Simon Frankel Partner
sfrankel@cov.com

Melanie Ramey Law Clerk

Covington & Burling LLP, San Francisco

Carpenter v. U.S.: What privacy rights do we have over our mobile phone data after all?

On 29 November 2017, the U.S Supreme Court heard oral arguments in *Carpenter v. U.S. Carpenter* focuses on the application of the 'third-party doctrine' concerning individuals' reasonable expectation of privacy in the context of law enforcement access to personal information held by service providers without a warrant. Simon Frankel and Melanie Ramey, Partner and Law Clerk respectively at Covington & Burling LLP, provide an overview of *Carpenter*, highlight the impact it may have on privacy and outline potential approaches that the Supreme Court may take in its judgement.

What expectation of privacy do you have in your smartphone, a device that has become such a central aspect of so many people's lives and livelihoods? Have you consented to a search of your location and other personal information simply by virtue of carrying around your mobile phone? These are the central questions currently before the Supreme Court in a case touted as one of the most important privacy cases in decades.

In *Carpenter*, the Supreme Court is considering Petitioner Thomas Carpenter's conviction for multiple counts of armed robbery. The central issue is whether law enforcement officers violated Carpenter's Fourth Amendment rights against unlawful search and seizure when they collected 127 days of his mobile site location information without a warrant. Armed with that information, the Federal Bureau of Investigation ('FBI') was able to place Carpenter's phone within a half-mile to two-mile radius of each of the robberies as they occurred. Relying on this evidence, a jury convicted Carpenter of all nine robberies and sentenced him to more than 115 years imprisonment.

Had the FBI surreptitiously collected this data *from* Carpenter in some way, it would likely be an unconstitutional search absent a warrant [emphasis added]. For example, in 2012, in *U.S. v. Jones*, the Supreme Court held that 28 days of location information secretly gathered by placing a GPS tracker on a suspect's car without a warrant was an unconstitutional search.

The third-party doctrine

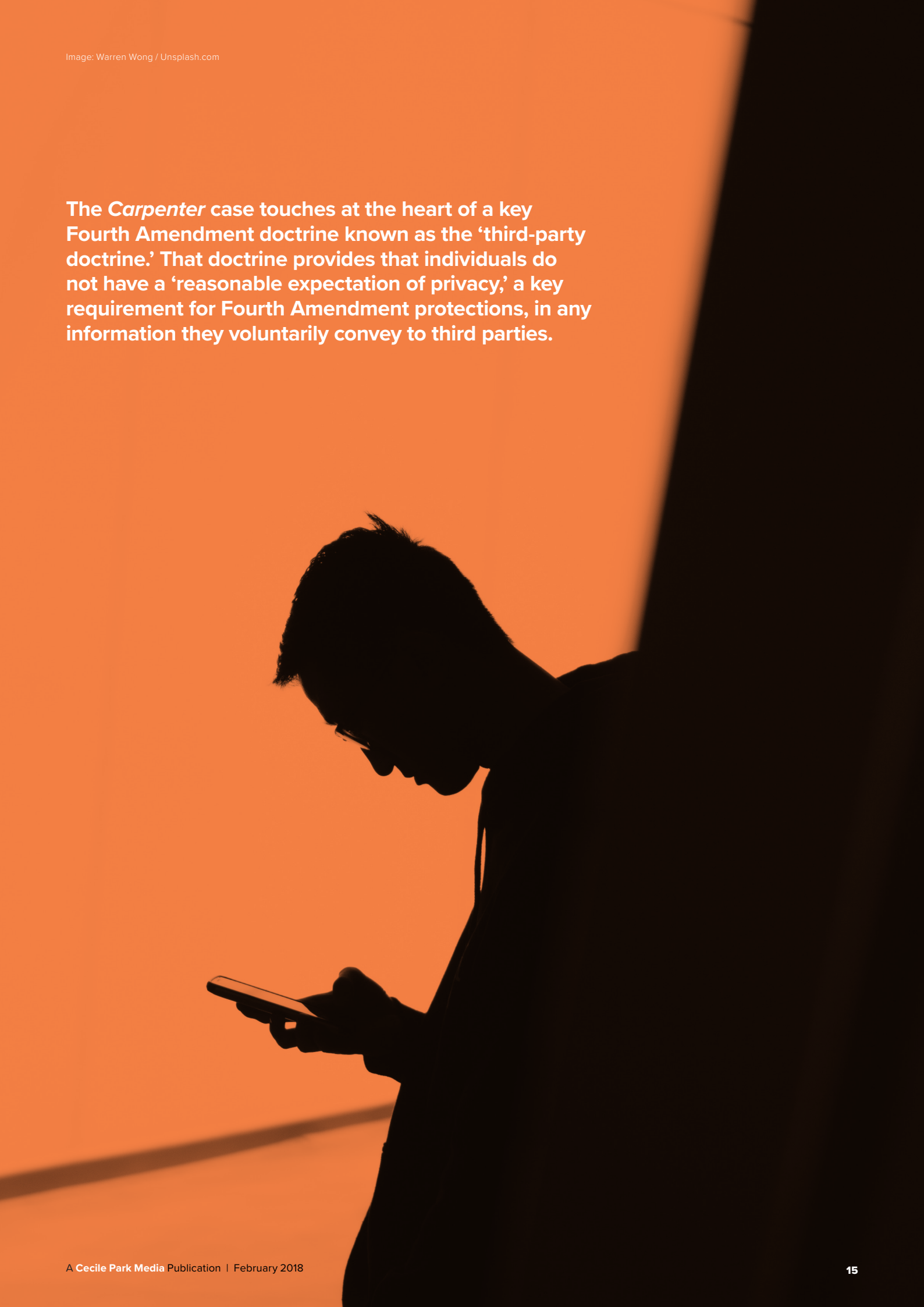
The *Carpenter* case, in contrast, touches at the heart of a key Fourth Amendment doctrine known as the 'third-party doctrine.' This doctrine provides that individuals do not have a 'reasonable expectation of privacy,' a key requirement for Fourth Amendment protections, regarding any information they voluntarily convey to third parties.

