Artificial Intelligence and Policing: Hints in the *Carpenter* Decision

Elizabeth E. Joh*

*Carpenter v. United States*¹ is a case riddled with ironies. A man accused of participating in the robberies of cellphone stores finds himself incriminated by his own cellphone. Several of the Justices—three of whom were born during the Great Depression—take note of the ubiquity of cellphones in our daily lives. The various opinions refer to the Cyber Age, eighteenth century dictionaries, and everything in between. For court watchers, this was a hotly debated case about the third-party exception to the Fourth Amendment that ultimately had little to do with that doctrine at all. The decision to find Fourth Amendment protections in the government’s collection of a person’s movements acknowledges that rapid advances in technology are changing Fourth Amendment boundaries. Lower courts are already grappling with how to apply *Carpenter*’s new protections.²

But let’s turn instead to a different aspect of the *Carpenter* decision. On its own terms, the majority opinion resolved a “narrow” question about the government’s collection of cellphone location information collected and stored by a customer’s wireless carrier.³ Chief Justice Roberts focuses on the quality of the information sought by the police as a means of deciding the case in Carpenter’s favor.⁴ Less obviously, however, the majority opinion also stresses the *nature of the policing* involved in Carpenter’s case: new technologies that do more than enhance human abilities. The majority makes no explicit claims about this focus. But the *Carpenter* decision reveals the Supreme Court’s first set of views on how it might evaluate police use of artificial intelligence. That contention, and the questions it raises, form the subject of this essay.

---

² See, e.g., Naperville Smart Meter Awareness v. Naperville, 900 F.3d 521 (7th Cir. 2018) (finding public utility readings at 15-minute intervals of home electricity use constitutes a “search”).
³ 138 S. Ct. at 2220 (“Our decision today is a narrow one.”).
⁴ Id. at 2217.

* Professor of Law, U.C. Davis School of Law. Many thanks to the Ohio State Journal of Criminal Law for the invitation to contribute to this volume, and to Ryan Calo, Dean Alan Michaels, and Charles Reichmann for helpful comments.
I. TIMOTHY CARPENTER AND THE TATTLING CELLPHONE

Timothy Carpenter and his half-brother (also improbably named) Timothy Sanders assembled a loose crew of changing characters to rob seven cellphone stores near Detroit and nearby Warren, Ohio. After one of the participants in the robberies confessed to the crimes and provided the cellphone numbers of the others, FBI agents applied for an order under the federal Stored Communications Act, rather than a warrant premised on probable cause. The government sought cell-site location information from these cellphones during the period when the crimes occurred.

That location information would have provided clues as to the defendants’ whereabouts. Cellphones continuously seek a signal, usually from the closest cell-site tower. Each connection generates a record about the time and location of connections between a user’s cellphone and a particular cell-site. In that way, these records provide a detailed map of where you have been. This cell-site location information is stored as a matter of course by most wireless carriers.

In Carpenter’s case, the court orders to Metro PCS and Sprint resulted in the production of 12,898 location points cataloging Carpenter’s movements during the four month period when the cellphone store robberies took place. At Carpenter’s trial, an FBI Agent created maps showing that Carpenter’s phone—and Carpenter by implication—was close to the vicinity of the robberies at the time when they occurred. A jury convicted Carpenter on Hobbes Act and federal firearms charges.

The Sixth Circuit rejected Carpenter’s claim that the collection of this cell-site location information amounted to a search under the Fourth Amendment and thus

7 138 S. Ct. at 2212.
8 Id. at 2211.
9 Id. at 2217 (noting that cell-site location information provides “detailed and comprehensive record of the person’s movements”).
10 Id. at 2212 (observing that wireless carriers collect this data “for their own business purposes” and that “they often sell aggregated location records to data brokers, without individual identifying information from the transmission of text messages and routine data connections.”).
11 Id.
12 United States v. Carpenter, 819 F.3d 880, 885 (“With the cell-site data provided by Carpenter’s and Sanders’s wireless carriers, Hess created maps showing that Carpenter’s and Sanders’s phones were within a half-mile to two miles of the location of each of the robberies around the time the robberies happened.”).
required a warrant rather than a court order under the Stored Communications Act. The government’s collection of this data from Carpenter’s wireless carriers fell plainly, in the court’s view, under the existing third-party exception to the Fourth Amendment. Cell phone data—even if it revealed a time machine into Carpenter’s whereabouts—were no different than other business records voluntarily conveyed to third parties and thus without Fourth Amendment protection.

