Tulsa Law Review

Volume 56 | Issue 2

Winter 2021

Facing Carpenter: Facial Recognition Technology and the Fourth Amendment

Daniel Weatherholt

FACING *CARPENTER*: FACIAL RECOGNITION TECHNOLOGY AND THE FOURTH AMENDMENT

I. INTRODUCTION

As Taylor Swift fans entered the Rose Bowl to attend her concert in May of 2018, they were met by a video display showing behind the scenes footage of Ms. Swift's

rehearsal and preparation for that night's performance.[1] Unbeknownst to her fans, these displays were equipped with outward facing cameras that were capturing images of the concert-goers' faces.[2] As the cameras collected the images, they were cross-referenced against a database that consisted of photos of Taylor Swift's known stalkers.[3] It is unclear whether any matches were made or, if there were matches, what became of the concert-going Taylor Swift stalkers.[4] However, it is clear that Facial Recognition Technology deployed alongside security cameras continues to find new applications and new users.

The proliferation of cameras in America has made it practically impossible to enter the public world without being caught on camera. Cameras are ubiquitous. Companies like Ring[5] and Nest[6] market increasingly sophisticated cameras to residential consumers at a growing rate, making residential and personal security cameras so widely available that they are hardly noticeable in our world today. However, these cameras have created a new vantage point into human activity that, until now, was hardly imaginable at any point in history.

Recent advances in cloud computing, data storage, machine learning, and processing power have brought about a revolution to security camera monitoring—Facial Recognition Technology ("FRT").[7] Law enforcement agencies have begun adapting this technology to serve policing purposes[8]—often forming ongoing relationships with the FRT providers.[9] Like many new technologies, creative applications of FRT and unforeseen consequences abound. These uses present new privacy threats to Americans and have almost no legal precedent or framework through which to regulate and control use of this emerging technology.[10] Many scholars have advocated for legislation to ban FRT nationwide.[11] However, many of the potential applications of FRT would, or do, lack a state actor and fall outside the reach of constitutional protection. Accordingly, this comment seeks to explore the relationship between law enforcement and FRT and argues that FRT is

---

1. Sophan Deb & Natasha Singer, *Taylor Swift Said to Use Facial Recognition to Identify Stalkers*, N.Y. TIMES (July 13, 2018), https://www.nytimes.com/2018/12/13/arts/music/taylor-swift-facial-recognition.html?module=inline.

2. *Id.*

3. *Id.*; *see also* Scott Raab, *Why Taylor Swift Welcomed You to New York*, ESQUIRE (Oct. 20, 2014) https://www.esquire.com/entertainment/music/a30491/taylor-swift-1114/ (detailing the volume of kidnapping and death threats, marriage proposals, and men who show up at Taylor Swift and her mother's houses).

4. Deb, *supra* note 1.

5. RING, https://ring.com/ (last visited Mar. 13, 2020).

6. NEST AWARE, https://store.google.com/us/product/nest_aware?hl=en-US (last visited Mar. 13, 2020).

7. Jay Stanley, *The Dawn of Robot Surveillance*, ACLU 1, 3 (2019), https://www.aclu.org/sites/default/files/field_document/061819-robot_surveillance.pdf.

8. Drew Harwell, *Oregon Became a Testing Ground for Amazon's Facial-Recognition Policing. But What if Rekognition Gets It Wrong?*, WASH. POST (Apr. 30, 2019), https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/.

9. *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (documenting free trials for police departments and discounted annual licensing, as well as promoting FRT to individual officers who would encourage procurement for the entire department).

10. *See* Stanley, *supra* note 7, at 44–45.

11. Hill, *supra* note 9 (quoting Woodrow Hartzog Professor of Law at Northeastern University, "I don't see a future where we harness the benefits of face recognition technology without the crippling abuse of the surveillance that comes with it. The only way to stop it is to ban it.").

analogous to another technology to which the Court recently extended constitutional protection.

The 2018 case of *Carpenter v. United States* is one of the few cases involving individual privacy that the United States Supreme Court has decided in the twenty-first century.[12] The *Carpenter* decision dealt with a criminal defendant's cell phone-generated cell-site location information, which investigating law enforcement agents used to place the defendant at the scene of multiple robberies scattered across multiple states.[13] The defendant challenged law enforcement's use of these records, and the Supreme Court found in the defendant's favor, concluding that the collection of these records constituted a "search" under the Fourth Amendment.[14] This comment seeks to explore what the Justices failed to address—the growing privacy threat that FRT adopted by law enforcement agencies poses to Americans.[15] Though the Supreme Court's holding in *Carpenter* strengthens individual privacy by expanding what constitutes a "search" under the Fourth Amendment, the decision falls short of addressing modern privacy threats to citizens by excluding law enforcement's adoption of facial recognition technology on new and existing surveillance camera networks. This comment argues that FRT deployed over a wide area camera network presents the same threat as cell-site location information presented in *Carpenter* and should also be protected from warrantless access or search by law enforcement.

Part II of this comment details the *Carpenter* decision. A string of robberies in and around Detroit, Michigan, drew the attention of state and federal law enforcement agents. Their investigation led the law enforcement agents to pursue a suspect's Cell-Site Location Information. Ultimately the accessing of this data was reviewed by the Supreme Court. This section reviews the Fourth Amendment precedent weighed by the Court and the privacy concerns that led to the Court's decision.

Part III introduces FRT and explores its application. This section briefly explains the technological advances that led to the current capabilities and explores how FRT is currently used and how the technology could be used as a tracking tool by law enforcement. This part also discusses a potential application of the technology in the United States by detailing its current use in China. Finally, this part argues that current and future applications of FRT violate Fourth Amendment privacy rights.

Part IV applies the *Carpenter* test to FRT and explores the similarity between cell-site location information and the tracking potential of FRT. Finally, this section makes the case against FRT in its current unregulated state and argues that applying the *Carpenter* analysis to it renders government access of data created by FRT an unconstitutional "search" that should be protected by the warrant requirement of the Fourth Amendment.

II. *CARPENTER V. UNITED STATES*: THE SUPREME COURT UPDATES THE FOURTH AMENDMENT

Unbeknownst to most cell phone users, cell phones generate large volumes of

12. Carpenter v. United States, 138 S. Ct. 2206 (2018).
13. *Id.* at 2212.
14. *Id.* at 2222–23.
15. *Id.* at 2220.

location specific, historical cell site location information.[16] Regardless of whether a cell phone is in use, it routinely transmits data to its wireless carrier if it is powered on.[17] Cell phones connect to nearby cell sites, which are radio antennas that receive and transmit radio waves, connecting wireless cell phones to the carrier's wired network.[18] Each time a cell phone connects to a cell site, a record is created which, in aggregate, is called cell site location information, or CSLI.[19] CSLI records capture the cell phone identity, the cell site the phone connected to, and the time of the connection.[20] Cell sites are commonly mounted on a tower—a cell phone tower. However, in urban areas cell sites can be mounted and integrated into light posts, flagpoles, buildings, and other urban fixtures.[21] The area a cell site covers depends upon the number of directional antennas installed and the amount of traffic the cell site handles.[22] As cell phone use and data consumption have grown, cell site concentration has increased, which in turn, has caused a decrease in the area each cell site covers.[23] As cell site coverage area shrinks, CSLI grows more accurate.[24] Early cell phones only generated CSLI at the beginning of a phone call.[25] However, as cell phone capabilities advance and grow, so too do the occasions to connect to the network.[26] Network communications range from sending or receiving a text message to phone applications running routine connections.[27] Increased cell phone connections and shrinking cell site coverage areas have resulted in increasingly accurate, frequent, and thorough CSLI collection.[28]

A. The Carpenter Decision Addressed a Tracking Tool that Most Individuals Carry in Their Pockets—Cell Phones.

In 2011, Detroit police arrested four suspects in connection with a string of robberies targeting Radio Shack and T-Mobile stores.[29] After being taken into custody, one of the suspects confessed that the group had robbed nine different stores across Ohio and Michigan.[30] The suspect implicated fifteen accomplices and provided the police with several of their cell phone numbers.[31] In addition, the FBI searched the suspect's phone and recovered cell phone numbers dialed around the time of each robbery.[32] Using these

