Arizona Law Journal of Emerging Technologies

Volume 4 *Article 4*

01-2021

FACIAL RECOGNITION TECHNOLOGY: HOW WILL LAWMAKERS AND THE COURTS RESPOND TO THE GROWING DEMAND FOR POLICY DEVELOPMENT?

Claire Bosarge
Tulane University School of Law

2020-2021 https://azlawjet.com **Vol. 4, Art. 3**

Arizona Law Journal of Emerging Technologies

FACIAL RECOGNITION TECHNOLOGY: HOW WILL LAWMAKERS AND THE COURTS RESPOND TO THE GROWING DEMAND FOR POLICY DEVELOPMENT?

Claire Bosarge, JD Candidate

Table of Contents

FACIAL RECOGNITION TECHNOLOGY: HOW WILL LAWMAKERS AND THE COURTS RESPOND TO THE GROWING DEMAND FOR POLICY DEVELOPMENT?

Claire Bosarge*

I. Introduction

> "Imagine a government tracking everywhere you walked over the past month without your permission or knowledge . . . [or] a database of everyone who attended a political rally that constitutes the very essence of free speech . . . This has long been the stuff of science fiction and popular movies – like . . . '1984' – but now it's on the verge of becoming possible." – Brad Smith, President of Microsoft[1]

This excerpt offers a glimpse of future America if the commercial and governmental use of facial recognition technology (FRT) persists without federal regulation.[2] FRT is a rapidly advancing biometric authentication method that identifies or verifies the identity of a person by comparing specific facial features detected in an image or video to faces stored within a database.[3]

Although the most well-known use of FRT is by law enforcement agencies, there are numerous other entities that utilize FRT, such as cell phone manufacturers, universities, social media companies, and retailers.[4] For instance, during American pop star Taylor Swift's *Reputation* tour, a mesmerizing screen displaying rehearsal footage was secretly

* J.D. Candidate, Tulane University School of Law, 2021

[1] Brad Smith, *Facial Recognition Technology: The Need for Public Regulation and Corporate Responsibility*, MICROSOFT (July 13, 2018), http://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/.
[2] *See id.*
[3] Steve Symanovich, *How Does Facial Recognition Work?*, NORTON http://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html (last visited Mar. 16, 2020).
[4] Symanovich, *supra* note 4.

used to scan and compare fans' faces to images of hundreds of the star's known stalkers.[5] Information on the use, collection, and storage of facial recognition data is scarce, but a 2016 study, released by the Center on Privacy & Technology at Georgetown Law, reported that the face of one in two American adults is in a facial recognition database.[6]

One false match in a facial recognition system can result in missed flights, police interrogations, or even a false arrest.[7] Nevertheless, the global market for FRT is projected to grow to $7 billion in 2024, from $3.2 billion in 2019.[8] The drastic expected growth is due to the escalating use of FRT in commercial applications.[9] Fittingly, it is expected that by 2023, U.S. Customs and Border Protection will have the ability to scan the faces of 97% of commercial airline passengers departing the U.S.[10]

Although FRT has become mainstream,[11] widespread, unregulated use of FRT creates serious privacy concerns.[12] While some state and local governments have placed restrictions on the use of FRT, the federal government has struggled to gain much traction limiting the uses of FRT by federal agencies.[13] Moreover, the U.S. Supreme Court has yet to hear a case regarding the use of FRT.[14] However, in *Carpenter v. United States*, the Supreme Court held that the government must obtain a warrant to acquire cell phone location data (CPLD) from a cellular provider.[15] The Court declared that an individual

[5] Steve Knopper, *Why Taylor Swift Is Using Facial Recognition at Concerts*, ROLLING STONES (Dec. 13, 2018, 11:24 AM), http://www.rollingstone.com/music/music-news/taylor-swift-facial-recognition-concerts-768741.
[6] Clare Garvie et al., *The Perpetual Line-Up: Unregulated Facial Recognition in America*, GEO. L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), http://www.perpetuallineup.org.
[7] Abdullah Hasan, *2019 Proved We Can Stop Face Recognition Surveillance*, ACLU (Jan. 17, 2020), http://www.aclu.org/news/privacy-technology/2019-was-the-year-we-proved-face-recognition-surveillance-isnt-inevitable/.
[8] *Facial Recognition Market Worth $7.0 Billion by 2024 - Exclusive Report by MarketsandMarkets™*, CISION: PR NEWSWIRE (June 27, 2019), http://www.prnewswire.com/news-releases/facial-recognition-market-worth-7-0-billion-by-2024--exclusive-report-by-marketsandmarkets-300876154.html.
[9] Symanovich, *supra* note 4.
[10] Allie Funk, *I Opted Out of Facial Recognition at the Airport—It Wasn't Easy*, WIRED (July 2, 2019, 9:00 AM), http://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/.
[11] Sharon Nakar & Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, 23 B.U. J. SCI. & TECH. L. 88, 91 (2017).
[12] Symanovich, *supra* note 4.
[13] Facial Recognition Technology Warrant Act of 2019, S.2878, 116th Cong. (2019) ("Currently, government agencies can use facial recognition technology to surveil a person without any unified federal law, regulation, or oversight.").
[14] *See* Clare Garvie et al., *The Perpetual Line-Up: Unregulated Facial Recognition in America-Risk Framework*, GEO. L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), http://www.perpetuallineup.org/risk-framework#footnote29_xbi6f92.
[15] *Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018).

