruled the government required a warrant before it could use private information arising from defendant Timothy Carpenter's cellular phone[5]—specifically, his cell site location information (CSLI). In the 5-4 decision, the Court ruled "narrowly" in favor of privacy, finding the government had constitutionally violated Mr. Carpenter's reasonable expectation of privacy by acquiring this private

---

* A.B., Stanford University; M.B.A., Columbia Business School; M.B.A., University of California, Berkeley Haas School of Business; J.D., University of California, Berkeley School of Law.

I am deeply grateful to all of the gracious individuals who have assisted me with this project, but especially long-time mentors, Dean Emeritus Jesse Choper, the Honorable Tom Campbell, and the Honorable C. Christopher Cox. Without their invaluable assistance and interest in my work, this Article would never have reached fruition.

I owe a profound debt of gratitude to all of my beloved mentors, my esteemed advisors in academia and law, and my inspiring Stanford professors, including the Honorable Edwin Meese III, the Honorable C. Christopher Cox, the Honorable Tom Campbell, the Honorable Lane Evans, the Honorable Rudi M. Brewster, the Honorable Mitchel R. Goldberg, the Honorable Dick Thornburgh, the Honorable Robert W. Naylor, Professor Lawrence M. Friedman, Ralph N. Schmidt, and all of the distinguished Senior Fellows at the Hoover Institution who I was extremely privileged to have worked with and known. A special, heartfelt thank you goes to Jonathan A. Sebastiani, Donald L. Lucas, Sr., and Kimberly R. Hauser. I am extremely fortunate and grateful to have had the encouragement and support of all of these fine individuals during my career.

I also thank Ryan G. Baker, Matthew M. Mahoney, Phil Burkhardt, Jaime Marquart, Charles L. Deem, and William V. Whelan for their steadfast support.

I dedicate this Article to Henri, Jeanne, Albért, Colette, and Lucien Chaker, M.P.B., B.B.L. – et toutes les personnes qui j'appelle ma famille.

1. Carpenter v. United States, 138 S. Ct. 2206 (2018).
2. Riley v. California, 134 S. Ct. 2473 (2014).
3. United States v. Jones, 132 S. Ct. 945 (2012).
4. Katz v. United States, 389 U.S. 347 (1967).
5. *Carpenter*, 138 S. Ct. at 2221.

information without a warrant.[6] It ruled that, as a cell phone customer, Mr. Carpenter could reasonably expect that his CSLI would be treated as private, even though it was in the possession of a third party.[7] In so ruling, the Court declined to apply the long-standing third-party doctrine of *United States v. Miller*[8] and *Smith v. Maryland*.[9] These cases, which stand for the proposition that there is a reduced expectation of privacy in information an individual knowingly shares with another, have thus been narrowed.[10]

Against a backdrop of stunningly advanced surveillance technology and the strictures of the United States Constitution, the question of how individual privacy comports with the need for police investigation is a complex and impressively difficult one. In the current political landscape, judicial vigilance becomes increasingly important in protecting the appropriate dimensions of individual privacy. The grave risks of governmental abuse may militate in favor of strengthened judicial oversight in determining the parameters of the state's broad investigative powers. Strong privacy protections may indeed serve to function as a safeguard against the risks of governmental overreach, police misconduct, and improper warrantless surveillance.

6. *Id.* at 2219.
7. *Id.* at 2220.
8. United States v. Miller, 425 U.S. 435 (1976).
9. Smith v. Maryland, 442 U.S. 735 (1979).
10. *Carpenter*, 138 S. Ct. at 2220.

* * *

I give the fight up; let there be an end,
A privacy, an obscure nook for me,
I want to be forgotten even by God.

Robert Browning, Paracelsus (1835)

INTRODUCTION

The United States Supreme Court again wrestled with the profoundly complex and bedeviling issue of individual privacy in the landmark case of *Carpenter v. United States*.[11] It is the most recent in a long line of Fourth Amendment cases that examine an individual's reasonable expectation of privacy. In *Carpenter*, the Supreme Court revisited and expanded upon this query from *Riley v. California*[12] and *United States v. Jones*[13]—both progeny of *Katz v. United States*,[14] the leading case in this area. In the 5-4 decision, Chief Justice John Roberts delivered the opinion of the *Carpenter* Court in favor of individual freedom, in which Associate Justices Ruth Bader Ginsburg, Stephen Breyer, Sonia Sotomayor, and Elena Kagan joined.

