SAY CHEESE: FACIAL RECOGNITION TECHNOLOGY IN A POST-*CARPENTER* WORLD

Jay D. Evans*

"Everyone in every house in every street open a front or rear door or look from the windows. The fugitive cannot escape if everyone in the next minute looks from his house." – Ray Bradbury, Fahrenheit 451

ABSTRACT

In 2018, the Supreme Court handed down its long-awaited decision in *Carpenter v. United States*. The Court held that the collection of cell-site location information was a violation of the Fourth Amendment. Not because of how police accessed the information but because of what the information revealed. The Court's decision has fundamentally changed Fourth Amendment analysis and its impact will reach other digital-age technologies, including facial recognition technology. This Article argues that, in light of *Carpenter*, certain police uses of facial recognition technology are unconstitutional. Furthermore, old doctrines are no longer useful to consider Fourth Amendment issues in an age of rapidly advancing technology and the changing nature of society's relationship with technology. Therefore, *Carpenter* has announced a new analytical framework—the *Carpenter* Test—through which courts can determine, in advance of any search using facial recognition technology, whether the search requires a warrant. This new framework will balance the threats posed by facial recognition technology with the benefits the technology offers to police.

* Staff Member, Texas Tech Law Review; J.D. Candidate 2022, Texas Tech University School of Law. The author would like to thank Dean Jack Wade Nowlin, Professor Jamie Baker, Professor Allison Myhra, Anna DuBois, and Joseph Best for their thoughtful advice, feedback, and encouragement. Also, the author would like to thank his parents who listened to him drone on and on about this Article and politely listened the whole time.

TABLE OF CONTENTS

I. INTRODUCTION

For years one intersection in Xiangyang, China used to be a nightmare.[1] Speeding cars and jaywalkers filled the street until police installed cameras linked to facial recognition technology.[2] Now when a camera detects a jaywalker several photographs are taken and within minutes the person's picture, government identification number, and home address are displayed on a screen above the intersection.[3] Without much notice, facial recognition has allowed China to become the most advanced surveillance state in the world.[4] Some uses of facial recognition may be harmless, even comical. Airport check-in has been reduced to a quick facial scan, customers at a KFC in Beijing stand for a facial scan and receive menu suggestions, and dormitories use facial recognition to stop nonresidents from entering.[5]

However, other uses of facial recognition are more concerning. Police in China are "able to locate and identify anyone who shows their face in public" in a matter of minutes.[6] Police can track where people have been and identify what kind

---

[1] Paul Mozur, *Inside China's Dystopian Dream: A.I., Shame and Lots of Cameras*, N.Y. TIMES (July 18, 2018), https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.
[2] *Id.*
[3] Rene Chun, *China's New Frontiers in Dystopian Tech: Facial-recognition technologies are proliferating, from airports to bathrooms*, THE ATLANTIC (April 2018), https://www.theatlantic.com/magazine/archive/2018/04/big-in-china-machines-that-scan-your-face/554075/.
[4] *Id.*
[5] *Id.*
[6] Clare Garvie et. al., *American Under Watch: Face Surveillance in the United States*, CTR. ON PRIV. & TECH. AT GEO. L. (May 16, 2019), https://americaunderwatch.com, [hereinafter *America Under Watch*].

of car they drive, their family members, and other people they have been in contact with and how often.[7] Chinese citizens currently live in a constant state of monitoring via facial recognition technology.[8] Despite a population of over 1.4 billion people, nearly every single Chinese citizen is included in the government's facial recognition database.[9] It is easy to think that the threat posed by facial recognition to privacy rights is a remote, future concern for the United States. But for millions of Americans, the threat has already arrived.[10]

One in every two American adults has their photograph in a database accessible to police for facial recognition searches, and a "significant number of law enforcement entities possess the ability to use facial recognition for a range of surveillance and law-enforcement activities."[11] In its most advanced forms, police can use facial recognition technology to examine surveillance footage and photographs to identify people and track their current and past locations, activities, and interactions.[12] As a result, facial recognition technology is increasingly changing the nature of law enforcement by permitting police to do what was once

[7] *Id.*
[8] Sarah Chun, *Facial Recognition Technology: A Call for the Creation of a Framework Combining Government Regulation and a Commitment to Corporate Responsibility*, 21 N.C.J.L. & TECH. 99, 109 (2020).
[9] *Id.*
[10] *See e.g.*, *American Under Watch*, *supra* note 6.
[11] Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, CTR. ON PRIV. & TECH. AT GEO. L (Oct. 18, 2016), https://www.perpetuallineup.org, [hereinafter *Perpetual Line-Up*]; Jake Laperruque et. al., *Facing the Future of Surveillance*, THE PROJECT ON GOV'T OVERSIGHT (Mar. 4, 2019), https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/, [hereinafter *Facing the Future*].
[12] *Facing the Future*, *supra* note 11.

nearly impossible or impracticable.[13] In the past, constraints on police resources limited traditional surveillance—there was not enough money or police officers to conduct the type of surveillance now made possible by facial recognition.[14]

Traditional Fourth Amendment analysis focused on places and access to those places.[15] Echoing the language of the Fourth Amendment, courts focused on searches of "persons, houses, papers, and effects." and how police performed those searches.[16] If the police wanted to enter your home and, for example, search or seize your personal letters, they generally needed a warrant.[17]

In 2018, a seismic shift occurred.[18] *Carpenter v. United States* broke from traditional Fourth Amendment understanding and the decision has the potential to shape the future of Fourth Amendment analysis and protection.[19] "To ensure that . . . technology does not hand the government too much power, *Carpenter* adds protection to information because of what it *may reveal*."[20] By focusing on the nature of the information sought, the Court suggests that collections of personal information may receive Fourth Amendment protections where the information can be used to locate people, and where the information, "provide[s] an intimate

---

[13] Elizabeth E. Joh, *Artificial Intelligence and Policing: Hints in the* Carpenter *Decision*, 16 OHIO ST. J. CRIM. L. 281, 284 (2018).
[14] *Id.* at 287.
[15] *Id.* at 286; Orin S. Kerr, THE DIGITAL FOURTH AMENDMENT (OXFORD UNIV. PRESS) (forthcoming).
[16] U.S. CONST. amend. IV; Joh, *supra* note 13 at 281.
[17] Joh, *supra* note 13 at 281.
[18] *See* Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357 (2019).
[19] *See id.* at 358.
[20] Kerr, *supra* note 15 (emphasis added).

window into a person's life."[21] The Court's holding in *Carpenter* should extend Fourth Amendment protection to information obtained through certain police uses of facial recognition technology.

However, "[d]etaching the Fourth Amendment from its traditional focus on places and things" presents a challenge.[22] Police need to know when a warrant is necessary to run a facial recognition search, "citizen[s] need[] to know what the police legally *can't* do," and courts need a new analytical framework to determine when access to certain personal information for a facial recognition search requires a warrant.[23]

Many lawyers and academics have discussed the threat posed by police use of facial recognition technology to Fourth Amendment rights.[24] Many have also discussed the impact of *Carpenter v. United States* on the future of Fourth Amendment jurisprudence.[25] However, the two have not been discussed in conjunction. This Article seeks to fill that gap. In light of the Court's decision in *Carpenter*, certain uses of facial recognition by police violate the Fourth Amendment.[26] This Article goes one step further and suggests that the Court in *Carpenter* introduced a new method of analysis through which a judge can

[21] Ohm, *supra* note 18 at 364 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).
[22] Kerr, *supra* note 15.
[23] *Id.*
[24] *See, e.g.*, *Perpetual Line-Up*, *supra* note 11; *America Under Watch*, *supra* note 6.
[25] *See, e.g.*, Ohm, *supra* note 18; Kerr, *supra* note 15.
[26] *See infra* Part II.

determine, in advance of any search, whether access to certain information collected through the use of facial recognition technology requires a warrant.[27]

Part II of this Article will provide a brief overview of how facial recognition technology works, how the technology is used by police, and a discussion of the development of modern Fourth Amendment jurisprudence. Part III will argue that, in light of *Carpenter*, certain uses of facial recognition technology threaten Fourth Amendment rights. Part IV will propose a new analytical framework, implicitly created by the Court in *Carpenter*, through which courts can determine whether a search of a database containing information collected through the use of facial recognition requires a warrant. Finally, Part V will apply the *Carpenter* test to three hypothetical uses of facial recognition technology.

II. THE CURRENT REALITY

Facial recognition technology is an extremely powerful tool used by police and government agencies on a daily basis.[28] In 2018, for example, the FBI ran over 52,000 facial recognition searches—an average of 4,000 searches each month.[29] These searches do not just include photographs of criminals or suspected criminals.[30] According to a report by the Georgetown Law Center on Privacy and Technology, one in two Americans have a pre-identified photograph stored in a

[27] *See infra* Part III.
[28] *Perpetual Line-Up*, *supra* note 11.
[29] *Facing the Future*, *supra* note 11.
[30] *Perpetual Line-Up*, *supra* note 11.

database used for facial recognition searches.[31] But while more law enforcement agencies adopt facial recognition technology, the law has struggled to keep pace.[32] Today, there is no comprehensive federal law governing the use of facial recognition technology.[33] Nor has any court addressed facial recognition technology in the context of the Fourth Amendment.[34]

This section provides a brief overview of how facial recognition technology works, how the technology is used by law enforcement agencies, and a discussion of modern Fourth Amendment jurisprudence from Katz v. United States to *Carpenter v. United States*. This section will conclude with a discussion of the *Carpenter* test—a new analytical framework implicitly created by the Court that can be applied to searches of databases containing information collected through the use of facial recognition technology.