16. *Id.* at 2211.
17. *Carpenter*, 138 S. Ct. at 2211–12.
18. *Id.* at 2211.
19. *Id.*
20. *Id.*
21. *Id.*
22. *Carpenter*, 138 S. Ct. at 2211–12.
23. *Id.*
24. *Id.* at 2212.
25. *Id.*
26. *Id.*
27. *Carpenter*, 138 S. Ct. at 2212.
28. *Id.* at 2211–12.
29. *Id.* at 2212.
30. *Id.*
31. *Id.*
32. *Carpenter*, 138 S. Ct. at 2212.

cell phone numbers, prosecutors, working with the FBI, applied for and were granted court orders to obtain cell phone records (from suspects) under the Stored Communications Act. One of the suspects targeted by prosecutors was Timothy Carpenter.[33] Based in part upon the cell phone information obtained by the court orders, prosecutors charged Carpenter with six counts of robbery and six counts of carrying a firearm during a federal crime of violence.[34] In addition to seven other suspects implicating Carpenter as the leader of the robbery ring, the FBI used information from Carpenter's cell phone to build a map that placed Carpenter near the vicinity of four of the robberies at the time that they occurred.[35] The information that the FBI used to build the map detailing Carpenter's location at the time of the robberies was cell site location information.[36]

Before the trial, Carpenter moved to have the CSLI data provided by wireless carriers suppressed.[37] Carpenter argued that the government had violated the Fourth Amendment by seizing his CSLI records without a search warrant supported by probable cause.[38] To obtain a search warrant with probable cause, law enforcement must have '"some quantum of individualized suspicion' before a search or seizure may take place."[39] As mentioned, the Government had obtained the CSLI data through two court orders issued by magistrate judges[40] pursuant to the Stored Communications Act.[41] The Act requires the government to show that cell site evidence "might be pertinent to an ongoing investigation."[42] The Court described this lower evidentiary burden utilized by the Stored Communications Act as a '"gigantic' departure from the probable cause rule."[43] The first court order sought 152 days' worth of CSLI and actually returned 127 days of data.[44] The second court order sought seven days' worth of CSLI and actually returned two days of data.[45] In total, the Government compiled 129 days of Carpenter's CSLI data—a total of 12,898 location points generated by Carpenter's cell phone for an average of 101 location points per day.[46]

The trial court denied Carpenter's motion to suppress.[47] At trial, the Government used this data to produce maps of Carpenter's location throughout the 129 day period, including maps that placed him near four of the robberies Carpenter was charged with.[48] The accuracy of Carpenter's precise location varied in "wedge shaped" sectors that ranged

33. *Id.*
34. *Id.*
35. *Id.* at 2212–13.
36. *Id.* at 2212.
37. *Carpenter*, 138 S. Ct. at 2212.
38. *Id.*
39. *Id.* at 2221 (quoting United States v. Martinez-Fuerte, 428 U.S. 543, 560–61 (1976)).
40. *Id.* at 2212.
41. *Id.* at 2221; *see also* 18 U.S.C. § 2703(d).
42. *Carpenter*, 138 S. Ct. at 2221.
43. *Id.*
44. *Id.* at 2212.
45. *Id.*
46. *Id.*
47. *Carpenter*, 138 S. Ct. at 2212.
48. *Id.* at 2213.

in size between one-eighth and four square miles.[49] The Government relied on this data to "clinch" the case.[50] On appeal the Sixth Circuit affirmed the trial court's decision to permit the CSLI data.[51]

B. A Majority of the Court Found Accessing CSLI to Be a Search Based on Concerns Over Unprecedented Access and Information that Personal Data Grants Law Enforcement

The Supreme Court broke new Fourth Amendment ground by holding that accessing Carpenter's CSLI data constituted a search. While addressing law enforcement access to CSLI, the Supreme Court moved beyond existing Fourth Amendment precedent. The Court rooted its analysis in the basic purpose of the Fourth Amendment, "to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[52] After the Court referenced basic precedential "guideposts,"[53] it acknowledged that CSLI maintained by a third party did not fit into any existing framework and instead fell at the "intersection of two lines of cases."[54] The first line of cases addresses a person's reasonable expectation of privacy in his physical movements and location.[55] The second line of cases concerns the degree of privacy an individual can expect in the information he shares with others.[56] Ultimately, however, the Court decided that an accurate Fourth Amendment analysis of CSLI required a new test to accommodate digitally generated and stored personal location information, breaking new ground in the realm of the 4th Amendment.[57]

i. Privacy in Physical Movement and Location.

The first line of cases the Court considered to resolve CSLI privacy violations in *Carpenter* addressed privacy in an individual's location and movement. In *United States v. Knotts*, the Government used a location beeper, the 1980s-era equivalent of a GPS tracker, to track the vehicle of a suspect.[58] The Government planted the beeper in a container that wound up in the suspect's vehicle.[59] Police used the beeper to measure the distance from the vehicle and assist law enforcement to visually track and follow the vehicle.[60] The Court found that an individual travelling through public streets and conveying their location to any observer had no expectation of privacy.[61] However, the

---

49. *Id.* at 2218.
50. *Id.* at 2213.
51. *Id.*
52. *Carpenter*, 138 S. Ct. at 2213 (quoting Camara v. Mun. Court of City & Cty. of S.F., 387 U.S. 523, 528 (1967)).
53. *Carpenter*, 138 S. Ct. at 2213–14.
54. *Id.* at 2214.
55. *Id.* at 2215.
56. *Id.* at 2216.
57. *Id.* at 2223.
58. *Carpenter*, 138 S. Ct. at 2215 (citing United States v. Knotts, 460 U.S. 276 (1983)).
59. *Id.*
60. *Id.*
61. *Id.* (citing United States v. Knotts, 460 U.S. 276, 281 (1983)).

Court also observed that different constitutional principles would be implicated if this pervasive form of tracking were available to follow a suspect around the clock.[62]

More recently, the Court held that warrantless GPS tracking of a suspect's vehicle over a period of twenty-eight days constituted a search under the Fourth Amendment.[63] In *United States v. Jones*, federal agents placed a GPS tracking device on the frame of a suspect's vehicle while the vehicle was parked at a public parking lot.[64] Law enforcement agents then used the GPS data to connect the suspect to a large drug conspiracy.[65] After receiving a life sentence, the defendant appealed the prosecution's use of GPS surveillance data at trial, which was procured without a warrant.[66] The Court found it was a search, as the Government had physically attached the GPS device to the suspect's car[67]—consistent with traditional Fourth Amendment property based notions of privacy.

Though the Court based its decision on property grounds, five justices concurred, indicating that continuous, twenty-eight day monitoring constituted a search, despite the tracked car's movements being observable by the public, expanding the holding of *Jones*.[68] An intrusion into an individual's privacy is considered a search when law enforcement invades their reasonable expectation of privacy.[69] The Court has recognized a reasonable expectation of privacy where an individual "demonstrated an actual expectation of privacy" and it is one "that society is prepared to recognize as reasonable."[70] In the *Jones* concurrences, two competing expectation of privacy theories were advanced. Justice Alito wrote, "society's expectation has been that law enforcement agents and others 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."[71] While Justice Sotomayor found a search in law enforcement's invasion of a "reasonable societal expectation of privacy in the sum of one's public movements."[72] Though these concurrences differ, they both advocate a search where law enforcement deploys "collective public monitoring over time."[73] Though the Court had found an expectation of privacy in physical movements and location, the scale of CSLI data addressed in *Carpenter* exceeded the scope of these cases.

ii. The Third-Party Doctrine.

Carpenter then shifted its focus to the 'third-party doctrine,' which provides that an

---

62. *Id.* (citing U.S. v. Knotts, 460 U.S. 276, 283–84 (1983)). In *Knotts,* the Court emphasized that the beeper used to track the defendant was rudimentary and did not reveal the defendant's movements completely, just those he revealed by entering the roadway. By emphasizing the limited capabilities of the beeper, the Court left the question of complete twenty-four hour tracking undecided. 460 U.S. 276, 283–84 (1983).