The *Carpenter* Court ruled the government required a warrant before it could use private information acquired from defendant Timothy Carpenter's cellular phone[15]—specifically, his cell site location information (CSLI). The Court ruled "narrowly" in favor of privacy, finding the government had constitutionally violated Mr. Carpenter's reasonable expectation of privacy by acquiring this private information without a warrant.[16] It ruled that, as a cell phone customer, Mr. Carpenter could reasonably expect that his CSLI would be treated as private, even though it was in the possession of a third party.[17] In so ruling, the Court declined to apply the long-standing third-party doctrine of *United States v. Miller*[18] and *Smith v. Maryland*.[19] The holdings in these cases, which stand for the proposition that there is a reduced expectation of privacy in information an individual knowingly shares with another, have thus been

11. Carpenter v. United States, 138 S. Ct. 2206 (2018).
12. Riley v. California, 134 S. Ct. 2473 (2014).
13. United States v. Jones, 132 S. Ct. 945 (2012).
14. Katz v. United States, 389 U.S. 347 (1967).
15. *Carpenter*, 138 S. Ct. at 2221.
16. *Id.* at 2219.
17. *Id.* at 2220.
18. United States v. Miller, 425 U.S. 435 (1976).
19. Smith v. Maryland, 442 U.S. 735 (1979).

narrowed.[20] Because of this striking departure from prior precedent, *Carpenter* is considered a landmark decision.[21]

Justices Anthony Kennedy, Neil Gorsuch, Clarence Thomas, and Samuel Alito, however, roundly criticized the opinion. Justice Clarence Thomas filed a dissenting opinion, and Justice Samuel Alito filed a dissenting opinion in which Justice Thomas joined. Justice Gorsuch also filed a dissenting opinion. The dissenting Justices seemed most concerned with what they considered the majority's lack of clear guidance and specificity as to what would constitute constitutional conduct during a police investigation.[22] Some Justices also expressed concern that law enforcement's legitimate need to investigate its cases could be compromised. Justice Alito, for example, stated that he believed the decision may imperil many valuable and entrenched investigative practices upon which law enforcement has historically relied[23]—a worry echoed by other dissenting Justices. As Justice Kennedy quoted from *Riley* to explain[24]: "In short, the Court's new and uncharted course will inhibit law enforcement and 'keep defendants and judges guessing for years to come.'" He deemed this to be a grave consequence for the "proper administration of justice."[25] A common, overshadowing thread in the dissenting opinions seemed to center around the extent to which the

---

20. *Carpenter*, 138 S. Ct. at 2217.

21. *See, e.g.*, *id.*; *Whether the Fourth Amendment Permits the Government to Obtain Six Months of Cell Phone Location Records Without a Warrant*, EPIC, https://epic.org/amicus/location/carpenter/ (last visited Aug. 11, 2018); *see also* Allen O'Rourke, *SCOTUS Issues Landmark Decision on Cell Phone Location Information with Major Implications for Fourth Amendment Privacy*, A.B.A. BUS. L. TODAY (July 17, 2018), https://businesslawtoday.org/2018/07/scotus-issues-landmark-decision-cell-phone-location-information-major-implications-fourth-amendment-privacy/.

22. Justice Kennedy, for example, wrote, "the majority opinion gives courts and law enforcement officers no indication how to determine whether any particular category of information falls on the financial-records side or the cell-site-records side of its newly conceived constitutional line." *Carpenter*, 138 S. Ct. at 2234 (Kennedy, J., dissenting). Justice Kennedy went on to note: "The Court's multifactor analysis—considering intimacy, comprehensiveness, expense, retrospectivity, and voluntariness—puts the law on a new and unstable foundation. *Id.* Justice Thomas stated: "Suffice it to say, the Founders would be confused by this Court's transformation of their common-law protection of property into a 'warrant requirement' and a vague inquiry into 'reasonable expectations of privacy.'" *Id.* at 2244 (Thomas, J., dissenting).

23. Justice Alito warned: "I share the Court's concern about the effect of new technology on personal privacy, but I fear that today's decision will do far more harm than good. The Court's reasoning fractures two fundamental pillars of Fourth Amendment law, and in doing so, it guarantees a blizzard of litigation while threatening many legitimate and valuable investigative practices upon which law enforcement has rightfully come to rely." *Id.* at 2246–47 (Alito, J., dissenting).

24. *Id.* at 2234 (Kennedy, J., dissenting) (internal quotation marks omitted) (quoting *Riley v. California*, 573 U.S. 134 S. Ct. 2473, 2493 (2014)).

25. Justice Kennedy noted: "[T]he Court fails even to mention the serious consequences this will have for the proper administration of justice." *Id.* at 2234 (Kennedy, J., dissenting).

scope of the third-party doctrine would be narrowed as well as how and where to draw these new constitutional boundaries. It is not entirely clear in what way the government's reliance on the third-party doctrine will be affected in future cases.