A. The Basics of Facial Recognition

Generally, facial recognition technology uses computer software to identify or verify a person's identity based on certain facial features.[35] Before identification, a computer program scans an image of an unknown person's face and creates a series of nodal points that can be numerically quantified—such as the location of

[31] *Id.*
[32] Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1595 (2017).
[33] *Id.*
[34] *Id.*
[35] *Facing the Future*, *supra* note 11.

the mouth in relation to the face as a whole.[36] Next, the nodal points of the original image are compared against other photographs or video footage of known persons.[37] Within a matter of seconds, the computer program returns a set of images with a numerical score reflecting the probability of a match between the original, unidentified image and the identified image.[38]

Currently, law enforcement agencies use facial recognition technology in one of four ways: to identify or confirm the identity of a suspect in police custody; to identify a person a police officer encounters in the field who is unable or unwilling to identify herself; to identify a suspect from a security camera, smartphone, social media post, or other surveillance footage after the commission of a crime; and to identify a person from a live video feed or archival video.[39]

Of course, facial recognition technology does not operate on its own and the power of a particular facial recognition system depends on three underlying types of technology.[40] First, the underlying computer software.[41] The most advanced facial recognition software can scan millions of pre-identified images in a short amount of time and return results with a high probability of positive identification.[42]

---

[36] *Perpetual Line-Up*, *supra* note 11.
[37] *Id.*
[38] *Id.*
[39] *Id.* These categories are referred to as arrest identification, field identification, investigative identification, and real-time surveillance respectively. *See Facing the Future*, *supra* note 11.
[40] *Facing the Future*, *supra* note 11.
[41] *Id*.
[42] *Id.* (noting, however, that real-time facial recognition surveillance requires more computer power than facial recognition systems that simply identify a person).

As departments adopt more advanced computer software, police can use real-time facial recognition surveillance to scan a large number of faces at once and store that footage for future use.[43]

The power of a particular facial recognition system also depends on the size and contents of the database used for facial recognition searches.[44] Currently, law enforcement agencies have access to a variety of government databases that can be used as a source of identification.[45] For example, police in Pennsylvania use a database of over 34 million DMV photographs, while police in Florida use a database of over 45 million DMV and mugshot photographs.[46] Recently, Immigration and Customs Enforcement (ICE) officials accessed a Maryland database containing more than 275,000 identified photographs of undocumented immigrants for a facial recognition search.[47]

Finally, the sources of photographs and video footage can determine the power of a particular facial recognition system.[48] While the United States does not have a network of closed-circuit television (CCTV) cameras like China or the United Kingdom, several large American cities do maintain a network of police

---

[43] *Id*.
[44] *Id.*
[45] Hirose, *supra* note 32 at 1598.
[46] *Facing the Future*, *supra* note 11.
[47] Erin Cox & Drew Harwell, *ICE has run facial recognition searches on millions of Maryland drivers*, WASH. POST (Feb. 26, 2020), https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/.
[48] *Facing the Future*, *supra* note 11.

CCTV cameras that feed into a central database for identification.[49] Also, it is becoming increasingly common for police officers to wear body cameras, an additional source of surveillance footage.[50] Finally, police have begun to turn to photographs posted on social media as an additional source of pre-identified photographs against which unknown photographs can be compared.[51]

While facial recognition use in the United States is not as widespread as other surveillance states like China, law enforcement agencies are increasingly relying on the technology.[52] At least one in four police departments have the capacity to run facial recognition searches.[53] For example, the Los Angeles Police Department can scan faces from surveillance footage against lists of wanted criminals or gang members while all 1,020 law enforcement agencies in Pennsylvania can access the state's facial recognition system.[54] Given the variety of uses, it would be impossible to describe all the ways in which facial recognition technology is deployed by police in this short section; however, a few examples are representative.

---

[49] *Id.*
[50] *Id.*
[51] *Id.*; *see also* George Joseph & Jake Offenhartz, *NYPD Used Facial Recognition Technology in Siege of Black Lives Matter Activist's Apartment*, GOTHAMIST (Aug. 14, 2020), https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment.
[52] *Perpetual Line-Up*, *supra* note 11.
[53] *Id.*
[54] *Id.*

The FBI has two of the largest facial recognition databases in the country: The Next Generation Identification Interstate Photo System (NGI-IPS) and Facial Analysis, Comparison, and Evaluation (FACE) Services.[55] NGI-IPS contains nearly 25 million state and federal criminal photographs, mostly mugshots along with fingerprints.[56] FACE Services runs facial recognition searches against a database of over 411.9 million photographs from several sources, such as driver's licenses, mugshots, and other photographs for identification purposes.[57]

Additionally, beginning in 2018, the Detroit Police Department began a facial recognition surveillance program that allows the police to "connect the [department's] facial recognition system to any interface that performs live video, including cameras, drone footage, and body-worn cameras."[58] One such interface is Project Green Light, a public-private partnership where businesses purchase and install high-definition cameras that feed directly to the police department.[59] Project Green Light locations include "churches, hotels, clinics, addiction treatment centers, affordable housing apartments, and schools."[60] Furthermore, the department's facial recognition system compares unknown faces against a Detroit

[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *America Under Watch*, *supra* note 6.
[59] *Id.*
[60] *Id.*

database of 50,000 mugshots and against a statewide database that includes driver's license photographs.[61]

Finally, the Chicago Police Department and Chicago Transit Authority have operated a facial recognition surveillance program since 2016. The program provides for "Real Time Screening using Facial Recognition on Chicago's vast camera monitoring system which includes nearly 20,000 street, transit[,] and other video cameras located throughout the city."[62]

While police departments are relying more and more on facial recognition technology, the law has not kept pace.[63] Despite calls for regulation, there is no comprehensive federal law that governs police use of facial recognition technology.[64] Furthermore, no court has addressed police use of facial recognition technology in the context of the Fourth Amendment.[65] Indeed, many courts are still grappling with how to apply the Fourth Amendment to technologies that are commonplace like cell phones.[66] Despite the slow pace with which courts have addressed these threats, recent decisions from the Supreme Court may suggest a growing concern about police uses of digital-age technologies.[67]

---

[61] *Id.*
[62] *Id.*
[63] Hirose, *supra* note 32 at 1594.
[64] *Id.* at 1595.
[65] *Id.*
[66] *Id.*
[67] *Id.*

B. The Emergence of Carpenter v. United States

In 2018, the Supreme Court handed down its much-anticipated decision in *Carpenter v. United States*.[68] Many have described the decision as a "blockbuster for the [d]igital Fourth Amendment."[69] While the Court's reasoning in *Carpenter* was certainly novel, the analysis was rooted in an established foundation.[70] The Court built on more than fifty years of shifting Fourth Amendment jurisprudence from *Katz v. United States* to *United States v. Jones* and finally to *Riley v. California*.[71]

1. From Katz *to* Riley

The Fourth Amendment to the United States Constitution protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[72] Traditionally, Fourth Amendment protections were tied to places and things and how police accessed those places and things.[73] That changed in 1967 in the case of *Katz v. United States*.[74] There, the government attached an electronic listening device to the outside of a public telephone booth to eavesdrop on Katz's telephone conversation.[75] Even though the government did not physically enter into the phone booth, the Court held that an

[68] Ohm, *supra* note 18 at 358.
[69] Kerr, *supra* note 15.
[70] *Id.*
[71] *See* Ohm, *supra* note 18.
[72] U.S. CONST., amend. IV.
[73] Kerr, *supra* note 15.
[74] *Id.*
[75] *See* Katz v. United States, 389 U.S. 347 (1967).

unconstitutional search occurred.[76] Writing for the majority, Justice Stewart famously reasoned that "the Fourth Amendment protects people, not places."[77] When Katz entered into the booth and shut the door behind him, he exhibited an expectation of privacy.[78]

In his concurring opinion, Justice Harlan articulated the reasonable expectation of privacy test that has survived to this day: "[F]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable."[79] Since 1967, the Court has applied the test in most instances.[80]

The changing nature of the Court's Fourth Amendment analysis continued in *United States v. Jones* and *Riley v. California*.[81] In *Jones*, police attached a GPS device to Jones's Jeep without a valid warrant and tracked the vehicle's movements continuously for four weeks.[82] The Court held that the attachment of and monitoring by a GPS device was a search.[83] While the majority based its decision

[76] *See id.*; Anthony P. Picadio, *Privacy in the Age of Surveillance: Technological Surveillance and the Fourth Amendment*, 90 PA. B.A. Q. 162, 165 (2019).
[77] *Katz*, 389 U.S. at 351.
[78] *Id.* at 352.
[79] *Id.* at 361 (1967) (Harlan, J., concurring). The mosaic theory, discussed below, is another framework frequently discussed by judges and academics. *See infra* notes 246249 and accompanying text (discussing the foundation and application of the mosaic theory).
[80] *See, e.g.*, United States v. Knotts, 460 U.S. 276 (1983); Kyllo v. United States, 533 U.S. 27 (2001); United States v. Jones, 565 U.S. 400 (2012).
[81] *See* Ohm, *supra* note 18.
[82] *See Jones*, 565 U.S. 400.
[83] *See Katz*, 389 U.S. 347.