maintains a legitimate expectation of privacy, for Fourth Amendment purposes, "in the record of his physical movements as captured through [CPLD]."[16] Given the similarities between CPLD and facial recognition data, the holding in *Carpenter* may be extended to a case challenging large-scale surveillance through the use of FRT.[17]

This Article addresses the privacy concerns presented by the widespread unregulated implementation of FRT and explores possible responses by the legislature and courts. Part II details the mechanics of FRT and recent technological developments. Part III addresses why FRT may be characterized as a double-edged sword by touching on (1) the various applications of FRT in different industries, (2) the fallibility of FRT, and (3) the criticisms of FRT that drive the need for policy development. Part IV provides a detailed analysis of *Carpenter*, and predicts how the courts may interpret the holdings in *Carpenter* when faced with a case challenging FRT. Part V demonstrates the need for federal regulations restricting FRT and provides the pending and enacted state and local legislative acts imposing restrictions on the use of FRT. Part V also proposes model legislation for regulating FRT. Part VI discusses the pervasiveness of surveillance cameras equipped with FRT in China to demonstrate the dystopic like society that can result from the widespread, unregulated use of FRT.

II. How Does Facial Recognition Technology Work?

Human beings have an innate ability to recognize and distinguish human faces, but only within the past fifty years have computers been programmed to exercise the same ability.[18] Using computer algorithms, facial recognition systems measure and analyze distinguishable landmarks, or nodal points, that exist on the human face.[19] Specific measurements–such as the distance between the eyes, width of the nose, depth of the eye sockets, and length of the jaw line–may be extracted from either a two-dimensional (2-D) face image or a three-dimensional (3-D) face model.[20] The 3-D face recognition software

[16] *Id.* at 2217.
[17] *See* Memorandum from Majority Staff on Hearing on *"Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties"* to be heard before the H. Comm. on Oversight and Reform, 116th Cong. (2019).
[18] Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, HOW STUFF WORKS, http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.html (last visited Feb. 16, 2020).
[19] *See id.*; Brian Newlin, *A Closer Look at Facial Recognition Technology*, CLICKONDETROIT (Oct. 4, 2019), http://www.clickondetroit.com/2019/10/04/a-closer-look-at-facial-recognition-technology-2/.
[20] Bonsor & Johnson, *supra* note 19.

captures the distinct geometry of a face from multiple angles.[21] By using depth and an axis of measurement that is unaffected by lighting, 3-D face recognition systems can detect a face in darkness and have the ability to recognize "a face in profile" if the head is positioned perpendicular to the camera's line of view.[22]

Despite advances in FRT that allow for 3-D facial imaging, many facial recognition systems still rely on 2-D imaging for the sake of convenience, as most images in facial recognition databases are stored in 2-D format.[23] The first systems were developed in the 1960s and operated by comparing 2-D images.[24] The difficulty posed by 2-D systems is that the newly captured image and the image within the database must be an equal distance from the camera, and have similar lighting, similar facial expressions, and similar facial alignment.[25] A deviation in light or orientation reduces the ability of the system to correctly match the newly captured image with a stored image, which consequently reduces the recognition accuracy.[26] In any event, 3-D systems have emerged and have proven to be more accurate than their 2-D counterparts.[27]

The process of identifying and verifying the identity of an individual through a facial recognition system involves several steps.[28] First, the system receives either a still photo, like those taken upon arrival at a U.S. airport, or a frame from a video of a person in motion.[29] Once the system detects a face within the 2-D image or video, it scales, rotates, and aligns the face "so that every face that the algorithm processes is in the same position."[30] When the front of the head is facing the camera, the face is in the best position

[21] Space and Naval Warfare Systems Center, *System Assessment and Validation for Emergency Responders Tech Note: Three-Dimensional Facial Recognition*, U.S. DEP'T OF HOMELAND SECURITY (May 2008), http://www.dhs.gov/sites/default/files/FacialRecognition-TN_0508-508.pdf.
[22] Bonsor & Johnson, *supra* note 19.
[23] Andrew Heinzman, *How Does Facial Recognition Work?*, HOW-TO GEEK (July 11, 2019, 6:40 AM), http://www.howtogeek.com/427897/how-does-facial-recognition-work/; *The Complete Guide to Facial Recognition Technology*, PANDA SECURITY (Oct. 11, 2019), http://www.pandasecurity.com/mediacenter/panda-security/facial-recognition-technology/.
[24] Bonsor & Johnson, *supra* note 19; Jesse Davis West, *A Brief History of Facial Recognition*, FACEFIRST (Aug. 1, 2017), http://www.facefirst.com/blog/brief-history-of-face-recognition-software/.
[25] Space and Naval Warfare Systems Center, *supra* note 22.
[26] *Id.*; Bonsor & Johnson, *supra* note 19.
[27] Song Zhou & Sheng Xiao, *3D Face Recognition: A Survey*, 8:35 HUMAN-CENTRIC COMPUTING & INFO. SCI. 1, 6 (2018).
[28] Bonsor & Johnson, *supra* note 19.
[29] Bill Mann, *How Does Facial Recognition Technology Work? – 5 Real World Use Cases*, BLOKT (Aug. 19, 2019), http://blokt.com/guides/facial-recognition.
[30] Clare Garvie et al., *The Perpetual Line-Up: Unregulated Facial Recognition in America - Background*, GEO. L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), http://www.perpetuallineup.org/background#footnoteref17_re3c47a.