Perhaps in an attempt to assuage the dissenting Justices' concerns, Chief Justice Roberts emphasized the ruling should only be considered a "narrow"[26]—or limited—win for individual privacy. The question of exactly where to judicially delineate the parameters of privacy is one that is far from over, however, particularly given the significant fissure in the Court regarding such issues. This query may become more complicated by the change in the composition of the Bench in the wake of Justice Kennedy's retirement and the confirmation of the most recently appointed Justice to the Supreme Court. President Trump is likely to nominate a judge that is significantly more politically conservative than Justice Kennedy, who was often a swing vote in close decisions.[27] Justices' views on privacy are notoriously idiosyncratic, however. Kennedy, a "moderate," was anti-privacy in the *Carpenter* case while Roberts, a "conservative," was pro-privacy.

Moreover, given the tenuous 5-4 majority, it is not a foregone conclusion that the same line of reasoning—or even a similar ruling in favor of privacy—will prevail during the next Fourth Amendment challenge. In already murky and uncertain waters, the change in the composition of the Bench further underscores the fragile nature of the alliance that formed in *Carpenter*, which only narrowly tempered the government's warrantless investigative reach.

I. DIGITAL TECHNOLOGY AND THE QUALITATIVELY DIFFERENT NATURE OF PRESENT-DAY CELLULAR DEVICES

Some facts may help contextualize this important ruling. In 2013, Timothy Carpenter was convicted of robbing Radio Shack and T-Mobile stores where—*ironically*—he stole new smart phones.[28] Because a firearm was involved in the commission of the crimes, the district court sentenced him to 1,395 months, or 116.25 years, in federal prison.[29] During its investigation, the government had obtained extensive location information from Mr. Carpenter's cellular phone, evidence which the

26. *Id.* at 2220 ("Our decision today is a narrow one.").

27. As of the writing of this Article, Judge Brett Kavanagh, a judge for the U.S. Court of Appeals for the D.C. Circuit, has been nominated by President Trump to fill the vacancy left by Justice Kennedy. Judge Kavanaugh is considered by most to be a politically conservative judge. *See, e.g.*, *The Path Ahead for Supreme Court Nominee Brett Kavanaugh*, WASH. POST, https://www.washingtonpost.com/graphics/2018/politics/supreme-court-justice-nominations/?noredirect=on&utm_term=.2a4f5a16eee7 (last updated July 9, 2018).

28. *Carpenter*, 138 S. Ct. at 2212.

29. *Id.* at 2213.

government then used to convict him.[30] Specifically, the government obtained 12,898 location points tracking Mr. Carpenter for over 127 days.[31] Interestingly, only *four* of those location points placed Mr. Carpenter near cell sites where the robberies had occurred.[32]

Technology is certainly our friend, but it is also capable of alarming intrusions and insidious insinuations into our personal lives. The very same technology that has become deeply entrenched into the fabric of daily life can be used to surreptitiously surveil and monitor those who rely on it in ways few could ever have imagined. In its opinion, the Court discussed the constitutionality of the government's warrantless use of the personal information that could be gleaned from "spying smart phones," including the CSLI at issue.[33]

The *Carpenter* Court found the ease with which the government can use smart phones to monitor people's whereabouts throughout the entirety of each day, and then store that information for lengthy periods of time, to be profoundly troubling.[34] The Court ruled the use of such "deeply revealing"[35] information—that had been obtained without a warrant—to be unconstitutional under two lines of legal doctrine.[36] First, the government's use of the CSLI data violated a person's reasonable expectation of privacy under a *Katz* analysis.[37] Second, it fell awry of the third-party doctrine under the *Miller* and *Smith* line of cases.[38]

In rendering its decision, the Court focused greatly on the public's ubiquitous reliance on cellular phones[39] and the great breadth of information that can be obtained from them.[40] The Court observed that personal devices are in widespread use with the vast majority of people relying on them on a daily, if not continual, basis.[41] It also looked to the fact that cellular phones are qualitatively far different today from analog phones—or even cellular phones of a prior generation.[42] These spying smart phones enable the government to obtain a tremendous amount of

30. *Id.* at 2212–13.
31. *Id.* at 2212.
32. *Id.* at 2213.
33. *Id.* at 2217–19.
34. *See id.*
35. *Id.* at 2223.
36. *Id.* at 2214–15.
37. *Id.* at 2217–19.
38. *Id.* at 2219–220.
39. *Id.* at 2211 ("There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people.").
40. *Id.* at 2217–18.
41. *Id.* at 2218.
42. *Id.* at 2217.

information about their users, which includes location data as well as a plethora of other personal information.[43]

Smart phones also often allow access to computer files and other personal information that is virtually stored in "the cloud."[44] Cellular phones have become mini-computers, cameras, stereo systems, telephones, alarm clocks, fitness trackers, and countless other consumer devices—all rolled into one pocket-sized, but very powerful and seemingly omniscient, device. A smart phone's functionality, however, necessarily relies upon the owner's private and often highly sensitive personal information. Bank account balances, credit card account numbers, the names and numbers of loved ones, personal photographs, text messages, health and medical history, fitness tracking, location information, access to digital personal and work files, and all sorts of other personal data are all easily accessible from the cellular phones of most individuals.