in a trespass theory, *Jones* is significant because of two concurring opinions written by Justices Alito and Sotomayor.[84]

Justice Sotomayor expressed concern that even during short-term monitoring, "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[85] Furthermore, Justice Sotomayor noted that GPS surveillance is "cheap" and "evades the ordinary checks that constrain abusive law enforcement practices." Finally, the government can collect and store records of a person's movements and "mine them for information years into the future."[86]

Along the same lines, Justice Alito argued that long-term location tracking, made possible through advanced technologies like GPS, intruded upon a person's reasonable expectation that police "would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[87] Like Justice Sotomayor, Justice Alito's reasoning hints at his concerns about what police may learn about a suspect from their physical movements.[88]

---

[84] Hirose, *supra* note 32 at 1606.
[85] *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).
[86] *Id.* at 415–16 (Sotomayor, J., concurring).
[87] *Id.* at 430 (Alito, J., concurring).
[88] Brief for Plaintiff-Appellants at 20–21, Leaders of a Beautiful Struggle v. Balt. Police Dep't, No. 20-1495, 2020 WL 2310452 (4th Cir. Nov. 5, 2020).

Two years later, in *Riley v. California*, the Court unanimously held that a warrant is required to search the digital contents of an arrestee's cell phone.[89] Writing for the majority, Chief Justice Roberts focused on the nature of the information police may discover while searching a cell phone.[90] As opposed to other objects that might be kept on an arrestee's body, a cell phone contains a record of nearly every aspect of a person's life.[91] Cell phones collect information that may "reveal much more in combination than any isolated record."[92] The "sum of an individual's private life can be reconstructed" through a cell phone as opposed to a single "photograph or two of loved ones tucked into a wallet."[93] Finally, certain types of data collected on a cell phone, such as internet browsing history, "reveal an individual's private interests or concerns."[94]

In the fifty years since the Court's decision in *Katz*, the Court has begun to acknowledge that in addition to protecting people from unreasonable searches, the Fourth Amendment protects people from what a search may reveal.[95] Building on the Court's continuing understanding of these Fourth Amendment principals, only

[89] *See* Riley v. California, 573 U.S. 373 (2014).
[90] See *id.*
[91] *Id.* at 394–97.
[92] *Id.* at 394.
[93] *Id.*
[94] *Id.* at 395.
[95] Aparna Bhattacharya, Note, *The Impact of* Carpenter v. United States *on Digital Age Technologies*, 29 S. CAL. INTERDISC. L.J. 489, 492 (2020).

a few years after *Riley*, the Court once again shifted the approach to understanding a person's expectation of privacy.[96]

2. Carpenter v. United States

Carpenter v. United States was a "milestone for the protection of privacy in an age of rapidly changing technology."[97] Following a string of robberies, police obtained records from Carpenter's cell phone provider that included the approximate location of where his calls began and ended based on connections to cell towers, also known as cell-site location information (CSLI).[98] The Court held that the police's warrantless acquisition of Carpenter's CSLI violated his Fourth Amendment rights against unreasonable searches and seizures.[99]

Rather than focusing solely on how police accessed Carpenter's CSLI, the Court focused on the nature of the *information sought* and the nature of *police activity* that produces the information.[100] Specifically, the majority focused on three general areas of concern: the aggregation of CSLI and the personal information it may reveal, location tracking through the use of CSLI, and the expansion of police power.[101]

---

[96] *Id.* at 495.
[97] Ohm, *supra* note 18 at 358.
[98] *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).
[99] *See id.*
[100] Joh, *supra* note 13 at 287 ("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.").
[101] *See Carpenter*, 138 S. Ct. 2206.

First, the Court held that police access to an extensive compilation of CSLI without a warrant violated the Fourth Amendment.[102] Access to CSLI provides a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[103] Because of the nature of this information, police now have access to "an intimate window into a person's life[,]"[104] which for many Americans holds the "privacies of life."[105]

Second, the Court held that "individuals have a reasonable expectation of privacy in the whole of their physical movements."[106] The Court reasoned that "[m]apping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts.[107] Furthermore, because a cell phone is "almost a feature of human anatomy[,]" when police track a person's movements using CSLI, they achieve "near perfect surveillance."[108]

Finally, the Court argued that unrestricted access to CSLI expanded the power of police beyond the scope of "Founding-era understandings."[109] Such an expansion was in conflict with an underlying principle of the Fourth Amendment

[102] *Carpenter*, 138 S. Ct. at 2219.
[103] *Id.* at 2220.
[104] *Id.* at 2217.
[105] *Id.* at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).
[106] *Id.* at 2217 (citing United States v. Jones, 565 U.S. 400, 430 (Alito, J., concurring)).
[107] *Id. Cf*. United States v. Moore-Bush, 963 F.3d 29 (1st Cir. 2020) (holding that a pole camera installed across from the defendant's home was not a Fourth Amendment violation because a single, stationary pole camera only captures what is in public view and does not track the whole of a person's movements over time).
[108] *Carpenter*, 138 S. Ct. at 2218.
[109] *Id.* at 2214.

because, "a central aim of the Framers was to 'place obstacles in the way of a too permeating police surveillance.'"[110] The Court reasoned that when CSLI is compared to traditional investigative techniques, access to CSLI is cheaper and more efficient.[111] Rather than using a significant amount of resources to track a suspect using traditional methods of surveillance, police can access "each carrier's deep repository of historical location information at practically no expense."[112]

3. The Carpenter *Test*

A key issued raised by *Carpenter* is when police seek access to a large database containing personal information constitutes a search under the Fourth Amendment.[113] According to Professor Paul Ohm, the Court in *Carpenter* held that the collection of CSLI constituted a search under the Fourth Amendment by implicitly introducing a new three factor test—the *Carpenter* test.[114] Under the *Carpenter* test, when police want to obtain information about a person collected in a database, the court should examine three factors to determine whether a warrant is necessary: 1) the "deeply revealing nature" of the information; 2) the "depth,

[110] *Id.* (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).
[111] *Id.* at 2217–2218 (2018); *Cf.* United States v. Knotts, 460 U.S. 276 (1983) (holding that monitoring the location of the defendant through the use of beeper signals was not an unconstitutional search because the surveillance amounted to following the defendant's vehicle on public streets and highways).
[112] *Carpenter*, 138 S. Ct. at 2218.
[113] *See* Ohm, *supra* note 18 at 361.
[114] *Id.*

breadth, and comprehensive reach" of the information; and 3) the "inescapable and automatic nature of its collection."[115]

The first factor of the *Carpenter* test protects information that is "deeply revealing" of some private aspect of the person under surveillance.[116] This factor flows from the Court's concern that certain information collected in a database may reveal intimate information beyond the scope of a criminal investigation.[117] The inquiry is forward-looking and focuses on the nature of the information that *may be revealed* without any consideration of what information is *actually revealed*.[118]

The second factor of the *Carpenter* test focuses on the "depth, breadth, and comprehensive reach" of the information collected.[119] Specifically, depth refers to the "detail and precision of the information stored," and should be considered in the context of the Court's concern in *Carpenter* that police, using 127 days of location information, could produce a detailed log of Carpenter's movements.[120]

---

[115] *Id.*; *Carpenter*, 138 S. Ct. at 2213.
[116] Ohm, *supra* note 18 at 37 (quoting *Carpenter*, 138 S. Ct. at 2213).
[117] Bhattacharya, *supra* note 95 at 495. The Court in *Carpenter* was not the first to consider intimacy as an important aspect of Fourth Amendment Rights, "intimacy is a longstanding consideration in Fourth Amendment law and the most well-established of the Fourth Amendment principles." Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 15 (2020). In general, the more intimate a place or thing targeted for investigation, the more likely such an investigation runs afoul of Fourth Amendment rights. *Id.* For example, the home has long received the strongest Fourth Amendment protection. *See, e.g.*, Kyllo v. United States, 533 U.S. 27 (2001). *See also* U.S. Dept. of Just. v. Rep. Comm. for Freedom of Press, 489 U.S. 749 (1989) (holding that the disclosure of contents from FBI rap sheets could reasonably be expected to constitute unwarranted invasion of personal privacy).
[118] Tokson, *supra* note 117 at 15.
[119] Ohm, *supra* note 18 at 372 (quoting *Carpenter*, 138 S. Ct. at 2223).
[120] *Id.*; *Carpenter*, 138 S. Ct. at 2217. The Court in *Carpenter* also concluded that information is protected "[w]hether the Government employs its own surveillance technology . . . or leverages the technology of a wireless carrier." *Carpenter*, 138 S. Ct. at 2217. As noted by Professor Ohm, this

When considering breadth, the inquiry is on "how frequently the data [was] collected and for how long the data has been recorded."[121] For example, CSLI data, as the Court suggested in *Carpenter*, allowed police to follow a suspect "every moment of every day for five years" and review the results of that surveillance at will.[122] In general, the more information that is collected, the more likely a warrant is required.[123]

Comprehensive reach focuses on the quantity of information collected.[124] As the Court in *Carpenter* noted, the government "obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day."[125] Such a large amount of data, the Court reasoned, provided police with a comprehensive record of Carpenter's physical presence.[126] In sum, the second factor directs future courts to "measure [] the extent and duration of a surveillance

quote calls into question the 'third-party doctrine' or the "bedrock rule that the Fourth Amendment concerns itself only with the activities of the government." Ohm, *supra* note 18 at 390. While the third-party doctrine is outside the scope of this Article, *Carpenter* suggests that the mere fact that personal information collected or stored by a third party does not insulate that information from Fourth Amendment scrutiny. *Id.*

[121] Ohm, *supra* note 18 at 372.