for detection.[31] However, the system is capable of recognizing a face so long as the head is not rotated more than thirty-five degrees away from the camera in a 2-D system, or more than ninety degrees in a 3-D system.[32]

Once the face is aligned, the facial recognition system extracts certain facial features and measures the curves of the subject's face on a sub-millimeter scale to create a template.[33] The template is converted into a unique, numerical code called a faceprint.[34] The faceprint can be compared to other faceprints within the database to find a potential match.[35] If FRT is used for verification purposes, or to confirm a subject's identity, the image is matched to only one other image in the database.[36] If FRT is used for identification purposes, the algorithm will compare the image to other existing images in the database and generate a "numerical score reflecting the similarity of their features."[37]

A recent development in FRT, known as Surface Texture Analysis (STA), analyzes skin biometrics or the uniqueness of skin texture to produce even more accurate results.[38] With a picture of a patch of skin, called a skinpatch, STA uses "algorithms to turn the patch into a mathematical, measurable space."[39] The software is then able to distinguish "the actual skin texture" as well as any lines or pores within the skinpatch.[40] STA is so advanced that it can "identify differences between identical twins, which is not yet possible using facial recognition software alone."[41] STA software may be used separately or in conjunction with other methods of FRT to increase accuracy.[42] According to one biometrics company, combining FRT with STA increases identification accuracy by 20 to 25%.[43]

Facial recognition systems are constantly advancing, as evidenced by the development of STA and even more recent developments like "real-time emotion recognition," which maps

[31] PANDA SECURITY, *supra* note 24.
[32] Bonsor & Johnson, *supra* note 19.
[33] *Id.*
[34] *Id.*; PANDA SECURITY, *supra* note 24.
[35] Bonsor & Johnson, *supra* note 19.
[36] *See* Bonsor & Johnson, *supra* note 19; Garvie et al., *supra* note 31.
[37] Garvie et al., *supra* note 7; see also Bonsor & Johnson, *supra* note 19.
[38] Bonsor & Johnson, *supra* note 19.
[39] *Id.*
[40] *Id.*
[41] *Id.*; *See also* Mara Calvello, *Facing the Reality of Facial Recognition: The Good and the Bad*, G2 (Oct. 15, 2019), http://learn.g2.com/facial-recognition.
[42] U.S. Gov't Accountability Office, GAO-15-621, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law* (2015), http://www.gao.gov/assets/680/671764.pdf.
[43] Bonsor & Johnson, *supra* note 19.

a subject's facial expressions to detect emotions such as anger, fear, and surprise.[44] However, this may create a false sense of progress, given that each of these advancements only improve the accuracy of 3-D face recognition systems and cannot be applied to systems that rely on 2-D images. Because most facial recognition systems in use today rely on 2-D camera technology,[45] the inaccuracy of facial recognition systems remains unresolved.[46]

III. Facial Recognition Technology: A Double-Edged Sword

a. The Many Uses of FRT in Law Enforcement and Beyond

Law enforcement agencies can benefit from FRT in several different contexts.[47] An officer on duty who encounters someone who is unable to identify themselves can take a photo of the individual and use facial recognition software to see if the photo matches any of the photos in the officer's database, which may include "mug shots, driver's license photos, or face images from unsolved crimes."[48] If there is video or photographic evidence of a suspect's face, then FRT also may be used to search an image against a database during an investigation.[49] Another common use of FRT is during "Real-time Video Surveillance," when police officers possess images of specific individuals they are trying to locate.[50] Once these images are uploaded to a database known as a "hot list," FRT is used to extract facial images from a live video surveillance feed and to compare them to the images on the "hot list."[51] Each individual who walks within the video camera's range of detection may be subject to this process.[52] The same FRT method can be applied to compare archived video images to a "hot list" database.[53]

[44] Bill Siuru, *Is Facial Recognition Technology Ready for Prime Time?*, POLICE & SEC. NEWS (Sept. 18, 2019), http://policeandsecuritynews.com/2019/09/18/is-facial-recognition-technology-ready-for-prime-time/.
[45] *Identity Matters: Facial Recognition in 2019*, GEMALTO, http://www.gemalto.com/review/facialrecognition/index.aspx (last visited Mar. 22, 2020).
[46] *See* Garvie et al., *supra* note 31.
[47] *See* Calvello, *supra* note 42.
[48] Garvie et al., *supra* note 7.
[49] The photo or video still of a suspect's face may be obtained from a security camera, smartphone, social media post, or even from an officer who clandestinely photographed the suspect. Garvie et al., *supra* note 7.
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*