The Supreme Court struck a different path. The Chief Justice acknowledged the potential applicability of two lines of decisions: both the third-party doctrine and the privacy-in-public cases. The third-party cases like Smith v. Maryland emphasize that information voluntarily provided to third parties like banks or phone companies loses Fourth Amendment protection. Similarly, in cases like United States v. Knotts the Court denied Fourth Amendment protection for one’s movements in public.

Neither group of cases proved to be critical to the Carpenter decision. Instead, the majority opinion focused on the “unique nature of cellphone location records” to conclude that “an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.” Such information, capable of providing an “all-encompassing record of the holder’s whereabouts,” constitutes a “qualitatively different category” of information warranting Fourth Amendment protection. The majority rebuked the government for “fail[ing] to contend with the seismic shifts in digital technology,” just as it had in Riley v. California just four years earlier.

Having concluded that the collection of cell-site location data counted as a Fourth Amendment search, the Carpenter majority decided that a court order under the Stored Communications Act was insufficient. Absent an “urgent situation” excusing its absence, law enforcement collection of cell-site location information

---

14 See 819 F.3d at 888 (“This case involves business records obtained from a third party, which can only diminish the defendants’ expectation of privacy in the information those records contain.”).

15 See United States v. Carpenter, 138 S. Ct. at 2218 (“With access to CSLI, the Government can now travel back in time to retrace a person’s whereabouts, subject only to the retention policies of the wireless carriers . . . .”).

16 442 U.S. 735, 744 (1979) (“When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business. . . .” “This analysis dictates that petition can claim no legitimate expectation of privacy here.”).

17 460 U.S. 276, 276 (1983) (“A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements.”).

18 Carpenter, 138 S. Ct. at 2216–17.

19 134 S. Ct. 2473, 2488 (2014) (“The United States asserts that a search of all data stored on a cell phone is ‘materi ally indistinguishable’ from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon.”).
must be obtained with a warrant.\textsuperscript{20} By identifying a search and requiring a warrant, the decision counters the government’s “powerful new tool” to investigate with a Fourth Amendment recalibration.\textsuperscript{21} The majority reversed the Sixth Circuit’s judgment in this case.\textsuperscript{22}

II. POLICING AND ARTIFICIAL INTELLIGENCE

Plotting geographic data on a literal map for a jury evokes little of the futurism associated with the term “artificial intelligence.” Loosely defined as the use of machines to approximate human thinking,\textsuperscript{23} artificial intelligence already envelopes our daily lives—including the use of iPhone autocorrect, social media photo tagging, and the recommendations that guide what to watch, what to buy, and whom to date. The future is likely to include robotic caregivers, autonomous vehicles, and machine-driven medical diagnostics.

The availability of massive amounts of data, leaps in computing power, and increasingly sophisticated algorithms have begun to change policing as well. We might define the use of AI in policing as the growing use of technologies that apply algorithms to large sets of data to either assist human police work or to replace it.\textsuperscript{24} And assistance is something of a misnomer. Artificial intelligence has begun to

\textsuperscript{20} Carpenter, 138 S. Ct. at 2223.


\textsuperscript{22} There were four dissents in the case. Two in particular are noteworthy. Justice Kennedy found little to distinguish the collection of cell-site location information from “other kinds of business records the Government has the lawful right to obtain by compulsory process.” Carpenter, 138 S. Ct. at 2224 (Kennedy, J., dissenting). That analogy is remarkably similar to Kennedy’s refusal to distinguish between fingerprints and DNA samples in Maryland v. King, another case in which technological advances raised questions about the limits of existing Fourth Amendment doctrine. See 569 U.S. 435, 436–37 (2013) (finding few differences between fingerprint and DNA sample collection). Justice Alito’s dissent points to another important question raised in the Carpenter majority: whether the decision alters existing doctrines about Fourth Amendment standing. See Carpenter, 138 S. Ct. at 2247 (noting that the Court permitting “a defendant to object to the search of a third party’s property” is “revolutionary”).