In *Carpenter*, the issue is whether he had a reasonable expectation of privacy in his mobile phone's location information, given that such information was necessarily provided to a third party, his mobile phone carrier. If the fact that his carrier would necessarily possess this information triggers the third-party doctrine, then law enforcement officers did not need a warrant to obtain this information.

The third-party doctrine is a rule created by the Supreme Court in a pair of decisions in the late 1970s. In *U.S. v. Miller*, the Supreme Court found no

Image: Warren Wong / Unsplash.com

The *Carpenter* case touches at the heart of a key Fourth Amendment doctrine known as the 'third-party doctrine.' That doctrine provides that individuals do not have a 'reasonable expectation of privacy,' a key requirement for Fourth Amendment protections, in any information they voluntarily convey to third parties.



Based on the briefs, prior case law, and the Justices' comments during oral arguments on 29 November 2017, the Supreme Court may draw the line between what is still considered private and what is not in one of several ways.

continued

expectation of privacy in the contents of original checks and deposit slips because (1) they were not confidential communications, but rather negotiable instruments, and (2) "all the documents obtained contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business[1]."

In *Smith v. Maryland*, the Supreme Court found the defendant similarly had no expectation of privacy in numbers he dialled into his phone, as by dialling he "voluntarily conveyed numerical information to the phone company and 'exposed' that information to its equipment in the normal course of business," thereby "assum[ing] the risk that the company would reveal the information to the police[2]." These two cases, decided only three years apart, created a rule that has become a cornerstone of legal understanding of the limits of Fourth Amendment protections, a rule that has so far been left relatively unmarred by nearly four decades of subsequent cases and technological advancements.

Exceptions to the third-party doctrine

While the third-party doctrine has remained relatively constant over several decades, the Supreme Court has limited the bounds of the doctrine to some extent by carving out several exceptions. For example, the Supreme Court found that individuals have a reasonable expectation of privacy in diagnostic test results[3]; in luggage placed in an overhead bin on a bus, despite the possibility of an external inspection by others[4]; and in hotel rooms where they are guests, despite the implied or express permission for third parties to access their rooms[5]. Significantly, the Sixth Circuit Court of Appeals found no loss of an expectation of privacy in email content, even if transmitted by a third party service provider[6]. Now, in an era where mobile phones and interconnected devices have become ubiquitous, the Supreme Court is considering whether to re-examine this doctrine, and if so, how it should redraw the line of what is and is not going to be considered private. *Carpenter* will require the Supreme Court to decide whether to narrow the third-party doctrine further, whether to leave the rule as it stands, or whether to change the rule more dramatically.