As FRT becomes less expensive, more and more industries will begin to use it.[54] FRT is used in airports to verify that a foreign traveler in a database is the same person who seeks entry into the United States.[55] Some banks use FRT at ATMs and check cashing kiosks in order to allow their customers to verify their identity using their faceprint in place of a personal identification number or card swipe.[56] There are healthcare mobile phone applications that use FRT to detect rare genetic disorders such as Cornelia de Lange syndrome and Angelman syndrome.[57] FRT is used in retail stores to identify known shoplifters that walk into the store.[58] An individual who is caught shoplifting in one store may have a digital record of their face shared with other store owners across the country who use the same FRT company.[59] One FRT provider stated that the police are automatically alerted any time the retail store's facial recognition system detects a known shoplifter's face, even if they are not shoplifting.[60] Whether users of Apple's iPhone X, iPhone 11 or iPhone 12 realize it or not, each time they gain access to their cellular device using "Face ID," they are using a form of FRT, as their "faceprint [is] mapped by the phone's front-facing camera."[61] Social media platforms, such as Facebook, utilize facial recognition software to "identify human faces in pictures uploaded to the [app] with up to 97% accuracy."[62]

FRT simultaneously serves the public welfare and raises serious privacy concerns.[63] For example, FRT is capable of tracking an individual's movements for purposes of long-term surveillance of their daily life.[64] But, it is also capable of identifying a missing, lost and wandering child walking on the street.[65] FRT may be used to identify every attendee at a political rally without their consent.[66] But, it may also allow law enforcement officials to identify a suspected terrorist, who is present at that rally, and intends to harm those in

[54] Bonsor & Johnson, *supra* note 19.
[55] *Id.*
[56] *Id.*
[57] James Vincent, *Facial Recognition and AI Could Be Used to Identify Rare Genetic Disorders*, VERGE (Jan. 15, 2019, 2:11 PM), http://www.theverge.com/2019/1/15/18183779/facial-recognition-ai-algorithms-detect-rare-genetic-disorder-fdna.
[58] *See* Alfred Ng, *With Facial Recognition, Shoplifting May Get You Banned in Places You've Never Been*, CNET (Mar. 20, 2019, 8:11 AM), http://www.cnet.com/news/with-facial-recognition-shoplifting-may-get-you-banned-in-places-youve-never-been/.
[59] *Id.*
[60] *Id.*
[61] Calvello, *supra* note 42; Brandon Vigliarolo, *Apple's Face ID: Cheat* sheet, TECHREPUBLIC (June 11, 2020, 7:43 AM), http://www.techrepublic.com/article/apples-face-id-everything-iphone-x-users-need-to-know/.
[62] *Id.*
[63] See Smith, *supra* note 2.
[64] *Id.*
[65] *Id.*
[66] *Id.*

attendance.[67] FRT is a double-edged sword and these conflicting uses illustrate the need "for thoughtful government regulation and for the development of norms around acceptable uses."[68]

b. The Fallibility of Facial Recognition Technology

Though FRT companies are steadily improving their facial recognition systems to overcome certain technical challenges, the technology remains far from perfect.[69] Unlike fingerprints or DNA, faces inevitably change over time.[70] For example, a subject's face can change over time due to fluctuation in body weight, change in hairstyle, growth or removal of facial hair, and the effects of aging.[71] Other factors that may interfere with an algorithm's ability to detect a subject's faceprint include the wearing of eyeglasses or sunglasses, and hair that obscures distinguishing nodal points.[72]

A more recent challenge to FRT is the growing popularity of facial plastic surgery, which can dramatically change the relationship between certain nodal points.[73] One study found "that appearance, feature-, and texture-based [facial recognition] algorithms are unable to effectively mitigate the variations caused by plastic surgery procedures."[74] Similarly, the popularity of "beautification apps," or mobile phone applications that allow users to retouch and reshape the face in an image, pose a challenge to FRT.[75] Finally, the greater the number of faces stored in a facial recognition system's database, the less effective the system, because more faces look similar to one another.[76] Although manufacturers of FRT are constantly improving their products to address these limitations, erroneous facial recognition results can have disturbing effects, the most devasting of which is putting innocent subjects behind bars.[77]

---

[67] *Id.*
[68] *Id.*
[69] *See* Siuru, *supra* note 45.
[70] *Id.*
[71] *Id.*
[72] Bonsor & Johnson, *supra* note 19.
[73] B.S. Sruthy & M. Jayasree, *Recognizing Surgically Altered Face Images and 3D Facial Expression Recognition*, 24 PROCEDIA TECH. 1300, 1301 (2016).
[74] Richa Singh et al., *Plastic Surgery: A New Dimension to Face Recognition*, 5:3 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 441-48, (2010).
[75] Christian Rathgeb et al., *Impact and Detection of Facial Beautification in Face Recognition: An Overview*, 7 IEEE ACCESS, 152667 (2019).
[76] Siuru, *supra* note 45.
[77] *See id.*

c. Criticisms of Facial Recognition Technology: Why People are Begging for Policy Development

