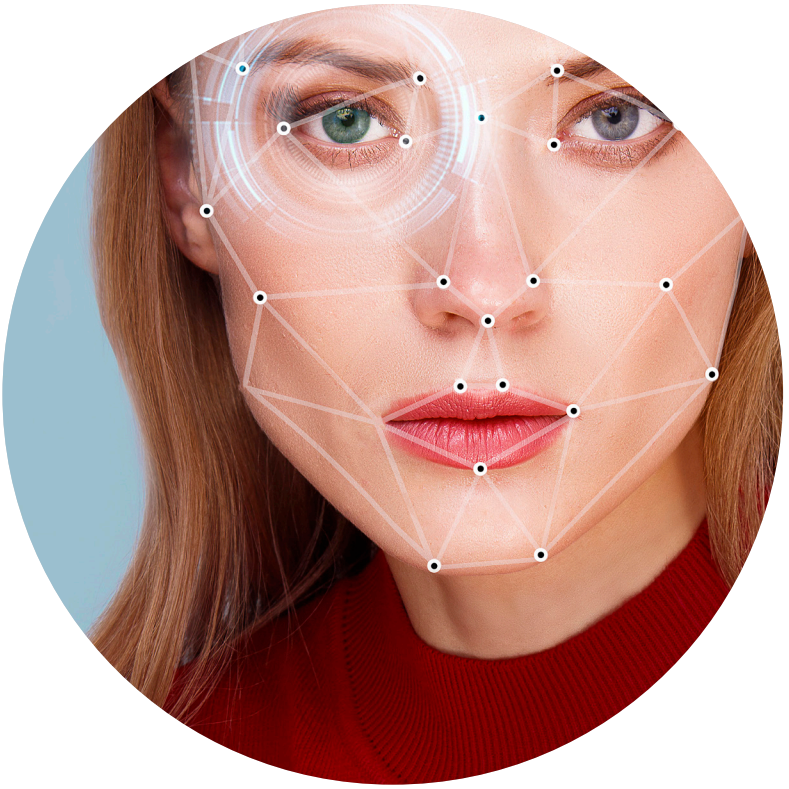

Facial Recognition Technology

Where Will It Take Us?

by KRISTINE HAMANN AND RACHEL SMITH

Technology is expanding, evolving, and improving at an explosive rate. Society, including law enforcement, is struggling to keep pace with these seemingly daily developments. This paper addresses facial recognition technology used by law enforcement to enhance surveillance capabilities and the associated legal issues it raises. Facial recognition technology provides a sophisticated surveillance technique that can be more accurate than the human eye. The use of this technology to enhance public safety will only increase and improve. Nevertheless, the criminal justice system must grapple with the many novel legal issues it poses. The legal landscape is far from settled. This article is not intended to be an in-depth legal analysis; rather, the goal is to provide an overview of the technology and an explanation of the evolving legal issues that law enforcement and the legal community may confront.

HowIt Works

Generally, facial recognition technology (FRT) creates a "template" of the target's facial image and compares the template to photographs of preexisting images of a face(s) (known). The known photographs are found in a variety of places, including driver's license databases, government identification records, mugshots, or social media accounts, such as Facebook.

Facial recognition technology uses a software application to create a template by analyzing images of human faces in order to identify or verify a person's identity. (Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, How Stuff Works, https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm (last visited Nov. 30, 2018).) FRT has the potential to be a useful tool in crime fighting by identifying criminals who are captured on surveillance footage, locating wanted fugitives in a crowd, or spotting terrorists as they enter the country. (*Id.*) FRT also can be used in other ways, such as to identify problem gamblers in casinos, greet hotel guests, connect people on matchmaking websites, help take attendance in schools, and identify drinkers who are underage (*7 Surprising Ways Facial Recognition Is Used*, CBS News, https://www.cbsnews.com/pictures/7-surprising-ways-facial-recognition-is-used (last visited Apr. 14, 2018).) FRT has effectively identified individuals in controlled environments with relatively small

KRISTINE HAMANN is the founder and executive director of Prosecutors' Center for Excellence. She can be reached at khamann@pceinc.org.