[122] *Carpenter*, 138 S. Ct. at 2218.

[123] Tokson, *supra* note 117 at 19 (2020); *see, e.g.*, United States v. Knotts, 460 U.S. 276 (1983) (holding that limited use of a GPS device attached to a vehicle did not constitute a search but suggested that a more prolonged search could raise Fourth Amendment concerns).

[124] Ohm, *supra* note 18 at 373 (Ohm writes that comprehensive reach refers to the number of people tracked but the author disagrees with that focus. Rather, this Article suggests that the Court in Carpenter was less concerned with the number of people who had their location tracked via CSLI than on what the aggregation of a person's collected data may reveal).

[125] *Carpenter*, 138 S. Ct. at 2212.

[126] Tokson, *supra* note 117 at 19.

practice or how much information about a suspect is ultimately obtained and stored."[127]

The third and final factor of the *Carpenter* test focuses on the "inescapable and automatic nature" of the information collected.[128] While the first two factors focus on the nature of the information, the final factor considers whether the suspect may have assumed the risk of collection or knowingly exposed their personal information.[129] Courts must consider the relationship between the technology that collects personal information and the people under surveillance.[130] In the case of CSLI, the Court reasoned that Carpenter did not voluntarily share his location information with his wireless carrier because cell phones are "such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society" and "faithfully follows its owner."[131] Additionally, there was no way for Carpenter to opt out of collection because his wireless carrier logged his CSLI "without any affirmative act on the part of the user beyond powering up."[132]

Seen as a vital law enforcement tool, the use and development of facial recognition technology continues to expand across the nation.[133] However, the law has been slow to keep pace and courts will soon have to address constitutional

[127] *Id.* at 18.
[128] Ohm, *supra* note 18 at 374 (quoting *Carpenter*, 138 S. Ct. at 2223).
[129] *Id.* at 376.
[130] *Id.*
[131] *Carpenter*, 138 S. Ct. at 2220 (quoting Riley v. California, 573 U.S. 373, 395 (2014)).
[132] Bhattacharya, *supra* note 95 at 493 (quoting *Carpenter*, 138 S. Ct. at 2219).
[133] *Facing the Future*, *supra* note 11.

challenges to police use of facial recognition technology.[134] If past cases are a guide, the Court is increasingly willing to reexamine Fourth Amendment doctrines.[135] *Carpenter*, in particular, seems to suggest that certain uses of facial recognition technology may not pass constitutional muster.[136]

III. THE END OF OBSCURITY: FACIAL RECOGNITION TECHNOLOGY THREATENS FOURTH AMENDMENT RIGHTS

The use of facial recognition technology by police departments and government agencies threatens Fourth Amendment rights.[137] Prior to *Carpenter*, this statement would not have been true. However, as previously discussed *Carpenter* set a course for rethinking Fourth Amendment rights in the digital age.[138] Despite Chief Justice Roberts's insistence that the Court's decision was a "narrow one[,]" the impact of *Carpenter* is likely to be far reaching.[139] Building on *United States v. Jones* and *Riley v. California*, the Court signaled its sensitivity to the wealth of private information that police may access, including location information.[140] *Carpenter* established the idea that when new technologies allow police to invade a person's privacy, the person's privacy must be protected regardless of what method police use.[141]

---

[134] *Id.*
[135] *See* Ohm, *supra* note 18.
[136] *See* Michael Price, Carpenter v. United States *and the Future Fourth Amendment*, 42–JUN CHAMPION 48 (Jun. 2018).
[137] *See e.g.*, *Perpetual Line-Up*, *supra* note 11; *Facing the Future*, *supra* note 11.
[138] *See* Price, *supra* note 136.
[139] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
[140] *See id.*
[141] Chun, *supra* note 8 at 115.

This section will argue that, in light of *Carpenter*, certain uses of facial recognition technology violate Fourth Amendment rights. Building on the Court's concerns regarding access to CSLI, certain uses of facial recognition technology present the same concerns.[142] Namely, facial recognition technology allows police to access large quantities of personal information, to locate and track a person's movements, and vastly expands police power.[143]

A. The Gathering Storm: Facial recognition technology allows police to access large amounts of deeply personal information

Facial recognition allows police to do more than capture a person's face as she walks down a street, it allows police to identify a person and retrieve an *aggregation* of personal information.[144] Consider, for example, the FBI face recognition unit or FACE Services, which has the ability to run facial recognition searches against a network of databases that includes over 185 million driver licenses and other ID photographs.[145] Such a search creates a "virtual line-up of millions of law-abiding Americans" and allows police to access otherwise unknowable personal information without consent or notification.[146]

Well before *Carpenter*, the Supreme Court endorsed the notion that the aggregation of data that may reveal private information is protected by the Fourth

---

[142] *See Facing the Future*, *supra* note 11.
[143] *Id.*
[144] *See* Hirose, *supra* note 32 at 1605–07.
[145] *Perpetual Line-Up*, *supra* note 11.
[146] *Id.*

Amendment.[147] In *United States Department of Justice v. Reporters Committee for Freedom of Press*, the Court found a privacy right in FBI "rap sheets" that include personal information such as date of birth, physical characteristics, arrest history, charges, convictions, and incarceration history.[148] While each individual piece of information was a public record and available to those who may request access, the Court held that people have a privacy right in the aggregate summary of information included in each record.[149]

Some may counter that when people step out of their homes, they invite strangers to look at their face as they pass by one another.[150] Even if the other person happens to be a police officer, no search has occurred because "what we knowingly expose[] to the public . . . is not a subject of Fourth Amendment protection."[151] However, the issue is not simply whether police may identify a person through the use of facial recognition technology, but whether police may identify a person *and* access a wealth of personal information.[152] The totality of information that could

[147] *See* U.S. Dept. of Justice v. Reporters Committee for Freedom of Press, 489 U.S. 749 (1989).
[148] *See id.*
[149] *Id.* at 764–65.
[150] Hirose, *supra* note 32 at 1603–04.
[151] Katz v. United States, 389 U.S. 347, 351 (1967).
[152] *See* United States v. Ellison, 462 F.3d 557 (6th Cir. 2006). In *Ellison* the Sixth Circuit held that police did not violate the Fourth Amendment privacy interests of a motorist when they used the license plate number of the vehicle to access personal information about the motorist. "[T]he Fourth Amendment was not implicated by the . . . search on the relatively uncontroversial fact that the operator of a vehicle has no privacy interest in the particular combination of letters and numerals that make up his license-plate number." *Id.* at 566 (Moore, J., dissenting). In his dissent, Judge Moore chided the majority for missing the real issue, whether the police can "conduct a search using the license-plate number to access information about the vehicle and its operator that may not otherwise be public or accessible by the police without heightened suspicion. *Id.* at 567.

be revealed when facial recognition technology is used to identify a person in public is not available to the general public or police without heightened suspicion.[153] People do not walk around in public with a sign adjacent to their face announcing personal information.[154]

B. Picture Perfect: Facial recognition technology allows police to track a person's precise movements

Facial recognition technology promises to become a powerful method of locating and tracking people.[155] While facial recognition is most often used to identify a person at a set time and location, the growing presence of surveillance cameras and body cameras could effectively allow police to use facial recognition to map out a person's movements for days, weeks, or months at a time.[156]

The Supreme Court has already held that tracking a person's movement over a period of time requires a warrant.[157] As previously discussed, the majority in *Jones* held that location tracking via the attachment of a GPS device for four weeks was a search.[158] Justices Alito and Sotomayor were especially concerned that

---

[153] Hirose, *supra* note 32 at 1607.
[154] *Id.*
[155] Jake Laperruque, *Preserving the Right to Obscurity in the Age of Facial Recognition*, THE CENTURY FOUND. (Oct. 20, 2017), https://tcf.org/content/report/preserving-right-obscurity-age-facial-recognition/, [hereinafter *Preserving the Right to Obscurity*].
[156] *Id.*
[157] *See, e.g.*, United States v. Jones, 565 U.S. 400 (2012); Carpenter v. United States, 138 S. Ct. 2206 (2018).
[158] *See Jones*, 565 U.S. 400. While the majority opinion, written by Justice Scalia, based the Court's holding in a trespass theory, two separate concurring opinions written by Justices Alito and Sotomayor expressed concern over the nature of information police may access through the use of a GPS device.

