Privacy and the third-party doctrine in the digital age
Carpenter v. United States, 585 U.S., 138 S. Ct. 2206, US Supreme Court, 22 June 2018

On 22 June 2018, the US Supreme Court (‘the Court’) handed down its decision in a case that drew significant public attention and interest from various parties including privacy experts, law enforcement, the criminal defence bar and some of the largest technology service providers. In a 5-4 decision, the Court ruled that law enforcement cannot access an individual’s historical cell-site location information (‘CSLI’) from a cell phone service provider without first obtaining a warrant supported by probable cause. The case stands as a significant development in jurisprudence on the Fourth Amendment of the US Constitution concerning an individual’s legitimate expectation to privacy - particularly as it concerns the increasingly important role of technology in daily life.

Background
The case arose out of a series of armed robberies of Radio Shack and T-Mobile stores around Detroit. In 2011, law enforcement arrested four suspects, one of whom identified 15 accomplices and provided their cell phone numbers to the Federal Bureau of Investigation (‘FBI’) to aid in its investigation. Based on the information provided by the suspect, prosecutors in the case applied for court orders under the Stored Communications Act 1986 to obtain cell phone records for the individuals identified, including the petitioner Timothy Carpenter. Based on the standard supplied by the Stored Communications Act, which allows the Government to obtain a court order compelling the disclosure of telecommunications records held by a third party by offering ‘specific and articulable facts showing that there are reasonable grounds to believe’ that the records sought are ‘relevant and material to an ongoing investigation’, prosecutors in the case were able to obtain CSLI information from Carpenter’s mobile phone carriers, Sprint and MetroPCS.

The Government obtained 127 days’ - roughly four months’ - worth of records from MetroPCS, and two days’ worth of records from Sprint. Between the two separate orders, the Government obtained 12,898 location points showing Carpenter’s whereabouts during the material time period.

The case at first instance
At trial, Carpenter moved, unsuccessfully, to suppress the CSLI records, arguing that they were obtained without a warrant, in violation of the Fourth Amendment. The CSLI records were admitted at trial, along with expert testimony from an FBI agent, who explained that, each time a cell phone checks into a mobile network, it produces a time-stamped record of the cell site and the particular sector of the cellular network in which the phone was used. With this information, the Government was able to demonstrate that Carpenter’s phone was near the scene of four of the robberies at exactly the times that they took place. Carpenter was subsequently convicted on six counts of robbery and five counts of carrying a firearm during a federal crime of violence. He was sentenced to over 100 years in prison.

Appeal
Carpenter appealed his conviction to the Sixth Circuit, which affirmed the trial court’s decision. The Sixth Circuit relied almost entirely on the ‘third-party doctrine’ that the Supreme Court had expounded in United States v. Miller (1976) (‘Miller’) (holding that Fourth Amendment protections did not extend to an individual’s bank account and transaction records held by the bank) and Smith v. Maryland (1979) (‘Smith’) (holding that an individual did not have a reasonable expectation of privacy to telephone numbers voluntarily conveyed to the phone company as a means of establishing communication). The Sixth Circuit held that Carpenter did not have a legitimate expectation of privacy in the CSLI information because he had voluntarily shared it with a third party - namely, his mobile phone carriers.

In reversing the Sixth Circuit, the Court spurned such a mechanical application of the ‘third-party doctrine.’ Instead, the Court framed the case, and its analysis, around the intersection of two contrasting lines of cases, each of which implicated its own separate privacy considerations. The first line of cases that the Court considered concerned the legitimate expectations of privacy that a person may hold in his or her physical location and movement, and the second concerned the aforementioned third-party doctrine.

In the first line of cases, the Court had previously ruled that individuals generally should not expect their physical location to be protected from law enforcement surveillance. In the 1983 case of United States v. Knotts (‘Knotts’), the Court held that a “person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to the other.” The Court’s decision in Knotts was premised on the notion that the movements and final destination of a vehicle were “voluntarily conveyed to anyone who wanted to look,” such that a tracking beeper that assisted police in following a suspect during a single, discrete automobile journey did not rise to the level of arbitrary government intrusion that the Fourth Amendment was designed to protect against. Significant to the Court’s later analysis in Carpenter, however, was the fact that the Knotts court’s decision reserved the question of whether “different constitutional principles may be applicable” if “twenty-four hour surveillance of any citizen of this country [were] possible.”
In United States v. Jones (2012)\(^1\) ("Jones"), the Court considered more sophisticated tracking technology in the form of a global positioning system ("GPS") device that had been installed on a suspect's vehicle to monitor its movements over the course of 28 days. In Jones, the Court determined that the tracking was a warrantless search, in violation of the Fourth Amendment. While the Court's judgment in Jones relied on the physical trespass on the suspect's vehicle to install the tracker, the concurring judges opined that similar privacy concerns would be raised by secretly activating the stolen vehicle tracking on the car or by conducting GPS tracking of the driver's cell phone. The concurrences noted that the capacity of GPS technology to track every movement that a person makes - particularly when such technology is utilised over an extended period of time - infringes on an individual's expectations of privacy, even if the movements are disclosed to the public at large.

The Carpenter decision expressed concern that historical CSLI presents an even greater invasion of privacy than GPS monitoring does, because people carry their cell phones virtually everywhere, noting that:

> "Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious and sexual associations.' [..]"