63. United States v. Jones, 565 U.S. 400, 404–05 (2012).

64. *Id.* at 403.

65. *Id.* at 403–04.

66. *Id.* at 404.

67. *Carpenter*, 138 S. Ct. at 2215 (citing United States v. Jones, 565 U.S. 400, 404–05 (2012)).

68. *Id.*; United States v. Jones, 565 U.S. 400 (2012).

69. ORIN S. KERR, COMPUTER CRIME LAW 401 (4th ed. 2018) [hereinafter COMPUTER CRIME].

70. *Id.* at 403.

71. United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring).

72. *Id.* at 415–16 (Sotomayor, J., concurring).

73. COMPUTER CRIME, *supra* note 69, at 404.

individual has no right to privacy for information that he voluntarily shares with a third party.[74] The doctrine is rooted in *United States v. Miller*.[75] While investigating Miller for tax fraud, the Government subpoenaed bank records and check stubs from Miller's banks.[76] Miller challenged the Government's collection of financial records as an unconstitutional search under the Fourth Amendment.[77] Noting that Miller never had "ownership or possession,"[78] the Court found that Miller had a limited expectation of privacy regarding the records because he had assumed the risk by sharing his personal information with another person.[79]

The Supreme Court expanded the third-party doctrine in *Smith v. Maryland*, where the Court held that an individual holds no reasonable expectation of privacy over phone numbers they dial when they share them with their telephone company.[80] In both *Miller* and *Smith*, the Court reasoned that the individuals in question had voluntarily shared their personal information with third parties, and thus, they had no reasonable expectation of privacy in that information retained in the regular course of business by the respective third-parties. But in contrast to these third-party doctrine cases, as the Court noted in *Carpenter*, the nature of the data held by the cell phone providers is of a "qualitatively different category" than call logs or bank records, which would suggest that the nature of the information sought by law enforcement may affect the applicability of the third-party doctrine.[81]

iii. Distinguishing the Privacy in Location and Third-Party Doctrines.

The *Carpenter* Court distinguished the Government's collection of CSLI from GPS tracking of physical movements and the third-party doctrine's accessing of a third-party's records compiled in the regular course of business. Though accessing CSLI yields information that is similar to information captured by GPS tracking of a vehicle, and the third-party doctrine is implicated because CSLI is information used and collected by a third-party wireless carrier, the nature of CSLI moved the Court beyond existing Fourth Amendment doctrines.

Government acquisition of CSLI data presents a greater intrusion into individual privacy than prior cases have addressed.[82] Prior to *Carpenter,* the Supreme Court found that individuals do not surrender their expectation of privacy by entering the public sphere.[83] This remains true for CSLI, but the information that data collected by CSLI reveals is drastically more invasive than the prior-considered GPS information. CSLI opens a "window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations'" to

74. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).
75. *Id.* at 2215 (citing United States v. Miller, 425 U.S. 435 (1976)).
76. *Carpenter*, 138 S. Ct. at 2216 (citing United States v. Miller, 425 U.S. 435 (1976)).
77. *Id.* at 2215 (citing United States v. Miller, 425 U.S. 435 (1976)).
78. United States v. Miller, 425 U.S. 435, 440 (1976).
79. *Id.* (finding no reasonable expectation of privacy in bank records).
80. Smith v. Maryland, 442 U.S. 735 (1979).
81. *Carpenter*, 138 S. Ct. at 2216.
82. *Id.* at 2217.
83. *Id.*

an even greater extent than GPS tracking previously had revealed about a suspect's life.[84] The Court also recognized the extent to which cell phones have practically become a "feature of the human anatomy," enabling near perfect tracking of the cell phone's owner.[85] Additionally, the Court observed that this "near perfect" form of surveillance can be achieved with remarkable ease and is "remarkably easy, cheap, and efficient compared to traditional investigative tools."[86] Despite the many similarities between the location-revealing nature of both GPS and CSLI data, the Court chose to treat the latter with a new analysis that recognized the much more powerful location tracking capabilities of CSLI.

Another unique aspect of CSLI is what the Court called the "[r]etrospective quality of the data."[87] The breadth of the historical record that CSLI data gives law enforcement is unprecedented. Previously, law enforcement was limited in their investigatory power both by time and the "dearth of records and the frailties of recollection."[88] This afforded American citizens a form of privacy inherent in the relationship between citizens and law enforcement. When an investigation commenced, law enforcement officials were limited by what they could reconstruct from a witness's memory and physical records and what they could observe going forward from the start of the investigation. CSLI seems to obliterate this check or limit on police power.

The Court distinguished CSLI from GPS; unlike GPS, with CSLI "police need not even know in advance whether they want to follow a particular individual, or when."[89] Because CSLI is being "continually logged for all of the 400 million devices in the United States," when a criminal investigation is opened or a new suspect identified "[w]hoever the suspect turns out to be, he has effectively been tailed every moment of every day."[90] Were the government allowed to access this information without a search warrant, effectively everyone would be tailed, every day, with only their wireless carrier's CSLI data retention policy for protection. Considering the invasive nature of CSLI and its near perfect surveillance capabilities, the Court held that when law enforcement accessed Carpenter's CSLI records, they "invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements."[91]

The Court explicitly declined to extend the third-party doctrine to cover CSLI. Regarding CSLI, the Court held, "[w]hether the Government employs its own surveillance technology" to capture CSLI or obtains it from a wireless carrier as in *Carpenter*, "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[92] The Court's willingness to extend Fourth Amendment protection beyond CSLI collected and stored by wireless carriers to CSLI captured directly by Government surveillance demonstrates how personal and revealing the Court found CSLI data to be regardless of its source. The Court articulated that

84. *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).
85. *Carpenter*, 138 S. Ct. at 2218 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).
86. *Id.* at 2217–18.
87. *Id.* at 2218.
88. *Id.*
89. *Id.*
90. *Carpenter*, 138 S. Ct. at 2218.
91. *Carpenter*, 138 S. Ct. at 2219.
92. *Id.* at 2217

obtaining CSLI from a wireless carrier is not "a garden-variety request for information from a third-party witness."[93] The technology that captures CSLI represents a "seismic shift in digital technology."[94] CSLI is a seismic shift because the data captured in CSLI is "nearly infallible;" it is an "exhaustive chronicle of location information" and is collected from everyone, not for a short period of time, but going back years.[95]

The third-party doctrine partly derives from the idea that individuals have a reduced expectation of privacy in information that they knowingly and voluntarily share with another.[96] However, the Court views detailed logs of an individual's physical location, compiled daily and stored for years, to be outside the scope of information covered by the third-party doctrine.[97] The nature of what CSLI reveals is simply too private. Significantly, the Court rejected the argument that an individual voluntarily shares CSLI with their wireless carrier. The Court did not see carrying a cell phone as a true choice, as cell phones are such an integral part of day-to-day life that "carrying one is indispensable to participation in modern society."[98]

Most importantly to individual privacy concerns, the Court noted the inescapable nature of the CSLI collection, observing that there is no way to "[a]void leaving behind a trail of location data."[99] Cell phones generate CSLI without any "affirmative act on the part of the user beyond powering up" the phone by receiving calls, texts, and checking for application updates.[100] Thus, the Court concluded that the user could not assume the risk of turning over CSLI voluntarily. Even though the Government obtained Carpenter's CSLI from a third party, this "does not overcome Carpenter's claim to Fourth Amendment protection," against government searches.[101] Accordingly, the Court found "[t]he Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment"[102] and held that law enforcement must secure a search warrant in order to access CSLI.[103]

iv. New Factors Considered by the Court to Protect CSLI Under the Fourth Amendment.

