The legal implications of digital privacy

January 15 2019, by Florencio Travieso

Credit: Japanexperterna.se/Flickr, CC BY

A June 2018 decision rendered by the Supreme Court of the United States established an interesting principle on digital privacy in a case related to a criminal proceeding.

The decision stated that the government must obtain a warrant in order to collect historical cell site location information (CSLI) of customers held by the cellphone companies. The case's decision is based on whether police must require a warrant in order to access information from users generated by cellphones of a suspect in a criminal investigation. This decision implies that in the future, law enforcement authorities will not have an "unrestricted access to a wireless carrier's database of physical location information" (From the majority by Justice John Roberts).

The origin of the case were several armed robberies of stores in the Detroit area in 2010. Timothy Carpenter was accused of planning the robberies, furnish weapons and operate as an external lookout.

In the case against Mr. Carpenter, the prosecutors used the records of cellphone towers – CSLI – that showed that his phone had been near the stores by the time of the robberies. The cellphone companies had provided 127 days' worth of location data from cellphone towers.

To illustrate the legal issues at stake, let us discuss, briefly, some of the main legal elements in the decision.

The legal nature of the collection of evidence

The Fourth Amendment of the US Constitution states: "The 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."

The amendment guarantees the inviolability of the person's privacy and its property against arbitrary searches or arrests by the government, unless probable cause justifies the issuing of a warrant to execute the search or seizure. Warrantless searches or seizures are possible but exceptional, its base being consent from the party being searched, imminent danger, or imminent destruction of evidence, for instance.

This guarantee is linked mainly to the persons, their private property and the limitation that the authorities have regarding its access (probable cause and hence, the issuing of a court-mandated warrant).

Under the Stored Communications Act (codified at 18 USC Chapter

121, of 1986), prosecutors must obtain a court order to track data (like cellphone related information) from suspects. But under this law (and following the 1994 amendment of §2703(d)), the standard is not a warrant, but a "lighter" proceeding: the prosecutors must demonstrate that there were "specific and articulable facts showing that there are reasonable grounds to believe" that the records are "relevant and material to an ongoing criminal investigation".

For those not familiar with the procedures in the USA to collect evidence in particular cases, the authorities (Investigators, police) might demand the issuing of a subpoena or a warrant (searches), depending on the standard of suspicion, urgency or relevance of the material to be accessed.

A *warrant* is a legal process through which the government can obtain evidence in the context of a criminal investigation. This implies to break into a third party's property where the evidence might be.

A *subpoena* (grand jury subpoena), in turn, will require the holder of the evidence to render it to the court or investigative authorities. In this case, there is no access to the property (Constitutional protection, through the fourth amendment technically applies, but it will be more modest).

In the case of a *search warrant*, the Fourth Amendment is at stake and it will require *probable cause* -a reasonable belief that the evidence will lead to the confirmation of the commission of the crime.

As Justice Kennedy stated in his dissent opinion, "(w)hile a warrant allows the Government to enter and seize and make the examination itself, a subpoena simply requires *the person* to whom it is directed *to make the disclosure*" (emphasis added). If the suspect has no expectation of privacy in the records, an objection to the measure is not possible. These matters can also be illustrated through a couple of cases from the

US Supreme Court.

In the Jones Case (2012) (United States v. Jones, 565 U.S. 400), a GPS device had been attached to the car of a suspect to monitor the suspect's movements. The device was authorized by a warrant (for ten days only), but the surveillance was considered to be excessive (over 28 days). The Court held that attaching a GPS device and using the consequent data collected was a search under the Fourth Amendment. It was also stated – in Sotomayor's concurring opinion – that modern surveillance mechanisms – cell phones – might not need a physical invasion or property, affecting privacy expectations. An element of analysis that, certainly, is brought back in the Carpenter decision.

The Riley Case (2014) (Riley v. California 573 U.S.) discusses the search and seizure of data stored in a cell phone during an arrest. In the case, the Police placed under arrest Riley after finding in his car two guns that were involved in a shooting. In the context of the arrest, his phone was searched (without a warrant) and the information obtained (pictures, text messages, cell phone contacts) allowed the Police to understand that the person was linked to illegal activities. The Court ultimately decided that a warrant is necessary to access the data in a cell phone that has been arrested.

The third-party doctrine. This doctrine is applicable to situation where the relevant evidence to be obtained from a particular person is in possession of a third party. It could be another individual (or entity, a bank) or stored by an online cloud service (email, file hosting service, or a cell phone company).

The question that rises is: what legal evidence collection mechanism will be used, and what would be the potential impact of the Fourth Amendment rights?

The third party doctrine is the main argument traditionally used by the government to justify circumventing the requirement a warrant. According to this "doctrine", once the user has disclosed records to a (cell phone) company – the cell towers in this case-, the user forgo your expectation of privacy. And the third party will not claim Fourth Amendment rights, as the data does not belong to them.