These location records "hold for many Americans the "privacies of life"."\(^2\)

The Court next considered and distinguished the line of precedent that established the 'third party doctrine,' under which law enforcement routinely obtains records without a search warrant, including records of telephone numbers dialled and received by a mobile phone, bank statements and credit card statements. In Carpenter, the Court recognised that CSLI records composed a "qualitatively different category" than the bank records and phone numbers at issue in those cases. In Smith and Miller, the Court had determined that in sharing transaction information with the third parties at the bank and telephone companies, the individuals had assumed the risk that those records would be divulged to the police. However, in its more recent decision in Riley v. California (2014)\(^3\), the Court had held unanimously that the warrantless search of the digital content of a cell phone was unconstitutional because cell phones "differ in both a quantitative and a qualitative sense from other objects"\(^4\) that people carry with them, given their immense storage capacity for information revealing "the sum of an individual's private life."\(^5\)

In addition to pointing to the sheer breadth of the records that can be accessed from an individual's cell phone, the Court's decision in Carpenter expressed significant concern about the "retrospective quality"\(^6\) of the CSLI data, which gives the Government the ability to reconstruct precisely a person's movements in a way that was previously beyond the scope of the available evidence. Because CSLI is collected almost continuously, the ability for law enforcement to retrace a suspect's whereabouts would be limited only by the retention periods of the wireless provider, which may retain such records for up to five years. Further, because of the ubiquity of cell phones in modern society (the decision begins by noting that there are approximately 396 million cell phone service accounts for a population of 326 million people), this ability to track an individual’s movements can be used against anyone, regardless of whether they are the subject of an investigation. As the Court pointed out, "whenever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may - in the Government's view - call upon the results of that surveillance without regard to the constraints of the Fourth Amendment."\(^7\)

Despite Carpenter’s emphasis that the Government must obtain a warrant to compel the production of documents protected by the Fourth Amendment that are in the hands of third parties, the Court suggested that, ultimately, such circumstances would be rare, stating, "The Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations."\(^8\) Moreover, the Court made it clear that the ruling should be narrowly construed as relating to the facts of the case, and declined to extend its ruling to "conventional surveillance techniques and tools, such as security cameras" or "business records that might incidentally reveal location..."\(^9\)
information\textsuperscript{18}.\textsuperscript{19} In addition, the Court allowed some room for warrantless searches on historical CSLI under certain exigent circumstances, including the need to pursue a fleeing suspect, protect individuals from imminent harm or prevent the destruction of evidence. Notably, the Court left open the possibility that historical CSLI for a period of less than seven days might be obtained without a warrant\textsuperscript{20}\textsuperscript{21}.

A number of prominent tech companies joined an amicus brief, which argued in support of a warrant requirement for the CSLI information at issue in this case\textsuperscript{22}\textsuperscript{23}. In support of their position, those companies were eager to point out that they had made extensive efforts to limit government access to their records, absent the proper showing, while providing greater transparency to customers regarding those requests. With the rapid growth in utilisation of network-connected, Internet of Things technologies that collect comprehensive digital troves of information about individuals simply as a consequence of their operation, the service providers appealed for more flexible frameworks for handling government requests in the future.

The Court’s analysis appears to do just that, by shifting the focus of the inquiry away from the simple technicalities of whether that information was disclosed to a third party to one that emphasises the nature of the underlying information and the individual and societal expectations of privacy that may entail. While the decision has been noted by many commentators as having a fairly broad nature of the underlying information and investigative methods brought about by the proliferation and advancement of new technologies. Further, while the decision may have weakened the third-party doctrine, it did not completely remove that principle from the debate. While the Court’s decision entrenches the principle that individuals have a legitimate expectation of privacy in their physical movements as captured through CSLI that is stored by a third party, the logic underpinning that expectation - that CSLI is “detailed, encyclopedic and effortlessly compiled”\textsuperscript{24} - does not necessarily extend to other new technological phenomena that pose privacy concerns.

For example, many would contend that individuals also have a legitimate expectation of privacy in a DNA profile generated through the use of an at-home testing kit. While DNA testing may share phenomena that pose privacy concerns. For example, many would contend that individuals also have a legitimate expectation of privacy in a DNA profile developed through the use of an at-home testing kit. While DNA testing may share

The views expressed in this article are those of the authors and not necessarily those of BakerHostetler or its clients.

2. 18 U.S.C. §2703(d).
7. Ibid. at 281, 282.
8. Ibid. at 281.
9. Ibid. at 283-284.
13. Ibid. at 2489.
14. Ibid.
16. Ibid.
17. Ibid. at 2222.
18. Ibid. at 2220.
19. Ibid. at 2217, n. 3.
20. See ‘Brief for Technology Companies as Amici Curiae in Support of Neither Party’.
24. Miller. After Carpenter, the weight that should be given to that type of affirmative sharing remains an open question.

Further, as recent events have demonstrated, an individual’s expectation of privacy may not always match the realities of third party service providers’ business activities. Many such service providers generate a significant amount of revenue by selling customer data to advertisers and data brokers. Sprint, one of the two carriers implicated in Carpenter, only recently announced that it had discontinued a practice of sharing customer location data with a series of third parties, after one such company was investigated by Senator Ron Wyden’s office for misuse of the data\textsuperscript{25}. As some companies attempt to distinguish themselves in the marketplace through privacy practices that may include policies for responding to requests from law enforcement, the courts may be forced to evaluate expectations of privacy based on the specific - and frequently changing - policies of each individual third party service provider.

This potential consideration is particularly salient for social media applications, search engines and other websites that collect a substantial amount of personal customer data and rely heavily on such business models. While the decision leaves open a number of interesting questions, the Court’s reasoning in Carpenter reflects an evolution in Fourth Amendment doctrine that recognises recent revolutionary advances in technology and corresponding changes in societal privacy expectations. However, by limiting its holding to address only historical CSLI, the ever-cautious Supreme Court has left room for lower courts and Congress to address privacy concerns relating to other types of personal digital data.