In addition to the consideration of previous Fourth Amendment doctrines, the Court based its decision, at least in part, on features unique to CSLI and future capabilities of the technology. With an eye toward the future, the Court observed that "the rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.'"[104] The Court's position was likely affected by the fact that it was

93. *Id.* at 2219.
94. *Id.*
95. *Id.*
96. *Carpenter*, 138 S. Ct. at 2219.
97. *Id.* at 2220.
98. *Id.*
99. *Id.*
100. *Id.*
101. *Carpenter*, 138 S. Ct. at 2220.
102. *Id.*
103. *Id.* at 2222.
104. *Id.* at 2218–19 (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).

considering events that took place in 2011 from a vantage point seven years later in 2018. However, there is a sense in the opinion that the Court was giving consideration to future advances beyond simply acknowledging the time that had passed since Carpenter's CSLI was accessed. As University of California Law Professor and Fourth Amendment scholar, Orrin Kerr, notes, one of the best examples of the Court's willingness to imagine future iterations of the capabilities of CSLI data is the discrepancy of the facts of the Carpenter investigation and the purported location tracking capabilities of CSLI data in the Court's opinion.[105] The CSLI evidence presented against Carpenter at trial placed him at the robbery locations with varied degrees of accuracy ranging from areas of one-eighth of a square mile to four square miles.[106] However, the Court discussed the ability of wireless carriers to pinpoint a cell phone's location within fifty meters.[107] The Court used the threat of CSLI accuracy to bolster its argument that this technology should be protected from the government by the requirement of a search warrant. Though Kerr is critical of the discrepancy,[108] the Court is right to be concerned by inevitable advancements in the capabilities of CSLI. The Court's willingness to consider present or near future technological capabilities is necessary in light of the staggering amount of personal data generated, collected, and stored in today's world.[109] The Court rightly takes some latitude in addressing a technology that has the potential to track every American carrying a cell phone around the clock.

C. The Carpenter *Test*

The Court held that CSLI is protected under the Fourth Amendment because of the "deeply revealing nature of CSLI;" its "depth, breadth, and comprehensive reach;" and the "inescapable and automatic nature of its collection."[110] This test reveals the factors the Court found to be the most repugnant to the Fourth Amendment's right to freedom from unwarranted searches. First, CSLI data is "deeply revealing."[111] The Court was concerned about the volume of information that can be gleaned from accessing a person's CSLI data—a lot.[112] Second, CSLI captures a "comprehensive" record of a cell phone user's life.[113] As the Court discussed, cell phones have become part of the human anatomy; essentially everyone has one, and almost everyone carries it wherever they go.[114] Third, cell phones automatically collect a user's location data without a meaningful alternative for the user. The Court acknowledged that there is no meaningful choice to opt-out of CSLI collection. The only real way to avoid generating CSLI is to turn off the cell phone

105. Orin S. Kerr, *Implementing* Carpenter (forthcoming) (manuscript at 14–15), https://ssrn.com/abstract=3301257.

106. *Carpenter*, 138 S. Ct. at 2218.

107. *Id.* at 2219.

108. Kerr, *supra* note 105, at 14–15.

109. Michael Kwet, *The Rise of Smart Camera Networks, and Why We Should Ban Them*, THE INTERCEPT (Jan. 27, 2020, 11:53 AM), https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks/; *The Great Hack* (Netflix July 24, 2019).

110. *Carpenter*, 138 S. Ct. at 2223.

111. *Id.*

112. *Id.* at 2218.

113. *Id.* at 2223.

114. *Id.* at 2218.

or go without it, which, the Court has already conceded is an unreasonable expectation.[115] The Court, in going beyond previous case law and identifying new characteristics to weigh in determining whether data generated by a new technology ought to be protected from government search absent a warrant, seems to signal that there are technologies that present such a great threat or undermine individual privacy to such an extreme that they fall under Fourth Amendment protection, despite who holds the actual records.[116]

Part of the *Carpenter* test also captures an awareness that the test '"must take account of more sophisticated systems that are already in use or in development.'"[117] This is accomplished by considering the advancements that CSLI technology has made in the time since the robberies occurred. The factors the test considers also reveal that justices in the majority recognized the significance of the threat to individual privacy presented by CSLI and other similar technologies. In fact, this threat is what pushed the majority to articulate a new test—the threat to privacy that big data generated by technology creates. Before articulating the test, the Court seemed to be self-aware of its own inability to address head-on the persistent privacy concerns that new technology, like CSLI, will present.[118] Despite the Court's desire to limit its decision to the facts before it, its reluctance to engage other technology-enabled privacy threats leaves doubt for law enforcement regarding how to apply the *Carpenter* test to emerging technologies in the future.

III. FACIAL RECOGNITION TECHNOLOGY, SECURITY CAMERAS, AND LAW ENFORCEMENT

In *Carpenter*, the Supreme Court declined to extend its holding to "conventional surveillance techniques and tools,"[119] insisting that its decision to require a warrant when law enforcement accessed encyclopedic-like location information held by a third party was a "narrow one."[120] However, the *Carpenter* analysis should be applied to another emerging technology—one capable of more invasive and revealing data collection—facial recognition technology ("FRT").[121] Specifically, the *Carpenter* analysis should be applied to FRT deployed on surveillance camera networks.

A. Incorporating Facial Recognition Technology on Existing Security Cameras

FRT, the ability of a computer to recognize a face, relies on "machine vision," which is the ability of a computer to analyze video input received from a camera.[122] Simply put, it gives a computer to the ability to see. Machine vision has enabled an array of advances in technology in recent years and has become ubiquitous in modern life.[123] Examples of

115. *Carpenter*, 138 S. Ct. at 2220.
116. *Id.* at 2222.
117. *Id.* at 2220 (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).
118. *Id.* at 2220 n.4.
119. *Id.* at 2220.
120. *Carpenter*, 138 S. Ct. at 2220.
121. Clare Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, GEO. L. CTR. ON PRIVACY & TECH. (May 16, 2019), https://www.americaunderwatch.com/ [hereinafter Garvie, *America Under Watch*].
122. Stanley, *supra* note 7, at 9.
123. *Id.*

machine vision applications include copyright enforcement, self-driving cars, Snapchat filters, and facial recognition.[124] Progress in machine vision has been enabled and accelerated by artificial intelligence, or the ability of a computer to learn.[125] Artificial intelligence not only allows a computer to recognize faces but also to register human behavior and perceive human emotion.[126] Artificial intelligence enables FRT and also powers other forms of video analytics.[127]

The United States contains more video surveillance cameras per capita than any other country in the world.[128] Studies suggest that the total number of cameras in the United States was around 40 million in 2014.[129] Though this number is staggering, it has undoubtedly continued to rise as technology has improved, costs have sunk, and ease of access to cameras has improved.[130] Despite the number of cameras, the video captured by surveillance cameras has remained siloed and difficult to analyze. Cameras and camera networks were, and for the most part remain, isolated between public and private entities, like large corporations and small businesses, or municipal and city governments and the federal government.[131] In addition, most video is never watched, both because it contains nothing of interest and because, as Department of Justice experts have noted, live monitoring of such video is both extremely "boring" and "mesmerizing."[132] Reviewing surveillance footage or live monitoring a camera feed is also difficult. One study found that "[a]fter only 20 minutes of watching and evaluating monitor screens, the attention of most individuals has degenerated well below acceptable levels."[133] Though an individual might be captured by any number of cameras across an array of applications, monitoring and analyzing captured video remains difficult, expensive, and time-consuming.[134] However, as FRT develops, it has the potential to unlock video that was previously inaccessible to review.

FRT does not operate in isolation; it relies on some form of input of images, typically from video cameras.[135] This relationship can be thought of as a surveillance video camera capturing images as the "eyes" and FRT processing the captured images as the "brain."[136] Thus, surveillance cameras observe and gather information while FRT analyzes the information. In 2012, Senator Al Franken described facial recognition technology as

---

124. *Id.*

125. *Id.* at 7.

126. *Id.* at 6.

127. *See, e.g.*, Stanley, *supra* note 7, at 4.

128. *Id.* at 3 n.3.

129. *Id.*

130. Stanley, *supra* note 7, at 3; *see* Megan Wollerton, *The era of the $200 security camera is over*, C-NET (July 5, 2020), https://www.cnet.com/news/the-era-of-the-200-security-camera-is-over/ (discussing the developing trend in low cost home security cameras).