II. THE REASONABLE EXPECTATION OF PRIVACY DOCTRINE UNDER KATZ AND THE RECENTLY EVOLVING FOURTH AMENDMENT LANDSCAPE

The Court ultimately ruled that the government's warrantless access to an individual's CSLI was unconstitutional.[45] So let us turn to the first facet of the judicial opinion which focused on a *Katz* analysis. In *Carpenter*, as in *Riley* and *Jones*, the Court retreated a bit from the Supreme Court precedent that seemed to allow law enforcement somewhat greater latitude in the post-9/11 era.[46] Instead, it harked back to one of the Fourth Amendment's most famous legal doctrines that has often historically served to narrow law enforcement's investigative reach. Evoking *Katz*, the Court reaffirmed that citizens have a reasonable expectation of privacy over highly personal information such as the CSLI at issue in this case.[47]

Some of the same privacy concerns the Court voiced in *Jones* and *Riley* resonated in *Carpenter*.[48] All three cases seem to center on the government's intrusive access to private information made possible by

---

43. *See id.*

44. *See, e.g.*, Christopher Soghoian, C*aught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. ON TELECOMM. & HIGH TECH. L. 359, 393–97 (2010).

45. *See Carpenter*, 138 S. Ct. at 2221.

46. *Id.* at 2218–19; *See, e.g.*, Illinois v. Caballes, 543 U.S. 405 (2005); Kyllo v. United States, 533 U.S. 27 (2001).

47. *Carpenter*, 138 S. Ct. at 2217.

48. Although the Court's decision in *Jones* ultimately turned on a property rights analysis as discussed in the *Knotts* and *Karo* line of cases, similar threads of concerns regarding an individual's expectation of privacy arose in *Jones*, *Riley*, and *Carpenter*. *See id.* at 2217–19; Riley v. California, 134 S. Ct. 2473, 2493 (2014); United States v. Jones, 132 S. Ct. 945, 949–52, 955–57, 963–64 (2012).

technological advances.[49] Chief Justice Roberts emphasized in *Carpenter*, as he did in *Riley*, that the public's ever-greater reliance on digital technology is a reality of modern life. Moreover, the widespread use of cell phones, which contain the "privacies of life,"[50] makes individuals' sensitive information particularly susceptible to intrusion.

Not only do cell phones allow access to a great amount of personal information and sensitive data, but cellular phones are often figuratively—if not literally—joined at the hip of their owners. This affords the government a wealth of additional information that derives specifically from the location data.[51] Given that most people carry their phones with them virtually everywhere, Justice Roberts observed that cell-site location records essentially provide the government with "near perfect surveillance, as if it had attached an ankle monitor to the phone's user."[52] This data enables the government to learn precisely where the phone—and thus the person—has been and at what time—as well as what other cellular phones were in the same area at that same time.[53] The *Carpenter* Court made specific reference to the highly intrusive nature of such information, which it characterized as the "detailed, encyclopedic and effortless" tracking of a person using CSLI data.[54]

The Court's observation that people would not expect police to track their every movement over long periods of time, which was exactly what cell site location records did,[55] was pivotal. The Court noted that, as a result of the CSLI, the government was also privy to possibly more sensitive collateral information.[56] This includes every location a person has traveled and nearly everyone she has met.[57] Moreover, the Court noted this information was available to law enforcement not only on a going-forward basis but also historically going back five years—*all without a warrant*.[58]

In *Jones*, the Court expressed similar concern over the government's ability to warrantlessly track, routinely surveil, and record an individual's

---

49. *See Jones* at 132 S. Ct. at 953–54, 963–64; *Carpenter*, 138 S. Ct. at 2217–19; *Riley*, 134 S. Ct. at 2493.

50. *Riley*, 134 S. Ct. at 2494–95 (2014) (citations omitted) ("Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'").

51. *Carpenter*, 138 S. Ct. at 2218.

52. *See id.*

53. *Id.*

54. *Id.* at 2216.

55. *Id.* at 2217.

