Carpenter v. United States

Davina Anderson

138 S. CT. 2206 (2018)

In *Carpenter v. United States*, the United States Supreme Court reversed and remanded the Sixth Circuit's judgment that the petitioner, Timothy Carpenter, lacked a reasonable expectation of privacy in his cell-site location information (CSLI) collected by the Federal Bureau of Investigations (FBI), because he voluntarily shared that information with his wireless carriers.[1] The Supreme Court held that Carpenter had a legitimate privacy interest in his CSLI and that the Government should have obtained a warrant for Carpenter's CSLI under the Fourth Amendment, instead of relying solely on a court order under the Stored Communications Act (SCA).[2]

I. BACKGROUND

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[3] According to the Court, "the basic purpose of [the Fourth] Amendment, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[4] Thus, when an individual seeks to preserve something as private, and his expectation of privacy is reasonable, official intrusion generally requires a warrant supported by probable cause.[5]

CSLI is a time-stamped record generated whenever a phone connects to a cell site.[6] Cell phones continuously scan their environments looking for the best signal, which generally comes from the closest cell site.[7] Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features.[8] With the development and technological expansion

1. Carpenter v. United States, 138 S.Ct 2206, 2209 (2018).
2. *See id.* at 2211.
3. U.S. Const. amend. IV.
4. *Carpenter,* 138 S.Ct. at 2213 (quoting *Camara v. Mun. Court of City and Cty. of San Francisco*, 387 U.S. 523, 528 (1967)).
5. *See id.* at 2209.
6. *See id.* at 2211.
7. *See id.*
8. *See id.*

of cell-sites, wireless carriers can pinpoint a phone's location within 50 meters.[9]

***

In 2011, police officers arrested four men suspected of robbing a series of Radio Shacks and T-Mobile stores in Detroit.[10] One of the suspects confessed that over a period of four months, the group had robbed nine different stores in Michigan and Ohio.[11] During interrogation, the suspect identified several accomplices and gave the FBI their cellphone numbers.[12] Based on the information given by the suspect, the Government applied for court orders under the SCA Section 2703(d) for petitioner, Timothy Carpenter, and several other suspects.[13] Section 2703(d) of the SCA "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.'"[14] Under the SCA, the Government obtained 152 days of CSLI from MetroPCS and seven days' worth of CSLI from Sprint.[15] From the 152 days of CSLI, the Government obtained "12,898 location points cataloging Carpenter's movements[,]" averaging 101 data points per day.[16] Carpenter moved to suppress the CSLI because he believed that the Government's seizure of the cell-site records without a warrant violated the Fourth Amendment.[17]

In *Carpenter*, the Court grappled with how to apply the Fourth Amendment to a "new phenomenon"—personal location information maintained by a third party—because it does not fit neatly under any existing precedent.[18] The Court ultimately addressed the question: "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements"[19]

II. ANALYSIS

To determine whether the Fourth Amendment applies, the Court first determined whether Carpenter sought to preserve his CSLI as private and

9. *Id.* at 2219.
10. *See id.* at 2212.
11. *See id.*
12. *See id.*
13. *See id.*
14. *Id.*
15. *See id.*
16. *Id.* at 2212.
17. *See id.* at 2209.
18. *Id.* at 2214, 2216.
19. *Id.* at 2211.

whether his expectation of privacy is one that society recognizes as reasonable.[20] Although there is no clear-cut definition of what society should recognize as reasonable privacy expectations, the Court looked to "historical understandings 'of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted.'"[21] The Court mentioned that one of the aims of the Framers of the Constitution when drafting the Fourth Amendment was to limit police surveillance.[22] Keeping the intentions of the Framers in mind in regard to limiting police surveillance, the Court looked at two issues in this case (1) whether Carpenter has an expectation of privacy in his physical location and movements; and (2) whether Carpenter has an expectation of privacy in the CSLI that is shared with his wireless carrier(s).[23]

A. Does Carpenter have an expectation of privacy in his CSLI records?

The Court relied on its prior ruling in *United States v. Jones* to aid in its decision on this issue.[24] In *Jones*, FBI agents installed a GPS tracking device on Jones' vehicle and tracked him for 28 days.[25] The Court held that, because GPS tracking devices track every movement an individual makes in that vehicle, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy – regardless whether those movements were disclosed to the public at large."[26]