131. Stanley, *supra* note 7, at 4.

132. Mary W. Green, *The Appropriate and Effective Use of Security Technologies in U.S. Schools*, NAT'L INST. JUST. 178265 (Sept. 30, 1999), https://nij.ojp.gov/library/publications/appropriate-and-effective-use-security-technologies-us-schools.

133. *Id.*

134. Stanley, *supra* note 7, at 4.

135. *Id.* at 3; VICE News, *How China Tracks Everyone*, YOUTUBE (Dec. 23, 2019), https://www.youtube.com/watch?v=CLo3e1Pak-Y.

136. Stanley, *supra* note 7, at 3.

creating a digital "faceprint;" similar to a fingerprint, the faceprint is "a unique file describing your face."[137] Like fingerprints, unidentified faceprints are referenced against a database of identified faceprints to create a match. This fingerprint metaphor is a helpful starting place for understanding the capabilities of FRT.

Broadly, FRT is a computer-based program that is capable of scanning an image or video of anonymous persons to identify the faces captured in the image or video frame.[138] FRT is able to recognize faces, scan the face down to the individual pixel, locate and catalog facial features as identifying markers, and create a template of the unknown face.[139] The markers on a template consist of measurements of the face, like the distance between eyes, or the width of the nose.[140] These measurements "make a face unique."[141] FRT also identifies "nodal points," or facial landmarks, and their measurements in relation to the face as a whole.[142] The newly generated template, also referred to as a "face signature" or a "map" of the unidentified face is matched against existing identified image databases.[143] Identified image databases range from private collections of images, like known Taylor Swift stalkers,[144] to public collections like states' driver's license databases or the national passport database.[145]

Privately held identified image collections can be as comprehensive as the databases held by the government. Facebook's 2010 feature "tag suggestions" was powered using facial recognition technology.[146] Tag suggestions enabled Facebook to help a user identify friends in photos the user uploaded, making it easier for the user to tag their friends in photos.[147] As a result, Facebook's database of "face templates"[148] or "faceprints" is thought to be the largest in the world, as Facebook had 800 million users in 2010.[149] Once an individual's face template has been created, Facebook is able to identify that individual in any other photograph uploaded onto the platform by any Facebook user, regardless of that individual's awareness or consent.[150] Though Facebook users are able to opt out of the tag suggestions feature, the function must be disabled manually.[151]

Through use of FRT, identification can be made both in real time and in retrospect.[152] Real-time scanning has been used to screen fans at sporting events. For

---

137. *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcommittee on Privacy Technology and the Law of the Committee on the Judiciary*, 112th Cong. 1 (2012) (statement of Senator Al Franken) [hereinafter *Hearing*].

138. Kristine Hamann & Rachel Smith, *Facial Recognition Technology*, CRIM. JUST., Spring 2019, at 9.

139. *Id.* at 10.

140. *Id.*

141. Patel v. Facebook, Inc., 932 F.3d 1264, 1268 (9th Cir. 2019).

142. Hamann, *supra* note 138, at 10.

143. *Patel*, 932 F.3d at 1268.

144. Deb, *supra* note 1.

145. Hamann, *supra* note 138, at 9.

146. *Patel*, 932 F.3d at 1268.

147. *Id.*

148. *Id.*

149. *Hearing*, *supra* note 137, at 2.

150. *Patel*, 932 F.3d at 1273.

151. *Hearing*, *supra* note 137, at 2.

152. Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Face Recognition in America* (Oct. 16, 2016), https://www.perpetuallineup.org/risk-framework. ("If cities like

example, in 2019, police in Wales used cameras attached to police vans to screen spectators on their way to a rugby match.[153] Police used a database of mug shots as a matching reference and monitored the system in real-time.[154] Conversely, FRT is also creating new retrospective capabilities to store and summarize surveillance footage.[155] FRT automates the indexing and storing of collected video, which will allow a human viewer to search existing video or review a summarized compilation.[156] Video search and summarization addresses the gap, or gulf, between the amount of recorded video that is created and the difficulty and cost of analyzing it.[157] There are a number of different methods to summarize video. However, they all seek to capture and emphasize important events, like license plate numbers, faces of people that walk through a specified area, cars, or any imaginable criteria.[158] Within a matter of minutes, a lightly traveled road or walkway can be summarized by showing each person or car that traveled through that area over the course of several hours or days.[159] With the advent of cloud storage, amassing and storing a large volume of video is no longer limited to large, "deep-pocketed organizations" with a high level of expertise.[160] FRT's tracking capabilities will continue to improve as software is perfected, cost of implementation drops, and cameras become more prevalent.[161]

B. Current FRT Applications Demonstrate the Technology's Powerful Tracking Potential

Though comprehensive location tracking, surveillance, and identification seem like something from a "dystopian dream"[162] of the future, it is becoming a reality around the world.[163] As of 2020, China has the most prolific application of FRT for purposes of state surveillance, specifically the deployment of FRT in the Xianjing region in the southwestern part of China. Xianjing is home to the Uighurs, an ethnic Muslim minority

---

Chicago equip their full camera networks with face recognition, they will be able to track someone's movements retroactively or in real-time, in secret, and by using technology that is *not* covered by the warrant requirements of existing state geolocation privacy laws").

153. Adam Satariano, *Real-Time Surveillance Will Test the British Tolerance for Cameras*, N.Y. TIMES (Sept. 15, 2019), https://www.nytimes.com/2019/09/15/technology/britain-surveillance-privacy.html?searchResultPosition=2.

154. *Id.*

155. Stanley, *supra* note 7, at 28.

156. *Id.*

157. *Id.*

158. *Id.* at 28–29.

159. *Id.* at 29.

160. Stanley, *supra* note 7, at 11.

161. *See* Lola Fadulu, *Facial Recognition Technology in Public Housing Prompts Backlash*, N.Y. TIMES (Sept. 24, 2019), https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html.

162. Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, N.Y. TIMES (July 8, 2018), https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html [hereinafter Mozur, *Inside China*].

163. *The Daily: The Chinese Surveillance State, Part 1*, N.Y. TIMES, (May 6, 2019) https://www.nytimes.com/2019/05/06/podcasts/the-daily/china-surveillance-uighurs.html [hereinafter *Chinese Surveillance Part 1*] (using facial recognition software for ethnic profiling and social control); *The Daily: The Chinese Surveillance State, Part 2*, N.Y. TIMES, (May 7, 2019) https://www.nytimes.com/2019/05/07/podcasts/the-daily/china-uighurs-internment-camps-surveillance.html [hereinafter *Chinese Surveillance Part 2*].

numbering approximately eleven million people.[164] Authorities in this region have adopted mass surveillance and identification as a tool in their effort to convert a long-occupied Muslim region into a more Chinese influenced and controlled area.[165] In recent years, police have turned to facial recognition technologies to assert control and monitoring over the Uighurs.

In this region of China, being recorded on camera and identified by FRT is not merely a risk upon venturing out in public, it is a certainty. In Guiyang, a "vast" and "sophisticated" camera system encompasses the city.[166] The system, which uses FRT and artificial intelligence to analyze video input, is able to locate and identify anyone who ventures into public within a matter of minutes.[167] Police can monitor citizens in real time and are also able to review a suspect's past movement as far back as a week.[168] Though authorities are using facial recognition technology to target persons with a criminal past, police are also programming the facial recognition system to track the Muslim Uighurs based on their distinctive skin tone and facial features.[169] The dataset used to program the distinction between ethnic groups is a set of pictures identified as either the Muslim minority or the ethnic Chinese.[170] The artificial intelligence is fed these identified pictures and is programmed, or learns, to distinguish between the two groups.[171] This enables Chinese authorities to target the Uighurs by identifying them and tracking their movement and activity, as well as who they associate with, both in real time and in retrospect.