56. *Id.*

57. *Id.*

58. *Id.* at 2218; Amy Davidson Sorkin, *In Carpenter, the Supreme Court Rules, Narrowly, for Privacy*, NEW YORKER (June 22, 2018), https://www.newyorker.com/news/daily-comment/in-carpenter-the-supreme-court-rules-narrowly-for-privacy ("Generally, cell-phone carriers keep such data for five years, but there is no technological limit.").

every movement[59] that would not have otherwise been subject to public view.[60] Justice Sotomayor worried that warrantless monitoring—such as with a GPS device or a smartphone—could serve to reveal the deeply personal information that derives from location data, such as "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[61] This speaks directly to the "privacies of life"[62] and the very core of our existence. The same alarm raised in *Jones* and *Riley* reemerged in *Carpenter*.[63] The Court therefore ruled a warrant would first be required for law enforcement to obtain location data from cellular phone carriers since Mr. Carpenter had a legitimate expectation of privacy in such information.[64]

III. THE THIRD-PARTY DOCTRINE

The second dimension of the legal analysis centered around the third-party doctrine, the tenet that a person has no legitimate expectation of privacy in information voluntarily turned over to a third party.[65] The *Carpenter* Court narrowed its prior holdings in *United States v. Miller*, which established the third-party doctrine, and in *Smith v. Maryland*, which extended the third-party doctrine to information related to telephone records.[66]

Justice Lewis Powell's words in *Miller* help explain the rationale underlying the third-party doctrine[67]:

> The depositor [i.e. an ordinary citizen] *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.

---

59. United States v. Jones, 132 S. Ct. 945, 953–54 (2012).

60. *Id.* at 955–56; *Carpenter*, 138 S. Ct. at 2217–18.

61. *Jones*, 132 S. Ct. at 955 (quoting People v. Weaver, 12 N.Y.3d 433, 441–42 (2009)).

62. *See Riley*, 134 S. Ct. at 2494–95.

63. *See Carpenter*, 138 S. Ct. at 2217–19.

64. *Carpenter*, 138 S. Ct. at 2221.

65. *Id.* at 2219–220.

66. *Id.* at 2220; Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

67. *Miller*, 425 U.S. at 443 (emphasis added) (citations omitted).

In other words, the *Miller* Court ruled the Fourth Amendment does not preclude the government from obtaining information without a warrant that a person voluntarily provides to a third party.[68] This reasoning rests on the premise that a person loses his "legitimate expectation of privacy" in information he himself reveals to third parties.[69] As such, the *Miller* Court deemed it constitutional that such information be freely passed on to the government.[70]

The *Jones* Court declined to overrule the third-party doctrine; however, it voiced stirrings of concern regarding this legal construct that later reemerged more forcefully in *Carpenter*.[71] Justice Sotomayor, for example, expressed her unease in her concurring opinion in *Jones* as follows[72]:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.

The Court questioned whether individuals would knowingly intend to waive their privacy rights if they allowed third party access to their personal information as they do on a prosaic, everyday basis—often by necessity[73]:

> 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 . . . 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.

She concluded in *Jones*, for example, that "[o]wners of GPS-equipped cars and smartphones do not contemplate that these devices will be used to enable covert surveillance of their movements."[74]

Justice Sotomayor's admonition in *Jones* seems to have presaged the

---

68. *Id.* at 444–46.
69. *See id.* at 443.
70. *Id.* at 443–45.
71. United States v. Jones, 132 S. Ct. 945, 957 (2012).
72. *Id.* at 956–57.
73. *Id.* at 957.
74. *Id.* at 956 (referring to the asterisked discussion of United States v. Karo, 468 U.S. 705, 707 (1984)).

Carpenter ruling.[75] The *Carpenter* Court voiced skepticism over the third-party doctrine as it did in *Jones*.[76] Given the extensive amount of deeply personal information people typically share with third parties on an everyday basis, the *Carpenter* Court concluded that ordinary citizens would likely not expect such information to be freely available to the government without a warrant.[77] The Court noted how certain third parties maintain encyclopedic knowledge on individuals in a manner that was not possible during the time *Miller* and *Smith* were decided[78]:

> Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.

A great degree of the intrusiveness characterizing the government's investigative practices stems from the highly advanced nature of current technology.[79] Within the context of today's digital age, advanced technology has allowed the sort of intrusion that had not been previously possible. But this is the reality of our new digital world.[80]

Such observations helped inform the Court's decisions in *Jones* and *Riley*.[81] The Court remarked that "seismic shifts in digital technology [have] 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."[82] This is possible because "modern cell phones generate increasingly vast amounts of increasingly precise CSLI."[83]

The Court concluded that an individual has a legitimate expectation of privacy over such CSLI that he would not intend to renounce only because of a cursory decision to use third party services[84]:

> Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by

75. *Id.* at 957.
76. *Id.* at 955–56; *Carpenter*, 138 S. Ct. at 2217–18.
77. *Carpenter*, 138 S. Ct. at 2217.
78. *Id.* at 2219.
79. *See id.* at 2218–19.
80. *See id.*
81. *Id.* at 2217–19; Riley v. California, 134 S. Ct. 2473, 2493 (2014); United States v. Jones, 132 S. Ct. 945, 955–57, 963–64 (2012).
82. *Carpenter*, 138 S. Ct. at 2219.
83. *Id.* at 2212.
84. *Id.* at 2217.