\textsuperscript{23} Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, 51 U.C. Davis L. Rev. 399, 404 (2017) (“There is no straightforward, consensus definition of artificial intelligence. AI is best understood as a set of techniques aimed at approximating some aspect of human or animal cognition using machines.”). Many computer scientists have understandably found fault with the imprecision with which the terms artificial intelligence and algorithms have been used in non-technical writing. For the purposes of this essay, however, the general but somewhat vague definition will have to do.

change the capabilities of the police by permitting them to do what was once nearly impossible or impracticable.

One change already ushered in by artificial intelligence is an expansion in what we might call the “surveillance discretion” of the police. Surveillance discretion refers to the decisional freedom of the police to pay attention to some person or persons rather than others—an uncontroversial aspect of ordinary policing. But resource constraints always checked traditional surveillance discretion: there are never enough officers nor enough money for cameras and other machines. But machine-generated analyses have changed that calculus. The police today enjoy a surfeit of data that can be collected, stored, mined, and sifted through easily and cheaply: license plate data, social media posts, social networks, and soon our own faces.

The mass collection of this data would be largely useless without quick, cheap, and easy ways to find connections and patterns. Whether we call it the age of algorithms, big data, or AI, today law enforcement agencies can increasingly turn to tools that enable them to sort through this data to look for persons already identified, or for patterns from as yet unknown persons that indicate suspicious behavior. Threat analysis software might comb through private and public records to help an officer assess the potential dangerousness of a driver in a routine traffic stop. Social network analysis might identify what persons pose the most likely threat of gun violence, either as perpetrator or victim.

For now, we might best think of these technologies as tools that enhance the abilities of traditional policing. Predictive policing algorithms help departments focus limited human patrol resources, for instance, by highlighting people most likely to commit crimes or places where crime is mostly likely to occur. But these...

---


26 Id. at 15.

27 See, e.g., Justin Jouvenal, The New Way Police are Surveilling You: Calculating Your Threat ‘Score’, WASH. POST (Jan. 10, 2016), http://wapo.st/1OcTX3K?tid=ss twbottom&utm_term=.d4d455f45465 (Intrado’s Beware software provides police with a threat “score” of a person. Exactly how the software determines this is protected by Intrado as a trade secret.).


29 See, e.g., John Eligon & Timothy Williams, Police Program Aims to Pinpoint Those Most Likely to Commit Crimes, N.Y. TIMES (Sept. 24, 2015), https://nyti.ms/1R48saA (describing “an experiment taking place in dozens of police departments across the country, one in which the authorities have turned to complex computer algorithms to try to pinpoint the people most likely to be involved in future violent crimes—as either predator or prey.”); Erica Goode, Sending the Police Before There’s a Crime, N.Y. TIMES (Aug. 15, 2011), https://www.nytimes.com/2011/08/16/us/16police.html (describing one program that “generates projections about which areas and windows of time are at highest risk for future crimes by analyzing and detecting patterns in years of past crime data.”).
applications can go well beyond mere enhancement. No single officer (nor a single department) can scan thousands of private and public records to make an assessment of a suspect’s dangerousness.\textsuperscript{30} No single law enforcement agency has the means to personally track every car in town and plot out its movements. No police department can deploy personnel to identify every jaywalker and fine them within seconds.\textsuperscript{31} In these ways the tools of artificial intelligence are changing the nature of policing itself.

Another way to think of this development is that policing is becoming increasingly \textit{automated}.\textsuperscript{32} Automation may be most frequently associated with jobs like truck drivers, cashiers, and file clerks, but many fields will be subjected to varying degrees of automation.\textsuperscript{33} This includes conventional policing. Certainly, many of the most mundane tasks of patrol, including traffic direction and report writing, will be delegated to machines.\textsuperscript{34} But even today the increasing interest in social network analysis, locational predictive policing, and threat analysis means that even the task of assessing suspicious behavior is subject to automation as well.

III. ARTIFICIAL INTELLIGENCE IN CARPENTER

A central concern in Fourth Amendment law focuses on how the government \textit{accesses} information. The police generally need a warrant to enter your house, whether they want to seize your most personal documents, or merely to look around.\textsuperscript{35} In a pre-digital world, the conceptual premise of the house, mailbox, and foot locker made sense.