Where will the Supreme Court draw the line for privacy?

Based on the briefs, prior case law, and the Justices' comments during oral arguments, the Supreme Court may draw the line between what is still considered private, and what is not, in one of several ways. One approach would be to consider the sensitivity of the information at issue. Information such as diagnostic test results might fall under the umbrella of privacy and require a search warrant, while call logs of numbers people dialled into their phones would not be sufficiently sensitive and so would not. Relying on the sensitivity of data to determine the level of protection it requires, however, would likely create unwieldy and uncertain results; it would be difficult to create a bright line rule as to what is sensitive enough to merit safeguarding.

During oral arguments, for example, Carpenter's counsel and Justice Alito disagreed on whether location information was more sensitive than financial records, access to which the Supreme Court already held did not constitute a search requiring a warrant. Another line the Justices could draw is to ask whether an individual actually gave the information at issue to the third party *voluntarily* [emphasis added]. During oral arguments, the Government pointed out that companies often require individuals to relinquish certain information in the course of obtaining a third party's services, arguing that an individual's happiness about this exchange should be irrelevant.

As technology progresses, however, the extent to which individuals are aware of this exchange, and the extent to which delivery of information is truly voluntary, becomes less and less clear. For example, an *amicus* brief in the case cited a survey suggesting that 'a strong majority of Americans do not understand that this [location] information is even accessible to, much less retained by, service providers.' Thus, the Justices could foreseeably create a rule distinguishing between information knowingly given and information unwittingly transmitted, mirroring the philosophy behind the third-party doctrine as initially conceived.

It is also possible the Supreme Court will draw the line somewhere else. It could hold that the volume of information collected is the determinate factor, though this seems at least somewhat arbitrary and disjointed from any potential charge that might be brought. It might also turn to the time period over which it is collected, which raises similar concerns and was highly criticised by the Justices during oral arguments. Another possibility altogether is to consider whether an individual has some kind of vested property interest in the information, a favourite theory of Justice Gorsuch, but one that was largely ignored by his colleagues.