> 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.

The dangers inherent to such trends and the reality of the greatly advanced digital world in which we live may have influenced the Court's decision. Although the *Carpenter* Court did not overrule *Smith* and *Miller* in their entirety, it also "decline[d] to extend *Smith* and *Miller* to cover these novel circumstances."[85] *Carpenter* may foreshadow a further narrowing of the third-party doctrine; and it will be interesting to see whether this contraction continues. The Court may well recognize that the increasing government intrusion possible as a result of ever-advancing technology, coupled with individuals' unintended relinquishment of private information to third parties, may run afoul of the Fourth Amendment.

IV. THE HIGHLY INTRUSIVE NATURE OF DIGITAL TECHNOLOGY MAY POTENTIALLY LEAD TO A FURTHER NARROWING OF THE THIRD-PARTY DOCTRINE

Notwithstanding the significance of this judicial decision, Chief Justice Roberts specifically characterized it as having a relatively "narrow" reach.[86] He noted, for example, that it does not affect other aspects of the third-party doctrine, such as banking records.[87] It also does not prevent warrantless "real time CSLI information or 'tower dumps,'"[88] access to cellular tower data in emergencies, or retrieval for "national security reasons."[89] Despite this caveat, this decision may set the stage for future legal challenges.[90] The *Carpenter* decision represents an important, albeit narrow, contraction of well-established Fourth Amendment precedent.

Because the *Carpenter* Court focused its concern on advanced technologies that allow the government to engage in highly intrusive investigative practices, areas involving warrantless data retrieval seem particularly ripe for future Supreme Court review.[91] Such future

85. *Id*.
86. *Id.* at 2220.
87. *See id.*; *see also* United States v. Miller, 425 U.S. 435 (1976).
88. *Carpenter*, 138 S. Ct. at 2220.
89. *Id.*
90. *Id.*; *see* Sorkin, *supra* note 58.
91. *Carpenter*, 138 S. Ct. at 2217–19; *see also, e.g.*, Soghoian, *supra* note 44, at 386.

challenges could increasingly constrict the scope of the third-party doctrine and further stem the greater investigative latitude the government has enjoyed in the post-9/11 era.[92] After all, the public seems to have begun to increasingly tolerate a certain degree of diminution in civil liberties in exchange for a greater sense of safety in a society rife with perceived terrorist threats.

The significant issues expressed in *Jones*, *Riley*, and *Carpenter* make it foreseeable that similar Fourth Amendment challenges are far from over.[93] Cloud computing, for example, seems like a perfect "domain" for improper law enforcement investigation and surveillance that may later result in judicial review[94]:

> The shift to cloud computing obviously brings many benefits to law enforcement: significantly reduced manpower requirements, no need to go before a judge or establish probable cause in order to obtain a warrant, as well as the complete elimination of physical risk to agents who might be shot or attacked during a raid.

From the government's point of view, the potential benefits of such digital investigations are myriad and deliciously tempting. With the advent of cloud computing, a person's entire digital life can be stored in cyberspace. Since files are already uploaded and stored on third-party servers, the government has far easier and likely greater access to an individual's digital information than it would with a traditional search of physical items in a home.[95] More importantly, the government can also

---

92. *See, e.g.*, Illinois v. Caballes, 543 U.S. 405 (2005); Kyllo v. United States, 533 U.S. 27 (2001). These cases represent judicial precedent that arguably afforded the government greater investigative latitude. *See also*, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (affording the government greater investigative latitude in order to fight the "War on Terror").

93. *See* USA PATRIOT ACT; *Carpenter*, 138 S. Ct. at 2217–19; Riley v. California, 134 S. Ct. 2473, 2493 (2014); United States v. Jones, 132 S. Ct. 945, 955–57, 963–64 (2012); *Caballes*, 543 U.S. at 405; *Kyllo*, 533 U.S. at 27.

94. Soghoian, *supra* note 44, at 387.

95. Here is one explanation of why this is: "So in this digital age, police often do not need to show probable cause of a crime when they want to find out details about your life that they used to find in your home. Instead, they can get your private files from corporations that store your records on their computers. And instead of a search warrant, the police might just need a subpoena—which is 'trivially easy to issue,' says Bankston of the Center for Democracy and Technology. Law enforcement doesn't need a judge's approval to obtain subpoenas—prosecutors can sign them on their own, as can authorized employees at federal and state agencies. And law enforcement agents don't need evidence that there's likely a crime. They need only to be able to show that the records they want are relevant to an investigation." Daniel Zwerdling, *All Things Considered: Your Digital Trail: Does The Fourth Amendment Protect Us?*, NPR (Oct. 2, 2013, 1:00 PM), https://www.npr.org/ sections/alltechconsidered/2013/10/02/228134269/your-digital-trail-does-the-fourth-amendment -protect-us.