Finding Fourth Amendment protections for Carpenter was difficult under the Court’s previous decisions because the government accessed none of the defendant’s spaces normally protected by the Fourth Amendment. Instead, the majority opinion avoids this difficulty by focusing instead on the \textit{nature} of the information sought:

\textsuperscript{30} About half of American law enforcement agencies employ few than ten full time officers. See Brian Reaves, U.S. Dep’t of Justice, Census of State and Local Law Enforcement Agencies, 2008 (2011), https://www.bjs.gov/content/pub/pdf/csllea08.pdf.


\textsuperscript{32} Elizabeth E. Joh, Automated Policing, 15 OHIO ST. J. CRIM. L. 559 (2018).

\textsuperscript{33} See, e.g., Natalie Kitroeff, Robots Could Replace 1.7 Million American Truckers in the Next Decade, L.A. TIMES (Sept. 25, 2016), http://www.latimes.com/projects/la-fi-automated-trucks-labor-20160924/ (“Trucks without human hands at the wheel could be on American roads within a decade, say analysts and industry executives.”).

\textsuperscript{34} Elizabeth E. Joh, Automated Policing, 15 OHIO ST. J. CRIM. L. 559 (2018).

“the qualitatively different category of cell-site records.” Location information—at least some amount of it—can be so revealing that its very existence requires traditional Fourth Amendment protections. Much of the commentary after Carpenter will likely take up the question of what other information also falls into the same qualitative category of data as cellphone locational information and not the unprotected data that the majority loosely defines.

But Carpenter does something yet more. The decision hints that Fourth Amendment protections also turn on the nature of the policing that produces the information at issue. What distinguishes the kind of policing in Carpenter from traditional methods also happens to describe the emerging ways in which police are relying upon artificial intelligence. Carpenter recognizes, perhaps more so than any other Supreme Court decision, that dramatic technological changes will rewrite the Fourth Amendment’s constraints on the government’s powers. In finding that we possess Fourth Amendment protections in locational data even when recorded by third parties, the Court chose to describe the data collection technique in Carpenter as superhuman, passive, and automated. This is noteworthy: these descriptions also characterize the very technologies of artificial intelligence that are becoming more commonplace in policing.

First, the new technologies of policing employ data collection, storage, and analysis methods that are both superhuman and cheap. They are superhuman because while human beings could do the same thing, it would be impracticable to do so. The collection of cell-site location information surpasses “the nosy neighbor who keeps an eye on comings and goings.” Instead, the technology is “ever alert, and [its] memory is nearly infallible.” Practical restraints like police staffing become much less important when there exist “tireless and absolute surveillance” methods available through technology.

And even if vastly more efficient and superior to the human resources of an average police department, equally important is the affordability of these technologies. Thousands of data points were available to the FBI in Carpenter’s case “at practically no expense.” The average American police department may

---

36 138 S. Ct. at 2216 (emphasis added).
37 Id. at 2220 (“We do not disturb the application of Smith and Miller or call into question conventional surveillance techniques and tools, such as security cameras.”).
38 Cf. “Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so for any extended period of time was difficult and costly and therefore rarely undertaken.” Id. at 2217 (quoting United States v. Jones, 132 S. Ct. 945 (2012) (Alito, J., concurring in the judgment)).
39 138 S. Ct. at 2219.
40 Id.
41 Id. at 2218.
42 Id.
not possess the means to create a real time crime center but increasingly it can buy off-the-shelf software or take advantage of data already being collected by third parties. Access to these technologies is no longer an option only for the most well-off municipal departments. As the Court observed in Carpenter, the collection of cell-site location information is “remarkably easy, cheap, and efficient compared to traditional investigative tools.”

Second, artificial intelligence applications permit the expanding uses of surveillance discretion with little additional effort required from the police. With vast amounts of data being collected all the time, “police need not even know in advance whether they want to follow a particular individual or when.” While police will continue to seek known persons suspected of criminal activity, they will also employ “collect all” data methods to see if suspicious persons and activities “emerge” from the data. In Timothy Carpenter’s case, the government was able to “access each carrier’s deep repository of historical location information” “[w]ith just the click of a button.” These passive forms of investigation vastly expand policing power.

Third, these technologies represent a decreasing emphasis on human skill in favor of automation. What we might have presumed to be quintessentially human talents in policing—identifying suspicious persons and activities and drawing inferences from seemingly disconnected data—are increasingly tasks assumed by machines. No one in Carpenter’s situation (i.e. anyone with a cellphone) could flee the “inescapable and automatic nature of its collection . . .” And those tasks can be assumed at a scale, with a speed, and with results that humans could not easily reproduce. In this way, the reasoning of the Carpenter decision appears to recognize that police use of artificial intelligence has far surpassed merely “augmenting the sensory faculties bestowed upon them at birth . . .”