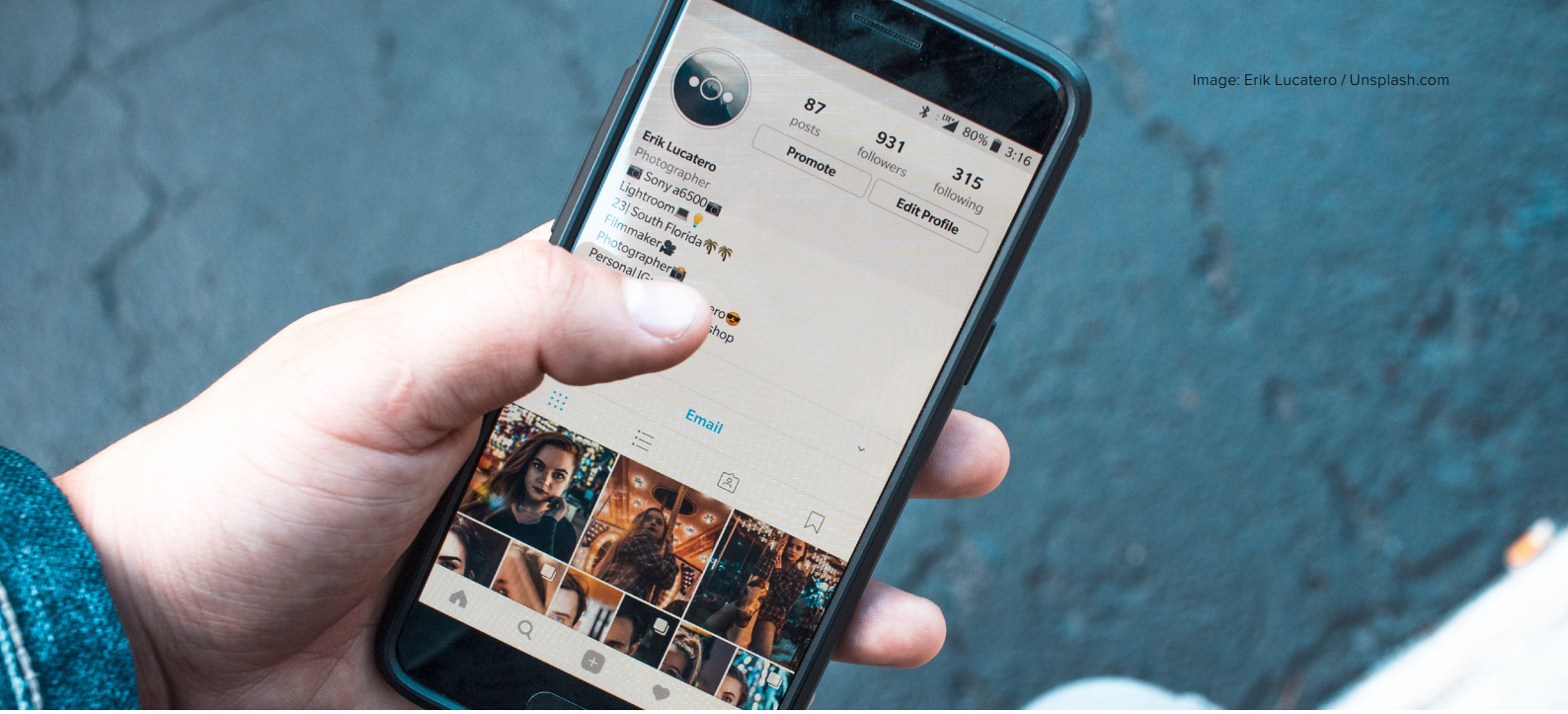


Image: Erik Lucatero / Unsplash.com

Defining what is and is not private in an increasingly connected world

Regardless of the distinctions the Justices make (or don't make), the *Carpenter* decision will likely have a profound impact on how courts define privacy in the modern era. In the 1970s when the third-party doctrine was created, defining what was and was not private was a simpler matter. The lines blurred when companies and other outside parties became involved, but we could at least be sure that the property we carried on our person and brought into our homes would be free from unwarranted government intrusion. With the advent of mobile phones, GPS trackers, and then smartphones, however, the line has seemed to disappear altogether, allowing our location and interactions to be monitored remotely, often without conscious thought on our part. Today, this monitoring and information collection has proliferated to nearly every aspect of our lives. Not only do we carry around smartphones in our pockets, tracking our location by pinging nearby cell towers, but now we also wear watches on our arms capable of tracking our heart rate and sleep patterns; we have smart thermostats in the house that constantly monitor when we are home or not; and we even have smart doorbells that can monitor who comes and goes from our house with both video and audio recordings. And, increasingly, the data associated with such everyday activity resides not only on our own devices or in our homes, but on third-party servers.

So, as data becomes ever more the currency through which we transact our day, and as data collection becomes ever more engrained into technologies that are requisite parts of our lives and livelihoods, the more our once-private lives increasingly rest in third party hands.

The impact of the ruling on law enforcement, companies and Americans' privacy

The Supreme Court's ruling in this case, therefore, will not only impact how readily law enforcement officers can access mobile location information - the accuracy of which the Justices acknowledge has improved quite dramatically in and of itself in the nearly a decade since Carpenter's information was first collected - but would also apply to any data that companies collect from their consumers.

Bringing this broad swath of activities under the umbrella of the third-party doctrine could give law enforcement access to all the information a company has collected on its users upon a mere showing that there are reasonable grounds to believe that this information might be relevant to an on-going investigation. Creating a carve-out for this seemingly automatic and mass-generated data, by contrast, would still allow law enforcement access, but only upon a showing that they have probable cause that the information is evidence of a crime.

The oral arguments in this case, heard in November, did little to paint a clear picture of how the Justices were leaning. Justice Breyer aptly summarised the back and forth, likening this issue to "an open box, we know not where we go." Wherever the Supreme Court goes, its ruling will almost certainly have a significant impact on the privacy of Americans in a world where so much personal information is now shared with third parties, whether we think about it or not.

The *Carpenter* decision will likely have a profound impact on how courts define 'privacy' in the modern era.

1. U.S. v. Miller, 425 U.S. 435, 435 (1976).
2. Smith v. Maryland, 442 U.S. 735, 735 (1979).
3. Ferguson v. City of Charleston, 532 U.S. 67 (2001).
4. Bond v. U.S., 529 U.S. 334 (2000).
5. Stoner v. California, 376 U.S. 483 (1964).
6. U.S. v. Warshak, 631 F.3d 266 (6th Cir. 2010).