The **Human Rights, Big Data and Technology** Project

Occasional Paper Series

Title: Beyond Carpenter v U.S.: Broadening Pathways for Protection of the Right to Privacy

Author: Vivian Ng

E·S·R·C ECONOMIC & SOCIAL RESEARCH COUNCIL

Human Rights Centre | University of Essex

Introduction

The U.S. Supreme Court recently decided the case of *Carpenter v United States*.[1] In short, the Court found that the government's acquisition of historical cell phone location records violated the right to privacy. This decision is significant as (a) the Court recognised the intrusiveness of accessing historical location data held by cell phone companies and (b) established an important precedent that a search warrant is required to access such records. Although the scope of the *Carpenter* decision was narrow, the case has been celebrated as a ground-breaking victory for the digital age, and other commentators have analysed how the reasoning of the Court has potentially broader implications for privacy in the U.S.[2] In the context of protection of the right to privacy in the digital age, it will be worth watching closely the cases building on *Carpenter*.

This paper examines how the *Carpenter* case reveals a fundamental difficulty in how the Court and other judicial bodies confront right to privacy cases in the digital age. The digital landscape involves complex connections between data, devices and other infrastructure, that are not necessarily bounded by borders. This big picture view is necessary for appreciation of the full implications on the right to privacy, which extend beyond this case and the U.S. context. Commentary on the case can enrich the value of the decision by contextualising it in the wider digital context, and locating some underlying issues that might present challenges for protection of the right to privacy more broadly.

[1] *Carpenter v United States*, No. 16-402, 585 U.S. ____ (2018).
[2] Nathan Freed Wessler, 'The Supreme Court's Groundbreaking Privacy Victory for the Digital Age' *ACLU* (22 June 2018) <https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-groundbreaking-privacy-victory-digital-age> accessed 19 November 2018.

1. Carpenter v U.S.: Application of the Fourth Amendment to New Technologies

This case arose in relation to a criminal investigation of a series of robberies in Detroit, where the historical cell phone location records of some suspects were obtained to assist the investigation. Historical cell phone location records (or cell site location information) refers to the time-stamped records generated every time a phone connects to a cell site (or a cell tower) for signal, and which are stored by cell phone companies. One of the suspects, Timothy Carpenter, was convicted based in part on cell phone location evidence that placed Carpenter's phone near the location of some of the robberies at the time they occurred. Carpenter, represented by the American Civil Liberties Union (ACLU), argued that the government violated his Fourth Amendment rights under the U.S. Constitution when it obtained his cell phone location records without a search warrant.[3]

For some background, the Fourth Amendment establishes that

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 Court had previously established that "the Fourth Amendment protects people, not places",[4] and that the Fourth Amendment applies to a "justifiable", "reasonable", or "legitimate" expectation of privacy.[5] Where such an expectation exists, a search warrant is generally required, and so the question facing the Court was whether acquisition of Carpenter's historical cell phone location records constituted a search within the meaning of the Fourth Amendment, and should therefore have required a warrant.

The Court determined that the case lay at the intersection of two lines of case law – those concerning a person's expectation of privacy regarding their location and movements, and those concerning a person's expectation of privacy regarding information shared with others.

Regarding the first line of cases, the Court referred to earlier surveillance cases and its evolving interpretation of when and how monitoring of a person's location and movements impinges on their reasonable expectations of privacy. The Court's understanding of what constitutes reasonable expectations of privacy has developed with the increasing sophistication of surveillance techniques. Addressing previously limited uses of technology and more rudimentary methods of tracking that were comparable to visual surveillance by law enforcement, the Court determined that travelling in public meant that an individual had no reasonable expectation of privacy.[6] The development of more sophisticated tools, however, has enabled more sweeping modes of surveillance. In responding to this development, the Court more recently determined that, regardless of whether one's movements had been disclosed to the public, "longer

[3] U.S. Const. amend. IV.
[4] See *Katz v United States*, No. 35, 389 U.S. 347 (1967), at 351.
[5] See *Smith v Maryland*, No. 78-5374, 442 U.S. 735 (1979), at 740.
[6] See *United States v Knotts*, No. 81-1802, 460 U.S. 276 (1983) at 282-285.

term GPS monitoring in investigations of most offenses impinges on expectations of privacy".[7] In light of the possibility of "twenty-four hour surveillance of any citizen of this country",[8] the Court reconsidered when a reasonable expectation of privacy may exist. The change here is significant as such pervasive surveillance is not only possible through GPS monitoring, but also through cell phone data. Indeed, this capability is inherent in smart technology.

On the second line of cases, which concerned a person's expectation of privacy regarding information knowingly shared with others, the Court referred to earlier cases relating to the so-called third-party doctrine and what it applies to. The Court had previously held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties".[9] It had applied this to business records held by banks,[10] as well as phone records held by telephone companies,[11] for legitimate business purposes. The third-party doctrine therefore meant that a search warrant was not required to access an individual's call records, since such information is voluntarily disclosed to companies in the ordinary course of business, such as for routing calls.