Though the Chinese Government is responsible for this surveillance and monitoring, it has been enabled by Chinese technology companies.[172] There are at least four major Chinese technology companies working to develop the technology for China's facial recognition systems, and each company is individually valued at over one billion dollars.[173] Companies working on China's surveillance camera networks have benefitted greatly from the Government's 2018 promise to invest billions of dollars in surveillance.[174] Indeed, one Chinese FRT company, MegVii, received a half a billion dollar investment in 2019, much of which came from a State operated venture capital fund.[175] These companies have helped facilitate the Government's targeting of the Uighurs and other non-Chinese ethnic minorities in China.[176] However, these minority

---

164. *Chinese Surveillance Part 2*, *supra* note 163.

165. *Chinese Surveillance Part 1*, *supra* note 163.

166. Garvie, *America Under Watch*, *supra* note 121.

167. *Id.*

168. *Id.*

169. Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html [hereinafter Mozur, *Face Scans*].

170. *Id.*

171. *Id.*

172. Zak Doffman, *Has Huawei's Darkest Secret Just Been Exposed By This New Surveillance Report?*, FORBES (Nov. 29, 2019) https://www.forbes.com/sites/zakdoffman/2019/11/29/has-huaweis-darkest-secret-just-been-exposed-by-this-new-report/#277a4e1a4061.

173. Mozur, *Face Scans*, *supra* note 169.

174. *Id.*

175. VICE News, *How China Tracks Everyone*, YOUTUBE (Dec. 23, 2019), https://www.youtube.com/watch?v=CLo3e1Pak-Y.

176. Mozur, *Face Scans*, *supra* note 169.

tracking capabilities are marketed as the technology's ability to recognize "sensitive groups of people."[177] Despite marketing efforts to dilute the potent potential of facial recognition technology, the Chinese Government remains open about how it is using facial recognition technology.[178]

Part of China's surveillance strategy is to conduct the surveillance in public. Billboards show video, captured by security cameras running FRT, of offenders jay walking, or committing other minor offenses and display the identity of the offender in public places for others to note and observe.[179] These billboards and the Government's surveillance capabilities are publicly known and often overstated, as the perception of surveillance is also a useful tool.[180] Coupled with China's growing FRT capabilities, the country has launched the pilot of a social credit score program.[181] The program aims to track all Chinese citizens using big data, cameras, and FRT to award a score based on an individual's behavior.[182] In 2018, China's National Public Credit Information Center reported that over seventeen million people with low social scores were barred from purchasing plane tickets.[183] While the full effects of China's adoption of FRT remain unclear, the present privacy and human rights conditions in China should serve as a warning as FRT continues to promulgate in the United States. Though China contains about four times the number of surveillance cameras as the United States—about 200 million cameras, with the goal of increasing that number to 600 million in the coming years[184]—the United States has a growing list of camera networks.[185] These are networks on which FRT could be readily deployed.[186]

C. Banning Facial Recognition Technology

In the United States, reception to FRT has been mixed. Some state and municipal governments have responded to the effects of FRT by banning government use of the technology. San Francisco, Oakland, Berkeley, and Somerville, Mass., have all banned municipal government—including police—use of FRT.[187] On a larger scale, the state of

---

177. *Id.*

178. Mozur, *Inside China*, *supra* note 162.

179. *Id.*

180. *Id.*

181. Divya Chowdhury & Neha Malara, *Reports of 'Big Brother' China Social Credit System Untrue: AI Expert Xue Lan*, REUTERS, (Jan. 22, 2020) https://www.reuters.com/article/us-davos-meeting-lan/reports-of-big-brother-china-social-credit-system-untrue-ai-expert-xue-lan-idUSKBN1ZL2P9; *see also Black Mirror: Nosedive* (Netflix original series released Oct. 21, 2016) (portraying a dystopian society where every individual rates their interaction with others on a scale of one to five to generate a social score. An individual's social score is visible to all people who they interact with.).

182. VICE News, *How China Tracks Everyone*, YOUTUBE (Dec. 23, 2019), https://www.youtube.com/watch?v=CLo3e1Pak-Y.

183. *Id.*; Joe McDonald, *China bars millions from travel for 'social credit' offenses*, ASSOC. PRESS (Feb. 22, 2019), https://apnews.com/9d43f4b74260411797043ddd391c13d8.

184. VICE News, *How China Tracks Everyone*, YOUTUBE (Dec. 23, 2019), https://www.youtube.com/watch?v=CLo3e1Pak-Y.

185. Mozur, *Inside China*, *supra* note 162.

186. Garvie, *America Under Watch*, *supra* note 121.

187. Evan Selinger & Woodrow Hartzog, *What Happens When Employers Can Read Your Facial Expressions?*, N.Y. TIMES (Oct. 17, 2019), https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html.

California has considered banning FRT in police-worn body cameras,[188] and in Europe, European Union officials have begun considering a total ban of FRT.[189] Meanwhile, in Florida, law enforcement has embraced FRT and its potential to identify criminal suspects.[190] In 2001, Florida became the first state to adopt FRT and later helped the FBI develop its own system.[191] It appears that Florida is not using FRT for wide area surveillance but instead for suspect identification (scanning a picture of an unidentified suspect with FRT), running an estimated 8,000 matches per month.[192]

The San Francisco ordinance contains the reasoning for the ban: "[t]he propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits . . . and the technology will exacerbate racial injustice and threaten our ability to live free of continuous government monitoring."[193] Studies have shown that FRT is significantly less accurate when scanning the faces of people of color and women.[194] Fairness and civil rights concerns are just some of the many issues raised by those who advocate for a total ban of FRT. In addition, proponents of a total ban of FRT argue that the lack of transparency and rules around the application of the technology justify banning it.[195] In Europe, the European Commission is considering a five-year ban of FRT to develop policy to prevent abuse and to improve regulation around data and privacy rights.[196] While the contemplation of a total ban is outside the scope of this comment, many of the same arguments for a total ban bolster the need to have FRT information protected by the search warrant requirement.

IV. APPLYING *CARPENTER* TO FACIAL RECOGNITION TECHNOLOGY

FRT deployed over a camera network covering a wide area represents a similar, if not a more severe, threat to individual privacy than the threat posed by CSLI in *Carpenter*. For that reason, accessing of FRT should be considered a search and should be protected by the warrant requirement of the Fourth Amendment. Specifically, wide area camera networks which are integrated with a facial recognition system. The threat requires two components: first, wide area camera networks, which require a physical infrastructure to feed data to; second, a facial recognition system, monitoring and compiling the input for real-time or historical analysis. Imagine a major walkable American city, where cameras proliferate every intersection, store front, parking lot, neighborhood entrance, apartment

188. Reis Thebault, *California Could Become the Largest State to Ban Facial Recognition in Body Cameras*, WASH. POST (Sept. 11, 2019), https://www.washingtonpost.com/technology/2019/09/12/california-could-become-largest-state-ban-facial-recognition-body-cameras/.

189. *Facial Recognition: EU Considers Ban of Up to Five Years*, BBC (Jan. 17, 2019), https://www.bbc.com/news/technology-51148501.

190. Aaron Mak, *Facing Facts: A Case in Florida Demonstrates the Problems with Using Facial Recognition to Identify Suspects in Low-Stakes Crimes*, SLATE (Jan. 25, 2019) https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html.

191. *Id.*

192. *Id.*

193. Shirin Ghaffary, *San Francisco's facial recognition technology ban, explained*, VOX (May 14, 2019), https://www.vox.com/recode/2019/5/14/18623897/san-francisco-facial-recognition-ban-explained.