Erroneous FRT evidence can produce wrongful convictions, enhance racial discrimination, and may be used by the police to punish individuals for political expression.[78] Researchers from MIT and Stanford University analyzed the accuracy rate of facial recognition software in identifying skin-type and gender.[79] The researchers compiled a database with over 1200 images, in which women and dark-skin individuals were better-represented than individuals who fell into neither category.[80] Each image was assigned a score–I, II, III, IV, V, or VI–based on the Fitzpatrick skin tone scale.[81] The researchers found that such systems had an error rate of no more than 0.8% when identifying white males, but the error rate when identifying darker-skinned women, or those assigned scores of IV, V, or VI, was 20.8%, 34.5%, and 34.7%, respectively.[82] A test conducted by the American Civil Liberties Union (ACLU) revealed that Amazon's facial recognition software "incorrectly matched 28 members of Congress, identifying them as other people who have been arrested for a crime."[83] Almost 40% of the incorrect matches were of people of color, even though they make up only 20% of Congress.[84] These studies demonstrate why adversaries of FRT fear that it may "exacerbate the disproportionate surveillance of minority communities, particularly people of color."[85]

A further criticism raised by opponents of FRT is that it endangers Americans' right to anonymity when participating in certain activities protected by the First Amendment, such as protests and political rallies.[86] An investigation conducted by the ACLU revealed that during the protests that erupted after Freddy Gray's death, the Baltimore Police Department used FRT in conjunction with a social media monitoring service to arrest protesters in the

[78] *See* Nicole Martin, *The Major Concerns Around Facial Recognition Technology*, FORBES (Sept. 25, 2019, 3:15 PM), http://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/#47fd01914fe3; PANDA SECURITY, *supra* note 24.
[79] Larry Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems*, MIT NEWS (Feb. 11, 2018), http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.
[80] *Id.*
[81] *Id.*
[82] *Id.*
[83] Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU (July 26, 2018, 8:00 AM), http://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.
[84] *Id.*
[85] The Constitution Project's Task Force on Facial Recognition Surveillance & Jake Laperruque, *Facing the Future of Surveillance*, POGO (Mar. 4, 2019), http://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/.
[86] *Id.*

crowd who were identified as having outstanding warrants.[87] The ease with which the government may remove the anonymity of a group's members, without consent, could chill First Amendment protected activities.[88]

A 2019 study conducted by Pew Research Center revealed "that a majority of Americans (56%) trust law enforcement agencies to use [FRT] responsibly."[89] However, several groups– particularly African Americans, younger Americans, and Democrats–expressed low levels of such trust in law enforcement agencies.[90] The same study revealed that between a third to over a half of Americans find it unacceptable for FRT to be used by landlords to track who enters or leaves their apartment buildings, or by advertising companies to gauge how people respond to public advertisement, or by employers to monitor their employees' attendance.[91] As this study shows, the fear that other organizations, aside from law enforcement agencies, will misuse this data, is very real.[92]

IV. How Will the Courts Interpret Privacy Interests in Light of Facial Recognition Technology?

The U.S. Supreme Court has yet to hear a case regarding the use of FRT and it is unclear how the Supreme Court will apply the Fourth Amendment and the ruling in *Carpenter v. United States* to a case challenging FRT.[93] The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[94] The majority opinion in *Carpenter*, written by Chief Justice Roberts, discusses the evolution of Fourth Amendment jurisprudence, beginning with the early cases in which courts took an exclusively property-based approach and leading to the modern understanding that "the Fourth Amendment "protects people, not places."[95]

[87] *Id.*
[88] *Id.*
[89] Aaron Smith, *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, PEW RES. CTR. (Sept. 5, 2019) http://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/.
[90] *Id.*
[91] *Id.*
[92] *See id.*
[93] *See* Garvie et al., *supra* note 15.
[94] U.S. Const. amend. IV.
[95] *Carpenter v. United States*, 138 S. Ct. 2206, 2237 (2018) (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)).

Roberts emphasizes that an individual does not relinquish all constitutional protection by stepping out in public.[96]

Although the Supreme Court has not directly ruled upon the constitutionality of law enforcement's use of FRT,[97] the Supreme Court's ruling in *Carpenter* may offer some guidance as to how the Court will handle other forms of surveillance technology.[98] The technology at issue in *Carpenter* is cell-site location information (CSLI).[99] CSLI refers to a time-stamped record that is created each time a cell phone connects to a nearby cell site.[100] For example, CSLI is created each time a phone is turned on, sends or receives a text message, or receives a phone call.[101] Most smart phones connect to a cell site several times a minute whenever their signal is on, regardless of whether the phone is being used.[102] The more cell sites within a geographic area, the more precise the CSLI, and the easier it is to pin down a cell phone user's location.[103]

Before *Carpenter*, under the Stored Communications Act, law enforcement could order wireless carriers to produce the CLSI associated with the suspect of a crime, by merely showing "that the cell-site evidence might be pertinent to an ongoing investigation."[104] This standard is significantly lower than the probable cause required for a typical warrant.[105] The facts of *Carpenter* provide that the FBI obtained 12,898 location points cataloging a robbery suspect's movements over 127 days.[106] The suspect at issue moved to suppress the data, arguing that the Government's acquisition of such data was unconstitutional, because it was a search within the meaning of the Fourth Amendment, which requires a warrant supported by probable cause.[107]