The Miller case (1976): The third-party doctrine emerges in this case (United States v. Miller, 425 U.S. 453), where the suspect was being investigated for tax evasion and the Government obtained financial information from Miller's banks (cancelled checks, deposit slips, monthly statements). When Miller claimed that the information was supposed to be protected by the Fourth Amendment, the court lately stated that the documents were not owned nor possessed by him, and that they were "business records of the banks". The nature of the records implied that the individual had no expectation of privacy, as the checks were "not confidential communications but negotiable instruments to be used in commercial transactions".

The Smith case (1979): In the Smith case (Smith v. Maryland, 442 U.S. 735, 741 (1979)), the SCOTUS maintained the same principles, but applied to the telecommunications sector. The principle in these cases refers to the fact that "a person has no legitimate expectation of privacy in information he voluntary turns over to third parties" (Smith 442 US, at 743-744 1979). When information is "knowingly shared" with somebody else, users cannot expect privacy. In cases as such, the authorities would be free to obtain the information without the need to grant the suspect with the Fourth Amendment protection.

Voluntariness

The question of voluntariness underlies the analysis of the case, which is pivotal in the analysis between the Carpenter and the Smith-Miller cases.

To what extent users are voluntarily sharing their cell phone location with the cell site towers (or with third-party services)? A cell phone logs to a cell site tower regardless of the user's specific decision and operation (beyond tuning the phone on). As the court states it: "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".

The majority opinion of the case is admitting that a full warrant protection is granted in case of third-party stored information, which implies a higher protection in the context of digital privacy (which we will discuss in the next section). The Court will hold: "A warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party". This rule will apply whether the required information is in the users' possession or in the cloud.

Shaping the new perimeter of digital privacy

The current interpretation will argue that, in view of the digital developments and ubiquitous data collection from users, the cell tower location information and other kinds of digital data gives, in fact, access to a person's private life.

The Court has established a number of interesting statements acknowledging the impact of modern technology and innovation. We believe that this decision has also been possible thanks to the long–lasting Supreme Court's contribution to the recognition of the importance of the current digital age.

The Court's decision is also relevant as it decides to delve – within the perimeter of a Constitutional right- into the implications of new technologies in everyday life. The Court chooses to take into consideration the "seismic shifts in digital technology" (Carpenter, Slip

Opinion, page 15) in the context of the current interpretation of privacy.

When discussing the legal nature of digital privacy and cellphones, the Court asserted that digital data could provide a comprehensive, detailed – and intrusive – overview of private affairs. In the past – the Court states – "few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialled digits, but a detailed and comprehensive record of the person's movements" (Carpenter, Slip Op., p.11).

Digital technology has quickly evolved, and in relation to cell site location information (CSLI) the growth in the last years has been remarkable. Cell-site records were not as accurate a few years ago, which means that they can be used today as a precise personal locator.

We find that the Supreme Court has also found the place to reflect a vision of what do cell phones mean in today's worlds' privacy. In relation to the number of days that Mr. Carpenter's data was analysed, the Tribunal stated that: "Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts […]. (T)he 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'."(C)ell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense." (Majority Opinion of the Court by Justice Roberts, Slip Op., p 12-13).

The Court states that a cell phone is almost a "feature of human anatomy" (as stated in the previous case "Riley", 2014), tracking almost all movements of its owners, who are "compulsively" carrying these objects all the time, following them to places that can reveal private

activities (doctor's offices, political headquarters, etc.) (Carpenter, Majority Opinion, Slip Op. p 13.).

Data can be retrieved not in a material manner, but also in a retrospective fashion; Government can "travel back in time to retrace a person's whereabouts" kept by the wireless carriers. "Only the few without cell phones could escape this tireless and absolute surveillance" (Carpenter, Majority Opinion, Slip Op. p.14).

So what's next?

This decision will certainly be remembered as the moment in which the collection of digital records of individuals (under the third-party doctrine) will be protected by Constitutional rights.

Carpenter has also been useful to update the interpretation of the third-party doctrine and the way digital behaviours are being understood and perceived by a court of law. This has led to extend users' protection through a more precise interpretation of digital privacy.

In days where privacy in general is not a popular trend, but a slight concern in the horizon, this decision helps to create a better understanding of how intrusive the access to data can be. This can be used to build behavioural patterns that, ultimately, could have a negative impact on the users' privacy.

The next frontier might be metadata (cookies, log-ins, network accesses, for example). All this data that can singularly be considered harmless, once combined and aggregated, it can reveal attributes of privacy. The way this data is accessed, shared and processed will certainly raise controversy not only from a legal perspective, but from an ethical one too.

But for now, let's leave our worries behind (for the time being), and enjoy this court decision that grants a larger protection on digital privacy.

Provided by The Conversation