194. Garvie, *America Under Watch*, *supra* note 121; Fadulu, *supra* note 161.

195. Garvie, *America Under Watch*, *supra* note 121.

196. *EU Considers Ban*, *supra* note 189.

building, subway station, and bus stop. An individual moving about a city with a wide area camera network could be easily and accurately tracked as they travel, getting picked up by different cameras. Passing beneath the lens of a single camera would not reveal much about an individual's daily activity. However, as the number of cameras that an individual encounters increases, so too does the amount of information about the individual that can be gleaned from the camera footage. Cities like New York City, Washington D.C., Chicago, Detroit, and Orlando are all examples of major population centers with the first component—wide area camera networks—already in place.[197]

The surveillance model in Detroit, Michigan, named Project Green Light, is the most alarming.[198] The Detroit Police Department ("DPD") and the City of Detroit have created a system where law enforcement can access live video from cameras located in businesses, health clinics, apartment buildings, and schools.[199] The program's initial goal was to deter crime at high traffic businesses open during late-night hours.[200] Since its inception, the program has grown substantially.[201] In 2019, Detroit's mayor proposed to expand the camera network and coverage by adding hundreds of traffic light cameras.[202] The combination of cameras in private businesses and public spaces would allow police to "track any shooter or carjacker across the city."[203] All Project Green Light cameras, no matter where they are located, transmit back to a control center monitored by the DPD.[204] DPD also has access to the driver's license database.[205] Regardless of the specifics of the second component—the facial recognition system and its capabilities, or how the video input is cataloged and how long it is stored[206]—Detroit has laid the foundation for a tracking system capable of following the people of Detroit almost anywhere they go, around the clock. This program is not hidden from the public, as locations with a participating camera have green lights installed to alert visitors that they are being monitored.[207] In theory, an individual could avoid visiting participating businesses and

197. Garvie, *America Under Watch*, *supra* note 121.

198. *Agreements: Memorandum of Understanding Project Green Light Agreement*, CITY OF DETROIT, https://detroitmi.gov/departments/police-department/project-green-light-detroit#block-views-block-related-links-block-1 (last visited Jan. 30, 2020) [hereinafter *Project Green Light Agreement*].

199. Garvie, *America Under Watch*, *supra* note 121.

200. *Id.*

201. Francis X. Donnelly, *Project Green Light Welcomes 500th Business*, THE DETROIT NEWS (Mar. 11, 2019), https://www.detroitnews.com/story/news/local/detroit-city/2019/03/11/project-green-light-welcomes-500th-business/3132789002/.

202. Amy Harmon, *As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias*, N.Y. Times, (July 8, 2019) https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html. [hereinafter Harmon, *Racial Bias*].

203. *Id.*; *see also* Click on Detroit | Local 4 | WDIV, *2019 Detroit State of the City address*, YOUTUBE (Mar. 5, 2019), https://www.youtube.com/watch?v=dXAZoMCl3qs (the Mayor's 2019 State of the City Address, promising hundreds of more video cameras at city intersections).

204. Garvie, *America Under Watch*, *supra* note 121.

205. *Id.*

206. *Project Green Light Agreement*, *supra* note 198 ("Storage: At the Owner's sole cost and expense, the Owner will ensure that footage from all cameras at that Owner's Covered Business(es) is stored on an Axis approved SD/SDHC card, and for at least thirty (30) days via a network-attached storage device ("NAS") or cloud-based storage that will be compatible with DPD's surveillance software provider.").

207. Harmon, *supra* note 202.

locations. However, Detroit currently has thousands of cameras deployed[208] with plans to install hundreds more, everywhere from traffic lights[209] to public housing.[210] Does a Detroit resident have a meaningful alternative to being filmed should they choose to avoid Project Green Light cameras?

Examples like the tracking of the Uighurs in China and the camera networks in the United States demonstrate the tracking ability, or potential tracking ability, of a facial recognition system fed by a wide-area camera network. However, the length of video retention remains a variable—that is, how far back in time FRT would be able to scan for an individual's face. However, it doesn't seem like a stretch to assume that once the video is collected, the party responsible for its collection will have an interest in retaining this data for a period of weeks or months at the minimum to be able to search the historical record.[211] This would give law enforcement, or third parties collecting this data, the ability to track a person's activity continuously within a surveilled area like a city. When law enforcement uses FRT to track an individual in real-time or search a database of video for a person's past activity (whether held by a third party or collected by the government), this action should constitute a search and fall under the protection of the Fourth Amendment's search warrant requirement.

A. Applying the Carpenter Test to FRT

In *Carpenter*, the Court considered a long list of characteristics that influenced its decision to hold that using a cell phone and accompanying CSLI records to track a suspect over an extended period of time violated the Fourth Amendment.[212] However, the Court highlighted three characteristics in concluding its opinion: (1) "the deeply revealing nature" of the collected information; (2) the information's "depth, breadth, and comprehensive reach;" and (3) "the inescapable and automatic nature of its collection."[213] In addition to this test, the Court expressed that the cell phone being used to track Carpenter was "almost a 'feature of the human anatomy.'"[214] By comparing CSLI and FRT and evaluating FRT through the *Carpenter* test, it is clear that tracking an individual using FRT raises the same constitutional concerns that CSLI raised in *Carpenter*.

i. Deeply Revealing Nature

The first factor of the *Carpenter* test focuses on the nature of the information being searched itself, rather than how the information was generated or the method used to collect it.[215] As professor Paul Ohm notes, this factor of the test protects information only

208. *Id.*
209. *Id.*
210. Garvie, *America Under Watch*, *supra* note 121.
211. *See generally* Lucas Mearian, *CW@50: Data storage goes from $1M to 2 cents per gigabyte*, COMPUTERWORLD (Mar. 23, 2017), https://www.computerworld.com/article/3182207/cw50-data-storage-goes-from-1m-to-2-cents-per-gigabyte.html (detailing the falling cost of data storage).
212. Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 370 (2019).
213. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).
214. *Id.* at 2218 (quoting Riley v. California, 573 U.S. 373, 385 (2014).
215. *Id.* at 2223; Ohm, *supra*, note 212, at 371.

if it is '"deeply revealing' of some private quality of the person under surveillance."[216] Professor Ohm argues that this factor represents a significant break from previous Fourth Amendment analysis because it centers on the collected information rather than what was done to collect it or prevent its collection.[217] The *Carpenter* test considers what the collected information reveals rather than the manner in which the information is collected.[218] This shift is preceded by two ideas articulated by precedent: first, that location information ought to be protected because it shows "familial, political, professional, religious, and sexual associations;"[219] and second, that cell phones "hold for many Americans the 'privacies of life.'"[220]

Location information collected by FRT meets the criteria of the first factor of the *Carpenter* test. FRT is capable of collecting deeply intimate information about an individual's life. As discussed above, cameras paired with FRT are currently in use to track Uighurs in all facets of their lives.[221] In Detroit, Michigan, private property owners have the option to purchase cameras that are connected to Detroit's Project Green Light. These cameras feed directly to the Detroit Police Department for monitoring.[222] Some of the locations participating in the program include schools, churches, and health clinics.[223] Outdoor cameras alone that monitor the exterior of these locations would generate deeply revealing information. Any individual who entered a school, church, or clinic would be recorded and memorialized. Monitoring would reveal persons who entered these places. But consider internal or indoor cameras, as the Green Light program mandates, which would reveal even more.[224] Internal cameras would expose what an individual did inside: whether they stayed in the waiting room of the clinic or received treatment from a care provider; picked up a child from school or voted in an election in the gymnasium; attended worship in the sanctuary or dropped off food at the church's food pantry. It would all be captured and potentially stored. The information collected by security cameras clearly reveals intimate details of life. FRT threatens to capture and catalog this information to make it more accessible and revealing to law enforcement. For many, our day to day activity reveals the privacies of life.[225] Because the video recorded, cataloged and searchable by FRT, has a "deeply revealing nature," it meets the first factor of the *Carpenter* test.

ii. Depth, Breadth, and Comprehensive Reach

The second factor of the *Carpenter* test centers on the "depth, breadth, and

---

216. Ohm, *supra* note 212, at 371.

217. *Id.*

218. Kerr, *supra* note 105, at 1.

219. Ohm, *supra* note 212, at 371 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

220. *Id.* (quoting *Riley*, 573 U.S. at 403 (2014)).

221. Mozur, *Face Scans*, *supra* note 169.

222. Garvie, *America Under Watch*, *supra* note 121.

223. Harmon, *supra* note 202 (project green light locations include apartment buildings, churches, and schools); Garvie, *America Under Watch*, *supra* note 121 (project green light locations included fifteen health clinics).

224. *Project Green Light Agreement*, *supra* note 198.