RACHEL SMITH is a senior attorney for the Prosecutors' Center for Excellence and a special prosecutor for the Circuit Attorney of St. Louis. She can be reached at rsmith@pceinc.org.

populations, for example, where an individual's face is matched to a preexisting image on an internal file. (State v. Alvarez, No. A-5587-13T2, 2015 N.J. Super. LEXIS 1024, at *2 (N.J. Super. Ct. App. Div. May 4, 2015); Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues,* Ctr. for Catastrophe Preparedness & Response, NYU (July 22, 2009).) On the other hand, FRT has not worked as well in more complex situations, such as finding an unknown face on a crowded street. (*Id.* at 3.) Nevertheless, while not yet being used as the sole basis for an arrest, FRT does aid police investigations and can be used to develop leads. (Alexander J. Martin & Tom Cheshire, *Legal Questions Surround Use of Police Facial Recognition Tech,* Sky News (Aug. 23, 2017), https://news.sky.com/story/legal-questions-surround-police-use-of-facial-recognition-tech-11001595.)

Measuring the Face

A template for FRT is created by use of measurements. The face is measured through specific characteristics, such as the distance between the eyes, the width of the nose, and the length of the jaw line. (Bonsor & Johnson, *supra*.) The facial landmarks, known as nodal points (*id.*), are measured and translated into a template with a unique code. New technologies are emerging that are improving recognition rates, such as 3-D facial recognition and biometric facial recognition that uses the uniqueness of skin texture for more accurate results. (*Id.*) Once the face in question is analyzed, the software will compare the template of the target face with known images in a database in order to find a possible match. (*Id.*; Jenni Bergal, *States Use Facial Recognition Technology to Address License Fraud*, Governing Mag. (July 15, 2015).)

Social Media and Technology Companies

Social media and technology companies have developed their own facial recognition software to use for "photo-tagging," a system where a photograph is automatically associated with a known person. For example, Facebook and Shutterfly rely on FRT to identify individuals in uploaded photographs. (*In re* Facebook Biometric Info. Privacy Litig., No. 15-cv-03747-JD, 2016 WL 2593853, at *1 (N.D. Cal. May 5, 2016); Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015).) Their facial recognition algorithm performs well as it is assisted and improved by its own users who tag themselves and fellow users in photos, many of which are taken at different angles and in different lighting. (Naomi Lachance, *Facebook's Facial Recognition Software Is Different from the FBI's. Here's Why,* NPR (May 18, 2016); Yaniv Taigman et al., *DeepFace: Closing the Gap to Human-Level Performance in Face Verification*, Facebook AI Research (June 24, 2014).)

Technological Limitations

FRT is an evolving scientific and diagnostic tool with enormous potential for law enforcement, but it does have limitations. When these images meet certain professional scientific standards, the accuracy rate when comparing each to one another is high. (*See* Introna & Nissenbaum, *supra*, at 3.) However, the accuracy of FRT decreases when there is no standardized photo for comparison or when the comparison comes from a photo from an uncontrolled environment. (*Id.*) Additionally, FRT works best when the picture is head-on and has no movement. (Lachance, *supra*. *See* David Nicklaus, *Cops' Start-Up Uses Facial Recognition to Improve Security*, St. Louis Post-Dispatch (Mar. 17, 2017).) Because faces change over time, unlike fingerprints or DNA (Richard Raysman & Peter Brown, *How Has Facial Recognition Impacted the Law?*, N.Y.L.J. (Feb. 9, 2016)), software can trigger incorrect results by changes in hairstyle, facial hair, body weight, and the effects of aging. (*Id.*) There is also some research indicating that FRT algorithms may not be as accurate in reading the faces of certain demographics, in particular African Americans. (Clare Garvie & Jonathan Frankel, *Facial-Recognition Software Might Have a Racial Bias Problem*, The Atl. (Apr. 7, 2016).)

Investigative Uses

General Surveillance

FRT has been used for general surveillance, yet, so far its results have been mixed. For example, FRT was used at the 2001 Super Bowl in Tampa, Florida, to screen for potential criminals and terrorists from the event. (Bonsor & Johnson, *supra*; Raysman & Brown, *supra*.) Law enforcement was able to identify 19 people with minor criminal records, although it was later admitted that the software only flagged petty criminals and resulted in some false positives. (*Id.*) More recently, facial recognition was used by Baltimore police to monitor protesters during the unrest and rioting after the death of Freddie Gray, leading to the apprehension and arrest of protestors that had outstanding warrants. (Benjamin Powers, *Eyes over Baltimore: How Police Use Military Technology to Secretly Track You*, Rolling Stone Mag. (Jan. 6, 2017). *See also* Kevin Rector & Alison Knezevich, *Maryland's Use of Facial Recognition Software Questioned by*

Researchers, Civil Liberties Advocates, Balt. Sun (Oct. 18, 2016 12:01 AM).)