[7] See *United States v Jones*, No. 10-1259, 565 U.S. ____ (2012), concurring opinion of Justice Alito, at 430.
[8] See *United States v Knotts*, at 283-284.
[9] See *Smith v Maryland*, at 743-744.
[10] See *United States v Miller*, No. 74-1179, 425 U.S. 435 (1976).
[11] See *Smith v Maryland*.

2. Expectations of Privacy regarding Cell Phone Location Records Held by Third Parties

In addressing these two lines of case law, Carpenter held that historical cell phone records give rise to greater privacy concerns than GPS monitoring. By making that comparison, the Court extended its decision in Jones, and held that a reasonable expectation of privacy existed in relation to an individual's locations and movements captured through historical cell phone location data. In reaching this finding the Court rejected the applicability of the third-party doctrine on two grounds.

First, it argued that historical cell phone location records were qualitatively different from the limited types of personal information addressed in Smith and Miller.[12] According to the Court, the records at issues are "detailed, encyclopedic, and effortlessly compiled",[13] and enable "near perfect",[14] "tireless and absolute surveillance",[15] and the ability to retrace a person's location for up to five years (the typical duration of wireless carriers' data retention policies).[16] The Court concluded that while location records are collected for the business purposes of wireless carriers, this "exhaustive chronicle of information" was a distinct category from the limited types of personal information that the third-party doctrine applied to.[17] The fact that the location information in this case was shared with cell phone companies did not reduce the legitimate expectation of privacy (elaborated further in its second objection below). Looking at the nature of the documents in Carpenter, the Court declined to apply the third-party doctrine.

Second, it argued that while cell phone location records are shared with wireless carriers, they cannot be considered to have been voluntarily exposed by the individual. Cell phone companies typically collect and retain information about the use of the network and device by its service users for legitimate purposes such as routing calls and billing. According to the Court, cell phones and the services they provide are "such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society".[18] It also argued that default and automated logging of the information occurs once a device is powered up, without any "affirmative act" by the user.[19] In the Court's view, a person thus does not – in a meaningful sense – "voluntarily assume the risk of turning over their location information".[20] The Court concluded the normal understanding of sharing one's data cannot apply to cell phone location information, and declined the extension of the third-party doctrine to Carpenter.

---

[12] See *Carpenter v United States*, at 11.
[13] See *Carpenter v United States*, at 10.
[14] See *Carpenter v United States*, at 13.
[15] See *Carpenter v United States*, at 14.
[16] See *Carpenter v United States*, at 13.
[17] See *Carpenter v United States*, 15.
[18] See *Carpenter v United States*, at 17.
[19] *Ibid.*
[20] *Ibid.*

3. Significance and Implications of the Court's Reasoning

The outcome of the case has been celebrated as a landmark Supreme Court opinion, and an inflection point in the history of the Fourth Amendment. Commentators have generally agreed that there are broader implications. The decision established that participation in the digital age does not weaken one's right to privacy. Others have argued that it provides a framework for the application of the Fourth Amendment to digital trails and ends the warrantless bulk surveillance of Americans.[21] It has also been suggested that since the Court's reasoning focused on the nature of the digital data at issue, Carpenter could also apply to other information beyond historical cell phone location records,[22] such as information that can locate people, or other types of sensitive and intimate records. The Court, on the contrary, asserted that this decision is "narrow".[23]

A number of questions are left open, including the exact scope of the third-party doctrine, and how it might apply in the future to "more sophisticated systems that are already in use or in development".[24] On the whole, existing commentaries have focused on the implications of the Carpenter case with a view to its future applicability in the U.S. In many ways, this is appropriate as the case concerned the specific applicability of the Fourth Amendment to historical cell phone location records. However, the essence of the Court's reasoning gives pause for thought regarding wider and persistent issues that affect the protection of the right to privacy in the digital age.

Carpenter delved into the specific intrusive capacities of historical cell phone location data to establish its distinctive qualities, which formed part of its basis for why the expectation of privacy should not be diminished and its navigation around the third-party doctrine. As others have said, this outcome is positive in that protection of the right to privacy is not necessarily limited by virtue of the information being shared with others. The implications of this element of the Court's reasoning does not end here.

By carving out historical cell phone location data as a particularly unique category, it appears to limit the scope of this decision to this type of data. While the Court is limited to looking at issues before it, the reality is that lines between silos of data and different types of information are not that clear. The extensive surveillance capabilities and the involuntary nature of exposure of historical location data can be similarly applied to other types of data. For instance, data may be generated actively or passively such as by simply connecting to a network. Data can be content data such as the contents of a message or metadata, which is data about data. The wealth of trace information that is passively generated in the digital society means that details about when, where, with whom, how, and for how long individuals engage in a particular activity can be logged on any device or network. This metadata does not only include time-stamped location data, it also includes information such as the duration of communications, frequency and patterns of activity.