225. *Riley*, 573 U.S. at 403.

comprehensive reach" of the information collected.[226] This three-part factor ultimately evaluates the "quantity of information stored."[227] One way to illustrate this factor is to imagine a spreadsheet or a table of information. The vertical columns represent the different types of information gathered, like the timestamp of *when* a record was created, the location or *where* it was created, and *who* was identified. The horizontal rows would each represent a single record. In *Carpenter,* a new row was created each time Carpenter's cell phone connected to a cell tower; the captured information included a timestamp of when a cell phone connected to the nearest cell phone tower (time), the location of that tower (place), and the cell phone number (identity).[228] The greater the volume of the information contained in this spreadsheet—in terms of columns and rows—the greater the protection it deserves from government search.

Depth refers to time; the longer an individual has been tracked, the more records have been generated and the greater the depth of the information collected.[229] In *Carpenter*, the CSLI in question spanned five years (because the wireless carrier arbitrarily chose a five-year retention policy),[230] but investigators had requested 127 days' worth of the data.[231] However, in a footnote, the Court observed, "[i]t is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search."[232] Although this does not completely clarify the issue of the length of time required to trigger a search, it served as a strong reference point.[233]

Breadth refers to the frequency at which the data is collected.[234] The more frequently datapoints are created, the greater the "breadth" of the data. Both "breadth" and "depth" contribute to the quantity of information that is collected, as the more frequently data is collected, over a longer period of time, the more complete a picture of an individual's life the data paints.[235]

Comprehensive reach refers to "the number of people tracked in a database."[236] In *Carpenter*, the Court observed that "location information is continually logged for all of the 400 million devices in the United States," and that "this newfound tracking capacity runs against everyone."[237] "Comprehensive reach" not only means that the data collection indiscriminately affects everyone, but also that it is constantly created, revealing a comprehensive record of an individual's life.

FRT meets this factor and its subparts. Like CSLI, the nature of the information

---

226. *Carpenter*, 138 S. Ct. at 2223.

227. Ohm, *supra* note 212, at 372.

228. *Carpenter*, 138 S. Ct. at 2225.

229. Other scholars argue that "depth" refers to "detail and precision of the information stored." Ohm, *supra* note 212, at 372. However, this makes an already tricky test—three factors with multiple sub-parts—unnecessarily burdensome to apply. The test ought to remain as clear and straightforward to apply as possible.

230. *Carpenter*, 138 S. Ct. at 2218.

231. *Id.*

232. *Id.* at 2217 n.3.

233. Ohm, *supra* note 212, 374–75 ("The Court gave no principled reason for selecting seven days as the cut-off, so we ought not consider it the precise dividing line. Future opinions will need to analyze the relationship between the temporal breadth of data and the impact on privacy interests.")

234. Ohm, *supra* note 212, at 372.

235. *Carpenter*, 138 S. Ct. at 2223.

236. Ohm, *supra* note 212, at 373.

237. *Carpenter*, 138 S. Ct. at 2218.

collected by FRT deployed over a wide area camera network is of a sufficient "depth, breadth, and comprehensive reach" to warrant protection from law enforcement. Security cameras capture video constantly, and the limits on storage capacity are vast. This means that camera feeds can be stored permanently and accessed at a later date to be searched for a suspect or target. Thus, there is practically no limit to the "depth" of the information collected. The "breadth" of FRT, while not as complete as CSLI, is sufficient to be protected from search by law enforcement. The frequency with which an individual is identified, or seen, by a camera depends on the saturation of cameras in a certain area. In the cities mentioned above, the frequency of being captured on camera is high. For example, an individual living in New York City who relies on the subway for their daily commute to work would be captured frequently just going about their day.[238] The "comprehensive reach" of FRT is similar to that of CSLI. Like CSLI, FRT is constantly collecting data and indiscriminately captures virtually everyone who walks in front of a camera. If there are cameras everywhere, then FRT enabled tracking could far surpass CSLI tracking—rather than knowing an individual's general location, the state can see who you were with, what you wore, and what you did in any given place.

iii. Inescapable and Automatic Nature of Its Collection

The third factor of the *Carpenter* test focuses on the "inescapable and automatic nature of its collection."[239] This factor considers what an individual did, or did not do, which led to the creation of the data. Inescapability refers to the real-world choices an individual has in creating the data, while "automatic collection" refers to the digital process which creates the data.[240] In *Carpenter*, "inescapable" referred to an individual's choice to use or not use a cellphone, while "automatic collection" referred to the digital process that created the data point, like making or receiving a phone call or a cell phone connecting to the nearest cell tower without an affirmative act by the phone's user. [241] The Court did not see cell phone use in modern-day society as a choice, observing that there are more cell phones in the United States than people[242] and noting that cell phones have become "almost a 'feature of human anatomy.'"[243]

The final factor of the *Carpenter* test is met when applied to FRT. Being filmed by a security camera represents an inescapable occurrence in an individual's life. While an individual may be able to escape being captured on camera by choosing a certain route, using an alternate entrance to a business, or wearing a sombrero, once camera saturation reaches a critical mass, being spotted on camera will become unavoidable. While an individual can choose whether or not to carry a cell phone—though the Court does not see

238. James Pasley, *I documented every surveillance camera on my way to work in New York City, and it revealed a dystopian reality*, BUS. INSIDER (Dec. 6, 2019), https://www.businessinsider.com/how-many-security-cameras-in-new-york-city-2019-12 (documenting how many surveillance cameras a New York City based journalist encounters on his daily commute).

239. *Carpenter*, 138 S. Ct. at 2223.

240. Ohm, *supra* note 212, at 376–77.

241. *Carpenter*, 138 S. Ct. at 2220.

242. *Id.* at 2211.

243. *Id.* at 2218 (quoting *Riley*, 573 U.S. at 385).

this as real choice[244]—an individual has much less autonomy and control over where cameras are mounted and ways to avoid being seen, scanned, and tracked by FRT. Though our society has come to rely on cell phones, they represent a modern convenience which an individual could reasonably go without and survive. The same choice does not exist when it comes to leaving one's home to work, eat, or socialize. FRT poses a more inescapable mode of surveillance than CSLI posed in *Carpenter* because cameras are more difficult to avoid than cell phones. FRT, like CSLI, is also automatically collected. The most distinguishable feature between the two is that the data FRT collects may have larger holes than that of CSLI. For example, if an individual is filmed walking into their workplace, there may not be a recording of that individual during working hours while they are in their office. However, despite potential holes in the data generated by FRT, the tracking capabilities are comparable to those of CSLI—inescapable, and automatic.

V. CONCLUSION

Though the Supreme Court's holding in *Carpenter* strengthens individual privacy by expanding what constitutes a "search" under the Fourth Amendment, the decision falls short by failing to limit how far into an individual's past the government can go in accessing personal information generated by other forms of technology. *Carpenter* demonstrates that there are technologies that present such a great erosion—and threat to—individual privacy that they fall under the protection of the Fourth Amendment. The CSLI in *Carpenter* revealed so much about an individual's life that government access to that information constituted a search. As facial recognition technology deployed over a wide area camera network shares many of the same characteristics as CSLI—though more accurate and more revealing—government access to information generated by FRT should also be considered a search and have Fourth Amendment protection extended to it. Though this expansion of the *Carpenter* holding would not disturb many of the alarming applications of FRT by companies and individuals, nor disturb their ability to share captured video with law enforcement, requiring a warrant to access information generated by FRT would make it more difficult for police to amass a complete record of an individual's activity. Taylor Swift would retain the right to screen her concerts for stalkers using FRT. However, government law enforcement agents would have an additional check on their powers—"prevent[ing] 'a too permeating police surveillance.'"[245]

- Daniel Weatherholt[*]

244. *Carpenter*, 138 S. Ct. at 2218.

245. *Jones*, 565 U.S. at 416–17 (Sotomayor, J., concurring) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

[*] Daniel Weatherholt is a Juris Doctor Candidate at the University of Tulsa College of Law. He currently serves as Notes & Comments Editor of the Tulsa Law Review. He would like to thank Professor Ido Kilovaty for setting him on this path, as well as Anna Sanger, Whitney Humphrey, Ryan Curry, and Caroline Lindemuth for their indispensable edits and feedback.