police "tracked every movement that respondent made in the vehicle he was driving" for four weeks.[159] Similarly in *Carpenter*, the Court reasoned that "mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts."[160]

In the same way that GPS tracking or CSLI provides police a near-perfect record of a person's location for any length of time, so too does facial recognition technology.[161] Identifying a person's location as she walks by a network of surveillance cameras allows police to map out that person's movements, both in real-time and to reconstruct her past movements.[162] Current limits on location tracking via facial recognition technology only exist because most cities have not yet developed a network of surveillance cameras.[163] However, "as the use of body cameras, CCTV, and public-private partnerships continue to expand, the capacity to use facial recognition for location [tracking] will expand as well."[164]

Police use of facial recognition technology to track a person's movements should be distinguished from identifying a person's specific location at a specific point in time.[165] The former poses a risk to Fourth Amendment rights while the latter does not.[166] Consider, for example, United States v. Moore-Bush where the

[159] *Id.* at 430 (Alito, J., concurring).
[160] *Carpenter*, 138 S. Ct. at 2217.
[161] *Facing the Future*, *supra* note 11.
[162] *Preserving the Right to Obscurity*, *supra* note 155.
[163] *See id.*
[164] *Facing the Future*, *supra* note 11.
[165] *See e.g.*, United States v. Moore-Bush, 963 F.3d 29 (1st Cir. 2020).
[166] *Id.*

First Circuit held that the government did not violate the defendant's Fourth Amendment rights when they installed a video camera on a utility pole across the street.[167] The defendant argued that *Carpenter* was controlling because the pole camera surveillance was "particularly 'unrelenting, 24/7, [and] perfect.'"[168]

However, the court rightfully disagreed. As opposed to *Carpenter*, a single, stationary pole camera only captures what is in public view, it "does not track the whole of a person's movements over time."[169] On the other hand, tracking a person's movements through the use of facial recognition technology does not occur in isolation.[170] Rather police rely on a network of surveillance cameras to track the whole of a person's movements over a particular area or over a period of time.[171]

Not only does facial recognition allow police to track *where* a person is or has been, but also *what* location a person visits or has visited.[172] Like GPS tracking in *Jones* and CSLI in *Carpenter*, tracking people via facial recognition reveals a wealth of detail about their private life.[173] Data collected via facial recognition will reveal trips to the "psychiatrist, plastic surgeon, the abortion clinic, the AIDS

[167] *Id.*
[168] *Id.* at 42.
[169] *Id.*
[170] *Facing the Future*, *supra* note 11.
[171] *Id.*
[172] *Id.*
[173] *See* United States v. Jones 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar."[174]

In fact, these highly-sensitive locations may even be targeted for surveillance.[175] For example, patients visiting Summit Medical Center, a reproductive and women's health center in Detroit, may notice a sign informing patients that the site is monitored by video cameras.[176] However, what the sign hides from patients is that the camera is connected to Detroit's facial recognition surveillance system.[177]

Finally, facial recognition technology is a powerful tool for cataloging participation in certain political meetings, protests, and other public gatherings.[178] For example, consider a Black Lives Matter protest. Police could take a photograph or video of the protest and then use facial recognition technology to identify every participant and catalogue their participation for future use.[179] As a result, police can see how many protests an activist has attended with little manual effort.[180] A hypothetical example is not even needed. In 2016 the Baltimore Police Department

[174] *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).
[175] *America Under Watch*, *supra* note 6.
[176] *Id.*
[177] *Id.*
[178] *Preserving the Right to Obscurity*, *supra* note 155.
[179] *Id.*
[180] *Id.*

used facial recognition "to locate, identify[,] and arrest certain people protesting Freddie Gray's death [while] in police custody."[181]

C. Super Police: Facial recognition technology dramatically increases police power

Facial recognition technology has created a super police force.[182] In the past, constraints on resources limited traditional surveillance—there was not enough money or police officers to conduct the type of surveillance now made possible by facial recognition.[183] Additionally, facial recognition technology has changed the nature of policing by permitting police to do what was once nearly impossible or impracticable.[184] The Court has recognized this threat, noting that "dramatic technological changes will rewrite the Fourth Amendment's constraints on the government's powers."[185]

As Justice Alito recognized in *Jones*, "[i]n the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but

---

[181] Clare Garvie & Neema Singh Guliani, Opinion, *Lawmakers need to curb face recognition searches by police*, L.A. TIMES (Oct. 24, 2016), https://www.latimes.com/opinion/op-ed/la-oe-garvie-guliani-face-recognition-20161024-snap-story.html. Another, more recent, example illustrates how facial recognition is used to identify protestors. *See XRVision Uses Facial Recognition to Identify Nazis Participating in Capitol Riot in DC*, Find Biometrics (Jan. 8, 2021), https://findbiometrics.com/xrvision-uses-facial-recognition-identify-nazis-participating-capitol-riot-dc-010801. On January 6, 2021, a violent mob of domestic terrorists stormed the U.S. Capitol. *Id.* During the riot, XRVision, a facial recognition and video analytics company, performed an analysis on the video footage and identified several individuals and shared the information with federal law enforcement. *Id.*

[182] *See* Joh, *supra* note 13 at 285.

[183] *Id.*

[184] *Id.*

[185] *Id.* at 287.

practical" and police would not and could not "secretly monitor and catalogue every single movement of an individual . . . for a long period of time."[186] Without facial recognition technology, police would need to employ a "super recognizer," an officer "with extraordinary skill at recognizing faces in crowds, to identify a person and retrieve information about that person as they are walking by."[187] However, no such superhuman is needed today.[188] Access to facial recognition technology is "no longer an option for only the most well-off municipal departments."[189] As with the collection of CSLI, the use of facial recognition technology is "remarkably easy, cheap, and efficient compared to traditional investigative tools."[190]

Some may rely on *United States v. Knotts* to counter that "[n]othing in the Fourth Amendment prohibits the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology" may afford them.[191] Generally, police may survey and identify a person while in

[186] United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring).
[187] Hirose, *supra* note 32 at 1607.
[188] *See Facial Recognition Technology: Strong Limits are Necessary to Protect Public Safety & Civil Liberties: Hearing Before the Presidential Comm'n on L. Enf't and the Admin. of Just.* (Apr, 22, 2020) (testimony of Jake Laperruque, Senior Counsel, The Const. Project at the Project on Gov't Oversight) [hereinafter Laperruque] (noting that police in Texas can identify a suspect via a facial recognition search of 48 million photographs in a matter of seconds).
[189] Joh, *supra* note 13 at 288.
[190] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (emphasis omitted).
[191] United States v. Knotts, 460 U.S. 276, 282 (1983). In *Knotts*, the Court held that monitoring the location of the defendant through the use of beeper signals was not an unconstitutional search because the surveillance amounted to following the defendant's vehicle on public streets and highways. *Id.* Simply because police relied on visual surveillance in conjunction with a tracking device did not lead to an unconstitutional search because the defendant's movements were visible to the naked eye. *Id.*

public without a warrant.[192] Facial recognition technology does not allow police to do anything more, the technology simply allows police to complete their work faster and more efficiently.[193] While this argument may have some merit, it vastly underestimates the true power of facial recognition technology.

Consider a real-life example. Police in Texas can use facial recognition to identify a person by searching a database containing 24 million mugshots and 24 million driver license photographs.[194] If police employed a super recognizer to conduct the same search, it would take over 555 days to review all 48 million photographs at a rate of one photograph per second.[195] Facial recognition conducts this entire search in a matter of a few seconds.[196]

Cheap and easy access to facial recognition technology also allows police to passively collect vast amounts of personal data.[197] Police no longer need to "know in advance whether they want to follow a particular individual."[198] When a suspect emerges, police can easily access a deep repository of location and personal information that was collected without the suspect's knowledge and without any real effort by police.[199]

---

[192] *See id.*
[193] Laperruque, *supra* note 188.
[194] *Id*
[195] *Id.*
[196] *Id.*
[197] Joh, *supra* note 13 at 285 (noting that "law enforcement agencies can increasingly turn to [digital] tools that enable them to sort through this [personal] data to look for persons already identified, or for patterns from as yet unknown persons that indicate suspicious behavior.").
[198] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).
[199] Joh, *supra* note 13 at 288.