---

[21] Sharon Bradford Franklin, '*Carpenter* and the End of Bulk Surveillance of Americans' *Lawfare* (25 July 2018) <https://www.lawfareblog.com/carpenter-and-end-bulk-surveillance-americans> accessed 19 November 2018.
[22] Paul Ohm, 'The Broad Reach of *Carpenter v. United States*' *Just Security* (27 July 2018) <https://www.justsecurity.org/58520/broad-reach-carpenter-v-united-states/> accessed 19 November 2018.
[23] See *Carpenter v United States*, at 17.
[24] See *Kyllo v United States*, No. 99-8508, 533 U.S. 27 (2001), at 36, as quoted in *Carpenter v United States*, at 14.

Collectively, these records are far more extensive than the "detailed chronicle of a person's physical presence compiled every day, every moment, over several years" enabled by historical cell phone location data.[25] They can similarly reveal "familial, political, professional, religious, and sexual associations".[26] This has been observed by the European Court of Justice in relation to data which providers of publicly available electronic communications services or of public communications networks retain. It held that "[t]hose data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[27]

Further, while the Court's observations regarding how revealing historical cell phone location data can be are correct, the intrusive capacities of data are not only derived from what type of data it is, but what can be done with it. Even if some data does not appear immediately sensitive, it can be combined with other data, processed, analysed and used to infer information about individuals and groups. It is not only easy and relatively inexpensive to collect data; current computing power also means that a large amount of data can be processed for sophisticated analysis and stored with relative ease. Analysis of the Court's reasoning thus needs to locate historical cell phone location records in the context of other types of data, and the current state of digital technology more broadly.

Digital technology is well integrated into individuals' daily lives and the architecture of society. A range of applications operate across a multitude of connected devices, and run across different aspects of life. Examples include social media platforms, navigation tools on smartphones, health and fitness trackers on wearable healthcare technology, and voice-controlled digital personal assistants in smart home devices. These have become the mechanisms through which individuals and groups communicate, access information and services, and even organise and mobilise. This connectivity has become commonplace, configuring and shaping the deepening relationship between humans and technology. Situating cell phones in this digital landscape gives a fuller view of how one truly interacts with the information they generate and apparently share with others. This is the real backdrop of the situation that the Court was responding to in Carpenter.

Accessing historical cell phone location data may bring into play the right to privacy, but the implications of this element of the Court's reasoning are wider. The Court alluded to the broader effects by noting how the privacies of life may be engaged if their "familial, political, professional, religious, and sexual associations" are revealed.[28] While the Court is limited to addressing the applicability of the Fourth Amendment, the right to privacy as understood in international law has an integral connection to other human rights.[29] The right to

[25] See *Carpenter v United States*, at 16.
[26] See *Carpenter v United States*, at 12.
[27] See *Digital Rights Ireland*, Judgment, European Court of Justice, Cases C-293/12 & C-594/12, 8 April 2014, at para 27.
[28] See *Carpenter v United States*, at 12.
[29] The Human Rights, Big Data and Technology Project, 'Written submission for OHCHR The Right to Privacy in the Digital Age Consultation' <https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/HRBDT.pdf> accessed 19 November 2018, para 8.

privacy is both essential in and of itself,[30] and also as a gatekeeper to the full exercise of all other human rights.[31] Interferences with the right to privacy can therefore also interfere with other rights. For example, social media has become a common forum for communities to organise and mobilise. Protests can be set up as events online where individuals can indicate their interest and check in virtually. If law enforcement police such events by accessing the data of individuals that attended, this affects not only the right to privacy but also the right to freedom of expression and the right to freedom of peaceful assembly. Appreciating the context of the technology and broadening the view of how individuals interact with technology thus enables a deeper analysis of the effects this case speaks to.

The Court firmly articulated the limits of the case at the end of its judgment, but the Court's reasoning regarding the issues before it indicates significantly wider implications and connections. Not only has the case been a step forward for the application of the Fourth Amendment, it has potentially broadened pathways for protection of the right to privacy, if underlying issues and challenges that must be addressed are recognised. Contextualising the case in the broader context indicates that data should not be understood in silos, and that given the connectivity of digital architecture isolating specific forms of technology can undermine effective analysis. The right to privacy is important not only as an independent right, but is interrelated with other rights, and digital technology must be mapped on to the full range of rights to understand its web of effects.

This work was supported by the Economic and Social Research Council [grant number ES/M010236/1].

[30] United Nations Office of the High Commissioner for Human Rights 'Report on The Right to Privacy in the Digital Age' (3 August 2018) UN Doc A/HRC/39/29, paras 1, 11.
[31] United Nations Human Rights Council Res 34/7 on the Right to Privacy in the Digital Age (23 March 2017) UN Doc A/HRC/34/7, preambular para 14.

The Human Rights, Big Data and Technology Project

Human Rights Centre,
University of Essex,
Colchester CO4 3SQ
+44 (0)1206 872877

@HRBDTNews
www.hrbdt.ac.uk