The Carpenter decision hints at the kinds of police technologies that may necessitate new ways of thinking about the Fourth Amendment. The majority opinion does not identify these new ways of thinking definitively, but instead raises new and provocative questions. Perhaps the most direct question raised by the case will be which new technologies will qualify as “conventional surveillance

43 Id. (emphasis added).
44 Id.
45 Id.
46 See Sarah Brayne’s excellent discussion of how these technologies have change policing within the LAPD. Sarah Brayne, Big Data Surveillance, 82 AM. SOC. REV. 977, 990 (2017) (“The shift from query-based to alert-based systems, represents, in part . . . a fundamental transformation in surveillance activities.”).
48 138 S. Ct. at 2223 (emphasis added).
techniques and tools” and thus trigger no Fourth Amendment protections. The likely questions to be raised here will include the use of facial recognition technology in public spaces, particularly if they become incorporated into police body cameras intended for ordinary patrol use.

The Court’s decision, however, to focus not only on the quality of the information collected but also the method of policing used to obtain it suggests that novel forms of technology-enhanced policing may trigger new Fourth Amendment protections. The security camera will longer be the paradigm of policing technology. Many objects besides cellphones are or will be connected to the internet and each other. Cloud computing will shift our perceptions of what a single source of data collection, storage, and analysis is. And increasingly our definition of policing may include responses to automated alerts. Or perhaps even automated responses to those automated alerts.

In other words, if part of what provides a person Fourth Amendment protection from surveillance is the fact that the policing method involved could be characterized as superhuman, passive, and automated, what other techniques might fall in that category? If police use 24-hour-a-day patrol robots capable of identifying people and vehicles in public spaces, are all of them engaged in perpetual Carpenter-type searches? If such robots are connected by cloud computing, how many Carpenter-type searches are taking place at once?

Moreover, the Court’s concerns about a type of tireless, automated, and inescapable data collection would seemingly characterize “smart” cities planned for the future. These visions of urban life in the future imagine an infrastructure characterized by a network of sensors intended to regulate traffic flow, respond to

50 138 S. Ct. at 2220.
52 See Andrew Guthrie Ferguson, The Internet of Things and the Fourth Amendment of Effects, 104 CAL. L. REV. 805, 813 (2016) (“Experts predict that the worldwide scale of such ‘smart,’ interconnected objects will continue to grow, reaching more than fifty billion objects in 2020, and one trillion by 2025 . . . . The result will be additional options for government surveillance that can reveal the patterns of everyday life.”).
emergencies, and manage energy consumption. Those very same sensors are ideal methods of data collection for law enforcement as well.

Finally, if I am right about the Court’s forward-looking approach to the Fourth Amendment and policing methods, it may begin to cast doubt on the extreme deference courts have given to the judgments of human police officers. Others have written extensively about the judicial reluctance to second guess police determinations of suspicion and the use of force. Such deference presumes an accumulation of individual and institutional skill that is human, and to some extent, unknowable. But if the future of policing is automated, those assumptions may not bear their weight.

IV. CONCLUSION

The use of artificial intelligence is nowhere to be found in the Carpenter decision. Indeed, the Court ends its decision eager to cabin it, “to ensure that we do not ‘embarrass the future.’” But in its choices to describe why the locational data obtained by the government warranted Fourth Amendment protection, the Court recognized not only the qualitatively distinct features of the information, but also the type of policing involved in obtaining it. This way of describing investigation—superhuman, passive, and automated—also happens to characterize the use of artificial intelligence in policing. And as technologies become more powerful and prevalent in ordinary law enforcement, those clues suggest what will concern the Court in the future.

54 Id. at 1.

55 See, e.g., Seth W. Stoughton, Policing Facts, 88 TUL. L. REV. 847, 864 (2014) (“In the context of determining whether a police use of force was constitutionally permissible, the Court has concluded that the circumstances in which police use force justify deference to the officers’ decisions.”).

56 138 S. Ct. at 2220 (quoting Northwest Airlines, Inc. v. Minnesota, 64 S. Ct. 950, 955 (1944)).