Here, the Court, by comparing GPS and cell phone location information, held that CSLI presents greater privacy concerns than GPS monitoring because CSLI gives the Government "near perfect surveillance and allow it to travel back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers."[27] Furthermore, unlike GPS tracking that can be left in the car, a person carries their cellphone everywhere, causing the Government to access pertinent, timely information.[28] CSLI surveillance provides an "intimate window into a person's life, revealing not only his particular movements, but his 'familial political, professional, religious, and sexual associations.'"[29]

Therefore, similar to the ruling in *Jones*, the Court held that Carpenter's reasonable expectation of privacy regarding his physical

---

20. *See id.* at 2213.
21. *See id.* at 2214.
22. *See id.*
23. *See id.* at 2209.
24. *See* United States v. Jones, 565 U.S. 400 (2012).
25. *See id.* at 403.
26. *See Carpenter*, 138 S.Ct 2206, 2215 (quoting *Jones,* 565 U.S. at 430).
27. *Id.* at 2210.
28. *See id.* at 2218.
29. *See id.* at 2217-18.

movements were violated when the Government accessed his CSLI from MetroPCS and Sprint.[30]

B. Is Carpenter's Expectation of Privacy Reasonable by Society?

The Court analyzed whether Carpenter has an expectation of privacy through prior rulings in both *United States v. Miller* and *Smith v. Maryland*. In *Smith*, the Court held that an individual does not have an expectation of privacy in information voluntarily turned over to third parties.[31] The Court extended *Smith's* ruling in *Miller*, when they held that no expectation of privacy exists "even if the information is revealed on the assumption that it will be used for a limited purpose."[32] As a result of both rulings, collectively known as the "third-party doctrine," the Government is typically allowed to obtain third-party information through a subpoena without triggering Fourth Amendment concerns.[33]

Despite its prior rulings in *Smith* and *Miller*, the Court did not extend these ruling to cover the new circumstances in *Carpenter*.[34] The Court stated that *Smith* and *Miller* was about limited personal information (i.e., pen registers and bank records), whereas the present case handles exhaustive personal data collected by wireless carriers.[35] Thus, according to the Court, *Carpenter* implicates privacy concerns far beyond those considered in both *Smith* and *Miller*.[36]

In *Carpenter*, the Court also discussed the "voluntary exposure" rationale under the third-party doctrine. The Court held that cell phone location information is not voluntarily shared because (1) cell phones are an "insistent part of daily life" and given the advancement in technology, it is unreasonable for an individual to not have one; and (2) cell phones always generate CSLI, without any "affirmative act on the part of the user beyond powering up."[37] The Court also stated that "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[38]

Therefore, unlike the rulings in *Smith* and *Miller*, the fact that the Government obtained CSLI from a third party does not overcome Carpenter's claim to Fourth Amendment protection.[39] The Government's possession of

---

30. *See id.* at 2219.
31. *See id.* at 2216 (quoting *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979)).
32. *Id.* (quoting *United States v. Miller*, 425 U.S. 435, 443 (1976)).
33. *See id.* at 2216
34. *See id.* at 2217.
35. *See id.* at 2219.
36. *See id.* at 2220.
37. *Id.* at 2220.
38. *Id.*
39. *Id.*

the CSLI was a search within the meaning of the Fourth Amendment and therefore a warrant was required.[40]

Given that the Court ruled that acquisition of Carpenter's CSLI by the Government was a search, the Court held that the Government should have obtained a warrant.[41] The acquisition of CSLI issued through a court order under SCA Section 2703(d) was not enough because the "reasonable grounds" standard required under the SCA falls short of the "probable cause" required for a warrant.[42] While the Court held that moving forward the Government will need a warrant to access CSLI, they realized that case-specific exceptions may occasionally apply.[43] For example, "one well-recognized exception applies when 'the exigencies of the situation' make the needs for law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment."[44] Exigencies include: "the need to pursue a fleeing suspect, protect individuals threatened with imminent harm, or prevent the imminent destruction of evidence."[45] The rule set forth in regard to obtaining a warrant for CSLI does not limit law enforcement's ability to respond to an ongoing emergency.[46]

III. CONCLUSION

The Supreme Court held that because of the unique nature of CSLI, information held by a wireless carrier (third party) does not by itself overcome a claim to Fourth Amendment protection.[47] The Court also held that an individual has an expectation of privacy in his or her CSLI information. As such, the CSLI gathered from Carpenter's wireless carriers was the product of a search, thus requiring a warrant.[48] The Court also makes it clear that their decision is a narrow one, meaning that it does not express views on matters unrelated to CSLI or "tower dumps."[49]