---

[96] *Id.* at 2217 (quoting *Katz v. United States*, 389 U.S. 347, 351-352 (1967)).
[97] *Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties*, Before the H. Comm. on Oversight and Reform, 116th Cong. (2019), https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=109521.
[98] Robyn Greene & Michael Pizzi, *The Supreme Court Made a Sweeping Decision About Privacy Rights*, NEW AM. (July 26, 2018), http://www.newamerica.org/weekly/edition-213/supreme-court-made-sweeping-decision-about-privacy-rights/.
[99] *Carpenter*, 138 S. Ct. at 2211.
[100] *Id.*
[101] Sabrina McCubbin, *Summary: The Supreme Court Rules in Carpenter v. United States*, LAWFARE (June 22, 2018, 2:05 PM), http://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states.
[102] *Carpenter*, 138 S. Ct. at 2211.
[103] *See id.*; McCubbin, *supra* note 102.
[104] *Carpenter*, 138 S. Ct. at 2221.
[105] *Id.*
[106] *Id.* at 2212.
[107] *Id.* at 2213.

In *Carpenter*, the Supreme Court held that an individual maintains a legitimate expectation of privacy, for Fourth Amendment purposes, "in the record of his physical movements as captured through CSLI."[108] The ruling in *Carpenter* requires that police obtain a warrant supported by probable cause to access CSLI from a wireless carrier, unless a case-specific exception to the warrant requirement applies, such as exigent circumstances.[109] Roberts reasoned that "a cell phone—almost a 'feature of human anatomy'—tracks nearly exactly the movements of its owner," and therefore presents heightened risks to privacy.[110] A person's face is most certainly a feature of human anatomy, and unlike cell phones, a face cannot be powered off or left behind. If the Supreme Court found that police acquisition of cell phone location data from third parties constituted a search, it seems plausible that the Court would find that police acquisition of facial recognition data from third parties would likewise constitute a search.[111]

Supporters of FRT may argue that the acquisition of facial recognition data from third parties is not a violation of privacy because under the third-party doctrine, the government is free to access, without a warrant, information that an individual voluntarily provided to a third party.[112] In *Carpenter*, the Court declined to extend the third-party doctrine to cell site records, on the grounds that in 1979, when the doctrine was established, "few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."[113] The Court also refused to apply the voluntary exposure rationale of the third-party doctrine, reasoning that CSLI is not truly "shared" because "carrying [a cell phone] is indispensable to participation in modern society" and CSLI is generated by virtually every action carried out on a cell phone.[114]

CSLI and FRT are both valuable investigatory tools, but both technologies have the potential to invade the privacy of Americans, and therefore must be regulated. Just as law

[108] *Id.* at 2217.
[109] *Id.* at 2222.
[110] *Id.* at 2218 (citation omitted).
[111] Memorandum from Majority Staff on Hearing on "*Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties*" to be heard before the H. Comm. on Oversight and Reform, 116th Cong. (2019), http://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-20190522-SD002.pdf.
[112] *See Smith v. Maryland*, 442 U.S. 735, 742-44 (1979) (holding that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties;" therefore, the government's acquisition of such information does not constitute a search under the Fourth Amendment).
[113] *Carpenter*, 138 S. Ct. at 2217.
[114] *Id.* at 2220.

enforcement is required to obtain a warrant before collecting cell phone location information, law enforcement should be required to obtain a warrant before using FRT to conduct public surveillance of an individual.

Quoting the Supreme Court's ruling in *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523 (1967), Chief Justice Roberts reminds the reader that the purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[115] Unfortunately, the holding in *Carpenter* is a narrow one.[116] As Chief Justice Roberts explains, the decision does not apply to real-time location tracking, nor does it "call into question conventional surveillance techniques and tools, such as security cameras," or "business records that might incidentally reveal location information."[117] This narrow ruling is unfortunate because it limits the extension of *Carpenter* to other activities that raise privacy concerns, namely the government's ability to obtain video footage from a camera mounted by a third party, such as a retail store.[118] Nevertheless, despite the Court's apprehension, Chief Justice Roberts notes that as technological innovations enhance the government's ability to intrude on constitutionally protected areas, the courts must interpret the Fourth Amendment in a more nuanced, as opposed to mechanical, fashion when deciding what constitutes a search for Fourth Amendment purposes.[119]

Given the rapid pace at which FRT is evolving, the courts, alone, cannot be relied on to address the privacy concerns posed by FRT.[120] Federal, state, and local policymakers must take steps to constrain the use of FRT.[121]

V. Legislation Regulating Facial Recognition Technology: The Enacted, Pending, and Absent

[115] *Id.* at 2213 (quoting *Camara v. Mun. Court of City & Cty. of San Francisco*, 387 U.S. 523, 528 (1967)).
[116] *See id*. at 2221.