Finally, facial recognition technology is unique among biometric identifiers, those distinct physical characteristics such as fingerprints and DNA.[200] Until recently, biometric information was collected on an individual, one-time basis, often at the point of arrest or following conviction.[201] If police wanted to obtain a sample of a suspect's DNA to compare with DNA collected at a crime scene or stored in a database, that suspect had to be present—the process was transparent and focused on a specific person.[202] Facial recognition changes the nature of the process.[203] Now police can identify multiple people from a distance—continuously—and then match that person to an aggregate of personal information stored in a database.[204]

While facial recognition technology has the potential to be a useful tool for police to identify suspects, police use of facial recognition presents a serious threat to Fourth Amendment rights.[205] Unregulated use of facial recognition technology will lead to a dramatic increase in police power.[206] Ultimately, people will no longer

[200] *Perpetual Line-Up*, *supra* note 11.
[201] *Id.*
[202] Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 415 (2012).
[203] *See id.* at 415.
[204] *Perpetual Line-Up*, *supra* note 11.
[205] Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, 34 SPG CRIM. JUST. 9 (2019).
[206] *See Perpetual Line-Up*, *supra* note 11.

be free to move about their day without fear that their movements, indeed their very identity, are under surveillance.[207] Proper safeguards are needed.[208]

IV. WHAT *CARPENTER* BUILT: A MODERN METHOD OF ANALYSIS TO ADDRESS THE GROWING THREAT OF FACIAL RECOGNITION TECHNOLOGY

Despite some groups in the United States calling for a moratorium or outright ban on the use of facial recognition technology by police, it appears that the use of the technology will continue.[209] Indeed, facial recognition technology does have the *potential* to provide considerable public safety benefits.[210] However, any potential benefits must be balanced against the protections the Fourth Amendment provides.[211] But what is the correct path forward? When police seek access to a database containing information collected through the use of facial recognition or seek to use facial recognition for investigative purposes, in what circumstances is a warrant required? This section contends that the *Carpenter* test is the answer.

A. The Carpenter *test is appropriate in the context of facial recognition*

As mentioned in Part I, Professor Paul Ohm suggests that the Court in *Carpenter* implicitly articulated a three-factor test to determine whether police access to databases containing personal information is a search under the Fourth

---

[207] *Id.*
[208] *Id.*
[209] *Id.*
[210] Chun, *supra* note 8 at 121.
[211] *Id.*

Amendment: 1) the "deeply revealing nature" of the information; 2) the "depth, breadth, and comprehensive reach" of the information; and 3) the "inescapable and automatic nature of its collection."[212]

Taking Professor Ohm's research one-step further, the *Carpenter* test should not be restricted to CSLI.[213] The *Carpenter* test is appropriate in the context of facial recognition for two reasons. First, the test focuses on the nature of the information collected rather than on how police collected the information.[214] This is appropriate given that the collection of information through the use of facial recognition is generally independent from any affirmative police action.[215] Under the *Carpenter* test, a higher level of inquiry applies when information provides an intimate window into a person's life.[216]

Second, the *Carpenter* test addresses the harms associated with police surveillance and directs an inquiry into the severity of government intrusion into a citizen's private life.[217] The more police seek to collect or access personal information, the more likely that a person will suffer constitutional harms "like the deterrence of lawful activities, interference with relationships, unauthorized information disclosure, risk of exposure and abuse, and psychological harms related

[212] Ohm, *supra* note 18 at 361.
[213] *See id.*
[214] *Id.* at 363.
[215] *See* Joh, *supra* note 13 at 284.
[216] Ohm, *supra* note 18 at 364.
[217] Tokson, *supra* note 117 at 30, 44.

to intrusion."[218] The *Carpenter* test allows judges to consider the nature of the information sought or the nature of the information likely to be revealed, thereby "separating out certain kinds of information and subjecting it to special treatment."[219]

Consequently, when police seek to search a database containing information collected through the use of facial recognition or seek to use facial recognition for other investigative purposes, a judge should conduct an analysis of the information sought or likely to be revealed using the *Carpenter* test.[220] If a judge determines that a warrant is necessary, police must show probable cause—the same standard for GPS and CSLI tracking—in advance of any search.[221]

Judicial approval—in the form of a warrant—under the *Carpenter* test would ensure that facial recognition serves as an effective tool for law enforcement and not as a tool for unconstitutional tracking or targeting.[222] This approval is important because, as the Court has recognized, "the warrant requirement is 'an important working part of our machinery of government,' not merely an inconvenience to be somehow 'weighed' against the claims of police efficiency."[223]

---

[218] *Id.* at 44.
[219] Kerr, *supra* note 15.
[220] Ohm, *supra* note 18 at 363.
[221] *Preserving the Right to Obscurity*, *supra* note 155.
[222] *Id.*
[223] Riley v. California, 573 U.S. 373, 401 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

B. Old doctrines are not useful when applied to digital-age technologies like facial recognition

Of course, the *Carpenter* test is not the first analytical framework that the Court or legal theorists have developed or proposed to determine whether a Fourth Amendment search has occurred.[224] Two tests in particular merit discussion, the reasonable expectation of privacy test and the mosaic theory. However, as discussed below, the *Carpenter* test is the most appropriate framework in the context of facial recognition technology.

1. The reasonable expectation of privacy test

The reasonable expectation of privacy test (or *Katz* test) is no longer useful as a stand-alone method of Fourth Amendment analysis.[225] First formulated by Justice Harlan in *Katz v. United States*, the *Katz* test asks two questions: 1) whether a person has exhibited an actual or subjective expectation of privacy; and 2) whether such an expectation is one that society recognizes as reasonable.[226] If the answer to both questions is yes, then a warrant must generally be granted prior to any search.[227] However, judges and legal scholars have argued that this test is incomprehensible and unworkable.[228]

---

[224] Ohm, *supra* note 18 at 385–390.
[225] *See infra* notes 228–236 and accompanying text (describing the inapplicability of the *Katz* test in an era of rapidly advancing technology).
[226] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
[227] *See* Tokson, *supra* note 117 at 6–8.
[228] *Id.* at 1.

The *Katz* test assumes that a reasonable person has a "well-developed and stable set of privacy expectations."[229] As noted by Justice Alito, technology can change a reasonable person's expectations of privacy.[230] Prior to the digital age, a reasonable person would not have expected police to be able to track her every move.[231] Dramatic advances in technology have made it more difficult to determine what is reasonable.[232] For some, the convenience that technology affords outweighs any privacy concerns.[233] For others, the reverse is true.[234] Prior to the omnipresence of digital technology, what was considered reasonable was generally static; that is no longer the case today.[235] As a result, determining what is reasonable more often than not involves judges substituting "their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks."[236] Indeed, the *Katz* test only exists to provide a "vehicle for some justices to 'update' the Fourth Amendment to conform to their personal views of what limitations ought to be placed on modern government surveillance."[237]

[229] United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring).
[230] *Id.*
[231] Kerr, *supra* note 15.
[232] *See Jones*, 565 U.S. at 427–31 (Alito, J., concurring).
[233] *See id.*
[234] *See id.*
[235] *See id.*
[236] *Id.* at 427 (Alito, J., concurring).
[237] Picadio, *supra* note 76 at 173.

The *Carpenter* test avoids the problems raised by the *Katz* test.[238] The *Carpenter* test places courts in their proper role: "[T]o protect the balance between the state (in the form of the police) and the people, refusing to let technological change eviscerate individual privacy and security from the state."[239] The *Katz* test too often asks whether society is prepared to accept a reasonable expectation of privacy under a descriptive inquiry—whether a particular police power *is* reasonable.[240] The *Carpenter* test, however, allows courts to consider a number of factors under a normative inquiry—*should* police have a particular power.[241]

Additionally, the *Carpenter* test adheres more closely to the text and history of the Fourth Amendment.[242] Privacy—or a reasonable expectation of it—is not mentioned in the Fourth Amendment.[243] Instead, the Fourth Amendment seeks to curb government power over its citizens by limiting the amount of information it knows about us.[244] The *Carpenter* test recognizes the amendment's foundation; each factor of the *Carpenter* test aims to restrict the power of police from accessing deeply revealing personal information.[245]

---

[238] *See infra* notes 239245 and accompanying text (describing the advantages of the *Carpenter* test over the *Katz* test and mosaic theory).
[239] Ohm, *supra* note 18 at 386.
[240] *Id.* at 386–88.
[241] *Id.* at 387–88.
[242] *Id.* at 389.
[243] *Id.*
[244] *Id.* at 390; *Facing the Future*, *supra* note 11.
[245] Ohm, *supra* note 18 at 390.

2. The mosaic theory

The mosaic theory is another framework to identify possible Fourth Amendment searches.[246] The theory was first introduced in *United States v. Maynard*, which involved the warrantless use of a GPS device attached to the defendant's vehicle for a month.[247] There, the court reasoned that "prolonged surveillance reveals types of information not revealed by short-term surveillance."[248] In simple terms, the mosaic theory applies the notion that the sum of information is greater than the individual pieces of information.[249]

The mosaic theory is a step in the right direction because it recognizes that prolonged facial recognition surveillance has the potential to reveal private information in the aggregate.[250] However, the theory fails to fully consider the nature of the information collected and instead focuses too heavily on the quantitative nature of the information collected.[251]

To understand the limitations of the mosaic theory, consider a hypothetical search. Police use real-time facial recognition surveillance to track a suspect over the course of ten days.[252] Police are able to see many locations the suspect visits,

---

[246] Kerr, *supra* note 15.
[247] *See* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 565 U.S. 400 (2012).
[248] *Id.* at 562.
[249] Picadio, *supra* note 76 at 175.
[250] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 321 (2012) [hereinafter *Mosaic Theory*].
[251] Kerr, *supra* note 15.
[252] The author created this hypothetical search.

but no location is particularly personal. Under the mosaic theory, a search may still have occurred because of the quantity of information produced.[253] Instead, what if police use real-time facial recognition surveillance to track the same suspect for only eight hours? Police are still able to see the locations the suspect visits but now the locations are more intimate; the suspect visits a strip club, a by-the-hour motel, and a Planned Parenthood health-center. Under the mosaic theory, a search may not have occurred because the quantity of information is more limited.[254] However, under the *Carpenter* test a search may have occurred because police seek access to information that is deeply revealing in nature.[255]

Carpenter made "it clear that the Court is willing to reconsider old doctrines that do not fit with the realities of the digital age."[256] The *Katz* test and the mosaic theory do not fit the realities of facial recognition technology. One test attempts to determine what may be reasonable when society's relationship with technology changes on an almost daily basis.[257] The other focuses too heavily on the quantity of information rather than on what may be revealed by that information—in small or large quantities.[258] Both frameworks fail to address the unique nature of facial

[253] *See Mosaic Theory*, *supra* note 250 at 333–35.
[254] *Id.*
[255] *See* Ohm, *supra* note 18 at 371.
[256] Price, *supra* note 136 at 50.
[257] *See supra* notes 229235.
[258] *See supra* notes 251255.

recognition technology. For these reasons, the *Carpenter* test should be established as the proper analytical framework in relation to facial recognition technology.