seek to bypass the warrant requirement and obtain the digital files with a mere subpoena, arguing that the individual had himself turned over the information to a third party.[96] A government agent would certainly welcome the ability to virtually access a target's most personal information in cyberspace, conveniently from the comfort of a well-lit, air-conditioned office—perhaps while sipping a cup of coffee.[97] No more cramped late-night stake outs or last minute surveillance runs.[98]

A cloud user—or government interloper—can also effortlessly manipulate, retrieve, and organize a typically extensive array of digital files at its leisure. This includes potentially unlimited, "on demand" access to a complete library of a person's most private information—including writings, photographs, and financial data—figuratively *and* literally. Depending on the third-party entity holding the sought-after information, the government could likely access this information with the mere request of a subpoena—a simple stroke of a pen—without the safeguard of a warrant.[99] After all, a subpoena requires very little.[100] A police officer or federal agent need only justify the request according to his department's own internal policies, which may be faulty or woefully deficient.[101] There is no judicial oversight of the request,[102] and law enforcement is not immune from mistake, impropriety, or abject wrongdoing. The implications of the government's far-reaching and relatively unfettered access to an individual's private information are grave and should therefore raise concerns for all.

V. IS THE GOVERNMENT'S VAST ARRAY OF AGGRESSIVE—AND HIGHLY INTRUSIVE—COVERT SURVEILLANCE PRACTICES CONSTITUTIONAL?

The *Carpenter* Court underscored the concern that investigational practices currently employed by the government are alarmingly—and unlawfully—intrusive.[103] The Internet of Things (IoT) is another area of technology ripe for governmental abuse. The IoT affords the public a vast array of conveniences while also concomitantly creating a potential conduit for the government to violate the sanctity of our homes and insinuate itself into our private lives.[104]

---

96. *Id.*
97. *See id.*; Soghoian, *supra* note 44, at 386.
98. *See Carpenter*, 138 S. Ct. at 2217.
99. Zwerdling, *supra* note 95.
100. *Id.*
101. *See id.*
102. *See id.*
103. *See Carpenter*, 138 S. Ct. at 2223.
104. Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. 805, 805 (2016) ("'Smart objects' connected to the 'Internet of Things' present new possibilities for technological surveillance.").

"Smart" televisions and other "smart" devices, for example, can monitor and store sounds and conversations that occur *inside* of the homes in which they are located—including bedrooms, living rooms, and nurseries.[105] The audio captured could be highly personal, including, for example, a child's giggle, a baby's gurgle, or a lover's whisper. Samsung has confirmed that "*even if the owner opts out of the voice-recognition feature . . . the set will still capture what is said*."[106] But the intrusion does not end there: After capturing those sounds, *these smart devices can possibly transmit that audio to third parties.*[107] Please allow me to rephrase: Some stranger somewhere might very well have the ability to spy on you or your family's most private moments as well as gain information about your children and your family's patterns of life.[108]

Depending on future judicial interpretations of *Carpenter*, the IoT could possibly bestow the government with a virtual superhighway into the most private areas of our lives. Questions of legality and constitutionality aside, many of us would consider these sorts of covert intrusions quite alarming. To most people, the implications of this are enormous. Many would feel these sorts of intrusions are not just wrong, but truly violating.

Of course, this is but one example. There are myriad other examples of covert surveillance which may potentially be available to police without a warrant. Some retail stores use cameras with facial recognition and surreptitious biometric iris scanning technology that can be easily hidden, for example, in mannequins.[109] The government itself utilizes long-distance iris scanners to surveil public places and amass biometric information on its citizenry—surreptitiously and without consent.[110] License plate scanners of automobiles on the roadway and in parking lots are in widespread use, monitoring our movements, driving habits, and travel patterns.[111] "Eyes in the Sky" have become increasingly common

---

105. *See, e.g.*, Martha Neil, *Be Careful What You Say When Your Smart TV Is On, Samsung Warns Customers*, A.B.A. J. NEWS. WKLY. (Feb. 9, 2015, 10:15 AM) (emphasis added), http://www.abajournal.com/news/article/be_careful_what_you_say_when_your_smart_tv_is_on_samsung_warns_customers.

106. *See id.*

107. *See id.*

108. *See id.*; Zwerdling, *supra* note 95.

109. *See* Mark G. Milone, *Biometric Surveillance: Searching for Identity*, 57 BUS. LAW. 497 (2001); *Facial Recognition*, EFF, https://www.eff.org/pages/face-recognition (last visited Aug. 31, 2018).