***

Kennedy, J., Thomas, J., & Alito, J., dissenting: The Court's ruling puts lawful and "congressionally authorized" criminal investigations at risk and places undue restrictions on law enforcement.[50] Justice Kennedy stated

---

40. *See id.* at 2221.
41. *See id.*
42. *See id.*
43. *See id.* at 2222.
44. *Id.* at 2223.
45. *Id.*
46. *See id.*
47. *See id.* at 2217
48. *See id.*
49. *See id.* at 2220 (tower dumps are a download of information on all devices connected to a particular cell site during a particular interval).
50. *See id.* at 2223.

that cell-site records are no different than other kinds of business records (i.e., pen registers and bank records) that the Government has a right to obtain without a warrant from a third party.[51] While the majority does not rely on its prior rulings in *Smith* and *Miller*, in both of those cases, the Court held "defendants could 'assert neither ownership nor possession' of records because the records were created, owned and controlled by companies."[52] That is similar to the facts here, and therefore Carpenter did not have a "reasonable expectation of privacy in the information that was 'voluntarily conveyed to the [companies] and exposed to their employees in the ordinary course of business.'"[53] The Court should not have rejected a straightforward application of *Smith* and *Miller*.[54]

Also discussed in the dissent was a more stringent view on whose property was searched and what a search entails. Justice Thomas points out, "[t]his case should not turn on 'whether' a search occurred, [] it should turn, instead, on *whose* property was searched. By obtaining the cell-site records of MetroPCS and Sprint, the Government did not search Carpenter's property."[55] Furthermore, Carpenter does not explain how he has a property right in the companies' records.[56] To be eligible for Fourth Amendment protections, Carpenter must prove that the CSLI are his.[57] Justice Thomas also stated that the major problem within this case is the Court's use of the "reasonable expectation of privacy test," which was first used in *Katz v. United States*.[58] The "reasonable expectation of privacy test[,]" now known as the *Katz* test, "invites courts to make judgments about police and not the law."[59] The *Katz* test strays from the Fourth Amendment because it focuses on the "concept of 'privacy,' … [which] does not appear in the Fourth Amendment."[60] Regarding the search, the Court "ignores the basic distinction between an actual search … and an order merely requiring a party to look through its own records and produce specified documents."[61] Not every subpoena needs to be supported by probable cause.[62] If that were the case, crimes such as "terrorism, political corruption, white collar crime, and many other offenses" would be hindered.[63] The Court should not have allowed a defendant to object to the search of a third party's property, because doing so destabilizes long-established Fourth Amendment doctrine.[64] The Fourth Amendment

---

51. *See id.*
52. *See id.* at 2227.
53. *Id.*
54. *See id.* at 2230.
55. *Id.* at 2235.
56. *See id.* at 2242.
57. *See id.*
58. *See id.* at 2236.
59. *See id.*
60. *See id.* at 2239.
61. *See id.* at 2247.
62. *See id.*
63. *See id.*
64. *See id.*

guarantees "the right of the people to be secure in *their* [own] persons, houses, papers, and effects."[65]

Justice Gorsuch in his separate dissent poses an interesting question; what is left of the Fourth Amendment?[66] His three responses to his question are: first, ignore the problems and maintain the third-party doctrine of *Smith* and *Miller*.[67] Second, set the rulings in *Smith* and *Miller* aside and analyze cases under the *Katz* "reasonable expectation of privacy" standard.[68] In order to do so, *Katz's* problems with the Fourth Amendment should be understood by the courts.[69] He further explains that, "[t]he Amendment's protections do not depend on the breach of some abstract 'expectation of privacy,' whose contours are left to the judicial imagination."[70] Third, Justice Gorsuch explains to look for answers elsewhere.[71] Unlike in *Katz*, the right to assert a Fourth Amendment claim should not depend on an individual's ability "to appeal to a judge's personal sensibilities about the 'reasonableness' of your expectations of privacy."[72] It should be tied to the law, rather than their own policy judgments and/or biases.[73]

65. *Id.* at 2257.
66. *See id.* at 2262.
67. *See id.*
68. *See id.*
69. *See id.* at 2264.
70. *Id.*
71. *See id.*
72. *See id.* at 2267.
73. *See id.* at 2268.