[117] *Id.* at 2220.
[118] *See* Shea Denning, *Pole Cameras After Carpenter*, UNC SCH. OF GOVT. (July 31, 2019, 6:05 PM), http://nccriminallaw.sog.unc.edu/pole-cameras-after-carpenter/; *see e.g.*, *United States v. Kay*, No. 17-CR-16, 2018 WL 3995902, *1 (E.D. Wis. Aug. 21, 2018) (holding that the investigators' warrantless use of pole camera footage was not a violation of Fourth Amendment rights).
[119] *See Carpenter*, 138 S. Ct. at 2214.
[120] *See* Greene & Pizzi, *supra* note 99.
[121] *See* Susan Crawford, *Facial Recognition Laws Are (Literally) All Over the Map*, WIRED (Dec. 16, 2019, 8:00 AM), http://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/.

The growing concern surrounding the privacy implications of FRT in certain contexts has driven some cities and states to place limits on its use.[122] For example, "San Francisco and Oakland, California, Brookline, Cambridge, Northampton and Somerville, Massachusetts have all banned the use of [FRT] by city agencies."[123] However, these prohibitions do not speak for all jurisdictions, as law enforcement agencies in several North Texas cities have increased the use of FRT despite the growing trend that recognizes the need for privacy protections from unregulated FRT use.[124] Some cities, like Detroit, fall somewhere in the middle, permitting the use of FRT only in certain circumstances, such as in connection with the investigation of violent crimes.[125] At the state level, California, New Hampshire, and Oregon have banned the use of FRT and other biometric tracking technology in body cameras worn by law enforcement.[126] As of January 17, 2020, ten states introduced bills to regulate, ban, or study FRT.[127] Although several state and local governments have placed restrictions on the use of FRT, there remains an absence of a unified federal law, regulation, or oversight.[128]

With no federal regulations currently in place, commercial and governmental entities are essentially free to use FRT as they please.[129] It is not expected that the federal government will enact any such regulation any time soon, as "Congress has so far been unable to pass even a basic federal online privacy law."[130] However, members of the House Committee on Oversight and Reform have been working since at least the beginning of 2019 to enact legislation that will "pause" the advancement of FRT, to give "Congress and federal

[122] Benjamin Hodges & Kelly Mennemeier, *The Varying Laws Governing Facial Recognition Technology*, IP WATCHDOG (Jan. 28, 2020), http://www.ipwatchdog.com/2020/01/28/varying-laws-governing-facial-recognition-technology/id=118240/.
[123] *Id.*
[124] Brian New, *Facial Recognition Use by North Texas Police Grows Along with Privacy Concerns*, CBS DFW (Feb. 4, 2019, 6:30 PM) http://dfw.cbslocal.com/2019/02/04/facial-recognition-texas-police-grows-privacy-concerns/.
[125] Hodges & Mennemeier, *supra* note 122.
[126] Crawford, *supra* note 121.
[127] Georgetown Law Center on Privacy and Technology (@GeorgetownCPT), TWITTER (Jan. 17, 2020, 11:25 AM), http://twitter.com/GeorgetownCPT/status/1218222879097049088.
[128] Facial Recognition Technology Warrant Act of 2019, S.2878, 116th Cong. (2019).
[129] Memorandum from Majority Staff on Hearing on "Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties" to be heard before the H. Comm. on Oversight and Reform, 116th Cong. (2019).
[130] Crawford, *supra* note 121.

regulators [time to understand] how the technology is being used now and put guardrails in place for its use in the future."[131]

According to Susan Crawford, a professor at Harvard Law School, action at the federal level is unlikely to happen any time soon, and if hundreds of cities across the country enact their own unique restrictions, tech companies will struggle to remain compliant.[132] Crawford speculates that as the patchwork of local laws grows, compliance will become too onerous and push "both companies and [the] government to reach a much-needed, national consensus on the use of biometric data."[133]

When the time comes to create unified restrictions on the use of FRT, lawmakers and the Courts should look to the ruling in *Carpenter* and the Illinois Biometric Information Privacy Act of 2008 (BIPA) for guidance. BIPA provides a framework for regulating the use of FRT in the private sector, and the ruling in *Carpenter* provides a framework for regulating the government's use of FRT. Under BIPA, private entities who wish to collect or store facial recognition data must (1) provide written notice to individuals that the collection will occur; (2) indicate the purpose of the collection; (3) describe the length of time the data is to be collected, stored, and used; and (4) receive informed written consent prior to collecting or sharing the collected data with third parties.[134] Although the BIPA requirements may be too burdensome in the federal context, imposing a general notice and consent requirement will force private entities to collect, use, and store facial recognition data responsibly.

Understanding that the BIPA requirements may curtail certain governmental applications of FRT that are beneficial to society, lawmakers should look to *Carpenter* when determining how to regulate the government's use of FRT. The proposed legislation should require government entities to obtain a probable cause warrant prior to using FRT for ongoing surveillance of an individual or for some other authorized investigative use. In addition, the warrant should specify the date on which the court order expires. These proposed guidelines not only protect fundamental Fourth Amendment privacy rights but also the government's right to use FRT for public safety reasons.