V. APPLYING THE *CARPENTER* TEST: CERTAIN USES OF FACIAL RECOGNITION TECHNOLOGY VIOLATE THE FOURTH AMENDMENT

Not all uses of facial recognition technology are the same.[259] The *Carpenter* test recognizes that some uses of facial recognition technology create new and sensitive risks that threaten Fourth Amendment rights.[260] Other uses of facial recognition are far less controversial and pose little risk to Fourth Amendment rights.[261] Using three hypothetical searches, this section categorizes certain uses of facial recognition according to risk, from those uses of facial recognition technology that pose the highest risk to Fourth Amendment rights—and would constitute a search—to those uses that pose little or no risk to Fourth Amendment rights—and would not constitute a search.

Consider the following hypothetical: on January 25, 2020 more than 10,000 women gathered in Grant Park in Chicago, Illinois for the annual Women's March.[262] Over the course of several hours, protestors marched from Grant Park to

---

[259] *See e.g.*, *Perpetual Line-Up*, *supra* note 11.
[260] *See supra* Part III, Section A.
[261] *See Perpetual Line-Up*, *supra* note 11.
[262] This hypothetical is based on a combination of several actual events—the Chicago Women's March on January 18, 2020 and the events surrounding the "Chicago Seven." *See* Angie Leventis & Madeline Buckley, *Women's March Chicago 2020*, CHI. TRIB. (Jan. 18, 2020), https://www.chicagotribune.com/news/breaking/ct-womens-march-chicago-saturday-morning-20200117-flkr7wstu5ejtkbzfq6mn5ifeu-story.html; Robert Davis, *The Chicago Seven trial and the 1968 Democratic National Convention*, CHI. TRIB. (Sep. 15, 2008), https://www.chicagotribune.com/nation-world/chi-chicagodays-seventrial-story-story.html.

Federal Plaza in support of a variety of issues impacting women and their families. While the majority of the protesters were peaceful and non-violent, several protestors broke store windows in the vicinity of Grant Park and Federal Plaza. Also, there were a few serious altercations with Chicago police officers along the outer edges of the protest. It is unclear whether the actual participants or others unaffiliated with the Women's March were responsible for these more violent and unlawful actions.

Chicago police have identified seven women they believe to be responsible, even if not directly, for these acts. These seven women are all well-known leaders of various advocacy organizations across Chicago.

Abbie Howard is one of the seven women identified by police. Abbie was shocked to hear about the violent actions during the Women's March. In fact, Abbie stayed at Grant Park the entire march because she was not feeling well. A few days before the Women's March, Abbie visited her local Planned Parenthood health-center to have an abortion. Her past two pregnancies were very difficult, and her doctor was concerned that her health would be at risk if she were to have a third child.

Along with Abbie, Bobbie Smith and Tina Hayden were also identified by police as possible suspects. Bobbie and Tina are married and lead an LGBTQ-rights organization in Chicago. The week before the Women's March, both Bobbie and Tina visited various gay and lesbian bars across Chicago to promote the march.

Lea West was also identified by police as a suspect. Lea leads a Catholic charity in Chicago that provides financial support to single mothers. During the week prior to the Women's March, Lea visited a number of Catholic churches to promote the march. Of course, as a devout Catholic, Lea prayed for a few minutes at each church she visited in addition to attending her regular mass.

Police now seek evidence to charge these women with specific crimes in relation to actions that took place during the Women's March.

A. High risk: Real-time facial recognition surveillance

Chicago Police would like to use the department's facial recognition surveillance system to track the movements of these seven women in real-time.[263] Also, police would like to use facial recognition technology to reconstruct each woman's location and movements for two weeks prior to the Women's March using surveillance footage stored in the department's database.[264] The department's facial recognition surveillance system operates across a network of 30,000 cameras

[263] The Chicago Police Department and the Chicago Transit Authority have had a facial recognition surveillance system since 2016. *See America Under Watch*, *supra* note 6. However, the capacity of the department's system is unclear. *Id.* According to DataWorks Plus, the vendor that provides the system to the city, the system includes "Real Time Screening using Facial Recognition on Chicago's vast camera monitoring system which includes 20,000 street, transit and other cameras located throughout the city . . . that allow Chicago to select any number of cameras to monitor using facial recognition." *Id.*

[264] Currently, the Chicago Police Department does not have this capacity; however, "[i]f cities like Chicago equip their full camera networks with face recognition, they will be able to track someone's movements retroactively or in real-time." *See Perpetual Line-Up*, *supra* note 11.

located across Chicago.[265] A local judge has been asked to determine whether a warrant is necessary.

Under the first factor of the *Carpenter* test a judge must consider whether the search is likely to reveal information of a deeply revealing nature.[266] The inquiry is forward-looking and focuses on the goal of the surveillance rather than what is actually found.[267]

Here, Chicago police seek to track the real-time movements of seven women across the city's vast network of surveillance cameras. Such precise and continuous location tracking would certainly reveal intimate, personal, and private information.[268] Consider Abbie Howard, it is likely that real-time surveillance will identify Howard as she visits her local Planned Parenthood health-center for any post-abortion appointments.[269] Regarding Bobbie Smith and Tina Hayden, not only will police likely learn that the two women are a lesbian couple but will also likely learn the sexual preferences of other men and women with whom Smith and Hayden associate.[270] Finally, consider Lea West, it is likely that constant facial recognition surveillance will identify West as she visits her local church for daily

[265] *See America Under Watch*, *supra* note 6.
[266] *See supra* notes 116–118 and accompanying text (discussing the first factor of the *Carpenter* test).
[267] Tokson, *supra* note 117 at 15.
[268] Tokson, *supra* note 117 at 57.
[269] *See supra* notes 175–177 and accompanying text (discussing how certain, sensitive locations may actually be targeted for facial recognition surveillance).
[270] *See Facing the Future*, *supra* note 11.

prayer.[271] The potentially revealing nature of such data provides an intimate window into each woman's life—in direct conflict with the Court's holding in *Carpenter*.[272]

Finally, Chicago police seek access to previously recorded surveillance footage to identify the seven women and then reconstruct their past movements prior to the Women's March. Despite the fact that police may have no interest in, for example, Howard's abortion or West's religious beliefs, police will learn this information during such a search.[273] Therefore, given the likelihood that police may learn intimate, private information, an analysis of the first factor weighs in favor of a warrant requirement.[274]

Under the second factor of the *Carpenter* test a judge must consider the depth, breadth, and comprehensive reach of the information likely to be revealed.[275] In practice, a judge may consider the precision of the information, the extent and duration of surveillance, and how much information is sought.[276]

Here, the surveillance is even more detailed and precise than GPS or CSLI data because facial recognition surveillance is tied to the location of each camera.[277]

---

[271] *Id.*
[272] *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
[273] *See supra* notes 197–199 and accompanying text (discussing how facial recognition surveillance allows police to passively collect information and access that information only after a suspect emerges).
[274] Ohm, *supra* note 18 at 371.
[275] *See supra* notes 119–127 and accompanying text (discussing the second factor of the *Carpenter* test).
[276] Ohm, *supra* note 18 at 373 (2019); Tokson, *supra* note 117 at 18.
[277] *Preserving the Right to Obscurity*, *supra* note 155.

GPS and CSLI require police to estimate the location of the suspect—no estimation is required here.[278] Chicago police seek access to a precise record of each woman's past and present location.