110. Milone, *supra* note 109; *Facial Recognition*, EFF, *supra* note 109.

111. *See Automated License Plate Readers (ALPRs)*, EFF, https://www.eff.org/pages/automated-license-plate-readers-alpr (last visited Aug. 31, 2018) ("Automated license plate readers (ALPRs) are high-speed, computer-controlled camera systems that are typically mounted on street poles, streetlights, highway overpasses, mobile trailers, or attached to police squad cars. ALPRs automatically capture all license plate numbers that come into view, along with the

as law enforcement has begun to employ warrantless drone surveillance programs.[112] The government has monitored electronic communications and accessed the stored data of individuals, including emails and computer files—all surreptitiously and without consent.[113] Indeed, the government has quietly built a series of warehouses of truly immense proportion in the Utah desert[114] to store the vast amounts of metadata it has compiled on its citizens.[115]

VI. THE COURT'S CALCULUS OF PRIVACY IN A SOCIETY MARKED BY INCREASING GOVERNMENT SURVEILLANCE

Against a backdrop of stunningly advanced surveillance technology and the strictures of the United States Constitution, the question of how individual privacy comports with the need for police investigation is a complex and impressively difficult one. In the current political landscape, judicial vigilance becomes increasingly important in protecting the appropriate dimensions of individual privacy. The grave risks of

---

location, date, and time. The data, which includes photographs of the vehicle and sometimes its driver and passengers, is then uploaded to a central server.").

112. *See, e.g.*, Nina Gavrilovic, *The All-Seeing Eye In The Sky: Drone Surveillance and the Fourth Amendment*, 93 U. DET. MERCY L. REV. 529, 529–30 (2016); *see also Drones/Unmanned Aerial Vehicles*, EFF, https://www.eff.org/pages/dronesunmanned-aerial-vehicles (last visited Aug. 31, 2018).

113. *See, e.g.*, James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html; James Risen & Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. TIMES (Dec. 21, 2005), https://www.nytimes.com/2005/12/21/politics/spying-program-snared-us-calls.html ("A surveillance program approved by President Bush to conduct eavesdropping without warrants has captured what are purely domestic communications in some cases, *despite a requirement by the White House that one end of the intercepted conversations take place on foreign soil*, officials say." (emphasis added)). *See generally NSA Spying: How It Works*, EFF, https://www.eff.org/nsa-spying/how-it-works (last visited Aug. 31, 2018) ("In the weeks after 9/11, President Bush authorized the National Security Agency (NSA) to conduct a range of surveillance activities inside the United States, which had been barred by law and agency policy for decades.").

114. The government's Stellar Wind Program is located at Camp Williams near Bluffdale, Utah. It is also known as the Intelligence Community Comprehensive National Cybersecurity Initiative Data Center. *See, e.g.*, Steve Fidel, *Utah's $1.5 Billion Cyber-Security Center Under Way*, DESERET NEWS (June 6, 2011, 1:10 AM), http://www.deseretnews.com/article/705363940/Utahs-15-billion-cyber-security-center-under-way.html.

115. Tim Cushing, *NSA's Stellar Wind Program Was Almost Completely Useless, Hidden from FISA Court by NSA and FBI*, TECHDIRT (Apr. 27, 2015, 12:34 PM), https://www.techdirt.com/articles/20150427/11042430811/nsas-stellar-wind-program-was-almost-completely-useless-hidden-fisa-court-nsa-fbi.shtml ("A huge report (747 pages) on the NSA's Stellar Wind program has been turned over to Charlie Savage of the New York Times after a successful FOIA lawsuit. Stellar Wind has its basis in an order issued by George W. Bush shortly after the 9/11 attacks. Not an executive order, per se, but Bush basically telling the NSA that it was OK to start collecting email and phone metadata, as well as warrantlessly tap international calls into and out of the United States.").

governmental abuse may militate in favor of strengthened judicial oversight in determining the parameters of the state's broad investigative powers. Strong privacy protections may indeed serve to function as a safeguard against the risks of governmental overreach, police misconduct, and improper warrantless surveillance.

It is possible the increasingly intrusive trend of governmental investigative activities in the post-9/11 period helped shape the *Carpenter* ruling and the resulting slight contraction of the third-party doctrine toward a more appropriate Fourth Amendment equipoise. Although characterized as a "narrow" ruling by the *Carpenter* Court, its significance could likely be far greater than stated at first blush—especially given the sort of advanced surveillance technology that has yet to come to light. Indeed, the Court may rely on its rationale in the *Carpenter* decision in the event of future legal challenges of warrantless digital searches where the government invokes the third-party doctrine as justification for those searches. Only time will truly tell. The Court's decisions in *Carpenter*, *Riley*, and *Jones*, however, could signal the beginnings of a contraction in the progressively greater investigative latitude the government has been enjoying in the post-9/11 era.