---

[131] Aaron Boyd, *Lawmakers Working on Legislation to 'Pause' Use of Facial Recognition Technology*, NEXTGOV (Jan. 15, 2020), http://www.nextgov.com/emerging-tech/2020/01/lawmakers-working-legislation-pause-use-facial-recognition-technology/162470/.
[132] Crawford, *supra* note 121.
[133] *Id.*
[134] 740 ILL. COMP. STAT. (2008).

VI. Is America Unknowingly Following in China's Footsteps?

Unregulated use of FRT seems incompatible with American values, yet many cities and states have not created any serious restrictions on facial recognition systems.[135] As FRT creeps into more and more law enforcement agencies with little notice or oversight, America grows closer to possessing a pervasive surveillance system similar to that deployed in China.[136] In China, cameras equipped with FRT are ubiquitous.[137] A report, released by industry researcher IHS Markit, states that by the end of 2021, over one billion cameras around the world will be used for surveillance, and over half will be located in China.[138] Surveillance cameras in China are able to track and quickly identify individuals over an enormous geographic area.[139] The use of FRT has become so extensive in China that the "[r]estrooms at some tourist attractions even require a facial scan in order to receive toilet paper to curb over-consumption."[140] Moreover, one Chinese company is reported to have developed a system for identifying individuals wearing a surgical mask, which includes most Chinese citizens in the wake of COVID-19, the disease caused by the novel coronavirus.[141] From an outsider's perspective, China appears to have become a dystopia, constantly monitoring its citizens' moral behavior in a fashion strikingly similar to that seen in George Orwell's *Nineteen Eighty-Four*.[142] However, the focused attention on China's use of FRT may be masking the pervasive use of FRT in the United States.[143] According to IHS Markit analyst, Oliver Philippou, "the US [is] nearly on par with China

[135] *See* Crawford, *supra* note 121.
[136] *See* The Constitution Project's Task Force on Facial Recognition Surveillance & Laperruque, *supra* note 86.
[137] Charlie Campbell, *'The Entire System Is Designed to Suppress Us.' What the Chinese Surveillance State Means for the Rest of the World*, TIME (Nov. 21, 2019), http://time.com/5735411/china-surveillance-privacy-issues/.
[138] Liza Lin & Newley Purnell, *A World With a Billion Cameras Watching You Is Just Around the Corner*, WALL ST. J. (Dec. 6, 2019, 1:00 AM), http://www.wsj.com/articles/a-billion-surveillance-cameras-forecast-to-be-watching-within-two-years-11575565402?mod=hp_listb_pos1.
[139] The Constitution Project's Task Force on Facial Recognition Surveillance & Laperruque, *supra* note 86.
[140] Kelly Wang, *China facial-recognition case puts Big Brother on trial*, TECH XPLORE (Jan. 8, 2020), http://techxplore.com/news/2020-01-china-facial-recognition-case-big-brother.html.
[141] Martin Pollard, *Even Mask-wearers Can be ID'd, China Facial Recognition Firm Says*, REUTERS (Mar. 9, 2020, 3:40 AM), http://www.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUSKBN20W0WL.
[142] Ryan Smith, *Destination Dystopia: Facial Recognition Payments Already a Thing in China*, CCN (June 30, 2019, 1:35 PM), http://www.ccn.com/destination-dystopia-facial-recognition-payments-Already-a-thing-in-china/.
[143] *See* Thomas Ricker, *The US, Like China, Has About One Surveillance Camera for Every Four People, Says Report*, VERGE (Dec. 9, 2019, 10:48 AM), http://www.theverge.com/2019/12/9/21002515/surveillance-cameras-globally-us-china-amount-citizens.

in terms of camera penetration, [and] future debate over mass surveillance is likely to concern America as much as China."[144]

VII. Conclusion

The characterization of FRT as a double-edged sword explains in part why the technology remains largely unregulated. Lawmakers and the courts face the difficult task of balancing Fourth Amendment privacy rights with the government's need to detect and prevent criminal activity. Despite the difficulties that lie ahead, lawmakers and the courts must act soon, because although *Carpenter* imposed a warrant requirement for cell phone tracking, no such limitation exists for FRT.

Since the rules for electronic location tracking established by the Court in *Carpenter* do not apply to FRT, law enforcement will opt to use FRT, instead of CSLI, to bypass the warrant requirement.[145] Accordingly, the only thing seriously limiting the American government's location tracking from reaching the level of that employed by China is the "relatively lower number of cameras continuously recording the public."[146] Therefore, it is critical to recognize that newer technologies, like FRT, provide the same capacity for monitoring location that cellphones do, and that legal standards restricting electronic location tracking should be preserved.[147]

Moreover, walking in public spaces is an indispensable part of modern life; therefore, in order to participate in normal daily life, people are left with no choice but to risk subjecting themselves to the "inescapable and automatic" collection of facial recognition data.[148] For that reason, the holding in *Carpenter* should be extended to the use of FRT for the purpose of large-scale surveillance. Unfortunately, until such a case is decided, or federal legislation is passed, the virtually unrestricted use of FRT will persist.

[144] *Id.*

[145] The Constitution Project's Task Force on Facial Recognition Surveillance & Laperruque, *supra* note 86.
[146] *Id.*
[147] *Id.*
[148] *Carpenter*, 138 S. Ct. at 2223.