Furthermore, police seek access to millions of data points.[279] Because of Chicago's immense network of 30,000 surveillance cameras, police may access 30,000 set of eyes in real-time in addition to every second of footage those 30,000 eyes have recorded over the past two weeks.[280] Given the likelihood that police seek access to a near-limitless category of precise, personal location information, an analysis of the second factor weighs in favor of a warrant requirement.[281]

The final factor of the *Carpenter* test directs judges to consider the inescapable and automatic nature of collection.[282] A judge should consider whether a suspect assumed the risk of information collection and whether there was any meaningful way to opt out of surveillance.[283] Police use of facial recognition technology is almost always inescapable because the technology relies on a "pervasive and insistent part of daily life"—the human face.[284] To participate in society, a person must venture out *into* society.[285] Here, that means that each

[278] *See supra* notes 161–164 and accompanying text (discussing how facial recognition technology creates a near perfect record of a person's movements).
[279] *See* Joh, *supra* note 13 at 287.
[280] *See America Under Watch*, *supra* note 6.
[281] *See* Ohm, *supra* note 18 at 372–76.
[282] *See supra* notes 128–132 and accompanying text (discussing the third factor of the *Carpenter* test).
[283] Ohm, *supra* note 18 at 376–77.
[284] *Id.* at 376.
[285] *See id.*

woman's face will be exposed to others as well as to police through surveillance cameras.[286]

Applying the *Carpenter* test to the hypothetical search above, Chicago police must obtain a warrant prior to any search or use of facial recognition technology by showing probable cause.[287] This search represents the most serious threat facial recognition technology poses to Fourth Amendment rights—real-time and historic surveillance.[288] Such a search would likely not be protected absent the *Carpenter* test.[289] While no American law enforcement agency currently has the capacity for such a search, the technology does exist—the only limitation is time.[290]

B. Moderate risk: Aggregation of personal information

Consider the same hypothetical again. During the course of the Women's March, various Chicago police officers recorded the protest using body-worn cameras.[291] The police suspect the same seven women but do not know their identity and seek access to the department's facial recognition system to identify these women. The department's facial recognition system compares images of unknown persons against a database of known persons.[292] The database contains

[286] Bhattacharya, *supra* note 95 at 495.
[287] *See* Ohm, *supra* note 18 at 378.
[288] *Perpetual Line-Up*, *supra* note 11.
[289] *Id.*
[290] *See Perpetual Line-Up*, *supra* note 11.
[291] Hamann & Smith, *supra* note 205 at 12 (noting that it may "soon be possible for an officer's body-worn camera to use [facial recognition technology] to identify a person he or she observes on the street.").
[292] *See Facing the Future*, *supra* note 11.

photographs from various sources, including those taken in connection with a suspected crime and DMV photographs.[293] It is estimated that the database contains an identified photograph for 75% of all Illinois residents.[294]

Additionally, for the past two years Chicago police have recorded and stored body-worn camera footage of similar protests.[295] Using the department's facial recognition system, police have identified protestors from this recorded footage and created a file for each identified person.[296] The file notes the person's participation in the protest along with other identifying information.[297]

Under the first factor of the *Carpenter* test a judge must consider whether the search is likely to reveal information of a deeply revealing nature.[298] Here, it is unlikely that police will learn about Howard's abortion or West's religious beliefs, but police may still learn personal information. In effect, Chicago police have created extensive data profiles of virtually every person at a protest over the past two years.[299] In addition to the current search, these profiles may be used for a variety of government purposes ranging from "profiling, to selective law

[293] Chicago currently has the capacity to search a database containing around seven million mugshot photographs. *America Under Watch*, *supra* note 6.
[294] The author created this fact. However, it is not out of the realm of possibility. *See* Laperruque, *supra* note 188 (noting that Texas police can access databases containing 48 million photographs for facial recognition searches).
[295] The Chicago Police Department does not currently have this ability. *See America Under Watch*, *supra* note 6. However, facial recognition makes such a system possible. *See* Joh, *supra* note 13.
[296] *See* Joh, *supra* note 13.
[297] *Id.*
[298] *See supra* notes 116118 and accompanying text.
[299] Preserving the Right to Obscurity, supra note 155.

enforcement investigations, to evaluations for civil service employment opportunities."[300]

Once police identify the seven women, they will likely know what protests, if any, they have attended over the past two years.[301] Consequently, an analysis of the first factor weighs in favor of a warrant requirement because police seek access into each woman's personal life, revealing their private actions and political associations.[302]

The second factor of the *Carpenter* test considers the depth, breadth, and comprehensive reach of the information likely to be revealed.[303] Here, police seek access to a system that is only comprised of past protest footage. As a result, police are unlikely to learn the whereabouts of the seven women except their location while at the Women's March or past protests. However, the inquiry should also consider how frequently Chicago police recorded protest activity.[304] For example, if police recorded footage at 100 protests and subsequently identified participants and catalogued the results, then it is likely that police would gain access to a large amount of personal, political information—weighing in favor of a warrant.[305] However, if police recorded footage at only ten protests, then it is likely that police

[300] Laperruque, *supra* note 188.
[301] *See Preserving the Right to Obscurity*, *supra* note 155.
[302] *See* Ohm, *supra* note 18 at 371.
[303] *See supra* notes 119127 and accompanying text (discussing the second factor of the *Carpenter* test).
[304] *See supra* note 121.
[305] *See supra* note 123.

would gain access to a smaller aggregation of personal, political information—possibly weighing against a warrant.[306]

The final factor of the *Carpenter* test considers the inescapable and automatic nature of collection.[307] Here police seek access to an aggregation of information that was passively collected from law-abiding citizens.[308] The department's database uses a number of sources against which to identify people. With the exception of photographs taken in connection with a potential crime, these photographs were intended to be used for non-criminal activity, namely obtaining a driver's license.[309] None of the women consented to or were even aware that police may use such a photograph to identify them in connection with a suspected criminal act.[310] As a result, an analysis of the third factor weighs in favor of a warrant requirement because police seek access to information that was collected without consent or event notice.[311]

Applying the *Carpenter* test to this hypothetical search, it is likely that Chicago police must obtain a warrant prior to any search or use of facial recognition technology by showing probable cause.[312] Viewed in isolation, it may appear that this search is constitutional because, as opposed to the use of real-time facial

[306] *See supra* note 123.
[307] *See supra* notes 128132 and accompanying text (discussing the final factor of the *Carpenter* test).
[308] *Perpetual Line-Up*, *supra* note 11.
[309] *Id.*
[310] *Id.*
[311] *See* Ohm, *supra* note 18.
[312] *See id.* at 376.

recognition above, the movements of the women were not tracked.[313] However, this search represents the threat posed by the aggregation of data collected through the use of facial recognition.[314] Depending on the frequency with which Chicago police recorded and identified protest attendees, police may access a category of otherwise unknowable information.[315]

C. Low risk: Identification only

Consider the original hypothetical a final time. During the course of the Women's March, various Chicago police officers recorded the protest using body-worn cameras. The police suspect the same seven women as above but still do not know their identity. Now, police would like to use the department's facial recognition system to identify these women. The system compares unknown images against database of known persons, but the database only contains photographs taken in connection with a suspected crime.[316]

This search may proceed without a warrant under the *Carpenter* test.[317] Here, Chicago police do not seek access to deeply revealing personal information. Because the database does not contain profiles of aggregate information, the only information that police will learn, if any, is the identity of the seven women.[318]

---

[313] *See supra* Part IV, Section A.
[314] Ohm, *supra* note 18 at 376.
[315] Joh, *supra* note 13 at 287.
[316] *See e.g.*, *Perpetual Line-Up*, *supra* note 11.
[317] *See* Ohm, *supra* note 18.
[318] *Perpetual Line-Up*, *supra* note 11 ("The primary characteristic of moderate risk deployments is the combination of a targeted search with a relatively targeted database.").

Furthermore, there is no indication that police saved protest footage for future use. While police may learn that the seven women participated in the protest, it is unlikely that such an isolated piece of information weighs in favor of a warrant requirement.[319] Finally, this facial recognition search is only against photographs obtained in connection with a suspected crime.[320] If any of the women do have an identified photograph saved in the database, it was taken with consent and notice.[321]

VI. CONCLUSION

In 1923, Chief Justice Taft wrote a letter to his brother in which he described the automobile as "the greatest instrument to promoting immunity from punishment for crime that we have introduced in many, many years, and we haven't as yet neutralized its effect."[322] Chief Justice Taft was concerned, how would the Court address the rise of the automobile in the context of the Fourth Amendment? Almost one hundred years later, a similar problem has arisen. How will the judicial system protect Fourth Amendment rights in an era of rapid development and use of digital technology?

The Supreme Court faced the problem head-on in *Carpenter v. United States*. The Court signaled its sensitivity to the wealth of private information that

[319] *Id.*
[320] *Id.*
[321] *See id.*
[322] Robert Post, *The Incomparable Chief Justiceship of William Howard Taft*, 2020 MICH. ST. L. REV. 1, 17–18 n. 58 (2020).

police may access. This shift is likely to have far reaching implications for other digital-age technologies, including facial recognition technology.

Despite the benefits the technology may offer, certain uses of facial recognition present a serious threat to Fourth Amendment rights. In particular, facial recognition technology allows police to access vast amounts of previously unknowable information. To balance against potential abusive uses of facial recognition technology, judges must determine when access to certain personal information collected through the use of facial recognition requires a warrant.

However, detaching the Fourth Amendment from its traditional focus presents a challenge that cannot be addressed by old doctrines. Rather, the proper analytical framework in the context of facial recognition lies in *Carpenter*. Now when police seek to access information collected through the use of facial recognition technology or to use the technology to identify unknown persons, a judge should consider the possible search results using the *Carpenter* test.

A founding principal of the Fourth Amendment was to place obstacles in the path of expanding police surveillance. It is now time to place another obstacle in the path of police surveillance. Only by accepting and adopting a modern method of Fourth Amendment analysis will Americans be protected against the threat of facial recognition technology.