Targeted Photo Comparisons

Unlike the challenges with using FRT for general surveillance, FRT has been used effectively to identify thousands of suspects relating to identification fraud, with particular success in cases of driver's license fraud. (Bergal, *supra*.) For example, New York has identified over 10,000 people with more than one driver's license with the help of FRT. (*Id.*) Similarly, New Jersey Department of Motor Vehicle officials have referred about 2,500 fraud cases to law enforcement since 2011. (*Id.*) Additionally, airports are using FRT to assist airlines by having passengers board planes based on photographic images they take instead of boarding passes. These photos are compared to previously stored photographs from passports and visas on file with the U.S. Customs and Border Patrol. (See Adam Vaccaro, *At Logan, Your Face Could Be Your Next Boarding Pass,* Bos. Globe (May 31, 2017).)

Active Criminal Case Investigations

The software also has been useful in investigations—not for conclusive identification of an individual, but in conjunction with other evidence. FRT has contributed to establishing probable cause for the arrest of suspected activity of assailants in videos of fights posted on YouTube (*In re* K.M., No. 2721 EDA 2014, 2015 WL 7354644, at *1 (Penn. Sup. Ct. Nov. 20, 2015)), for passport fraud (United States v. Roberts-Rahim, No. 15-CR-243 (DLI), 2015 WL 6438674, at *3 (E.D.N.Y. Oct. 22, 2015)), and in identity theft cases (United States v. Green, No. 08-44, 2011 WL 1877299, at *2 (E.D. Penn. May 16, 2011)). Facial recognition software also was used in an attempt to find the suspects of the Boston Marathon Bombings in 2013, though the use of the software was ultimately unhelpful, due in part to the uncontrolled environment in which the surveillance images were taken. (Brian Ross, *Boston Bombing Day 3: Dead-End Rumors Run Wild and a $1B System Fails*, ABC News (Apr. 20, 2016); Sean Gallagher, *Why Facial Recognition Tech Failed in the Boston Bombing Manhunt*, arsTechnica (May 7, 2013).) Recently, the NYPD arrested an individual related to a shooting after taking a surveillance image from a nightclub of the shooter and creating a full 3-D image of him, then running it through a facial recognition software program that revealed 200 likely matches. (Greg B. Smith, *Behind the Smoking Guns: Inside the NYPD's 21st Century Arsenal*, N.Y. Daily News (Aug. 20, 2017).) Officers then compared the images looking for similar physical characteristics between them, which enabled officers to narrow it down to a single image that was utilized in a photo array that was then shown to witnesses. (*Id.*)

Trial Evidence

With increasing reliability and use of FRT, at some point soon, prosecutors will seek to introduce the technology into evidence in court, either to establish probable cause or as evidence of an identification. At that time, the scientific reliability of FRT algorithms may have to be established by prosecutors under either the *Frye* or *Daubert* standard in court before the evidence is ultimately accepted. (See Daubert v. Merrell Dow Pharms., 509 U.S. 579, 580 (1993).)

Future Use

Progress and improvements in facial recognition are made daily and increased accuracy is foreseeable. (See Smith, *supra*.) Ultimately, it is expected that law enforcement will seek to use FRT for real-time analysis of faces and immediate identification. For example, it soon may be possible for an officer's body-worn camera to use FRT to identify a person he or she observes on the street. (See Barak Ariel, *Technology in Policing: The Case for Body-Worn Cameras and Digital Evidence,* PoliceChief; Ava Kofman, *Real-Time Face Recognition Threatens to Turn Cops' Body Cameras into Surveillance Machines*, The Intercept (Mar. 22, 2017).). Also, state and local governments are investing tremendous resources and increasingly relying on biometric and pattern recognition technologies to help thwart domestic terrorism and other crime, representing a shift in how such investigations are conducted. (Introna & Nissenbaum, *supra*, at 47.)

The federal government has invested approximately $1 billion in the FBI's Next Generation Identification system (NGI) database. (Jose Pagliery, *FBI Lauches a Face Recognition System*, CNNtech (Sept. 16, 2014).) A component of the database, the Interstate Photo System, incorporates facial recognition and search capabilities into a photo database, consisting of photographs of different sources, including both criminal mugshots and noncriminal sources, such as employment records and background check databases. (Christopher De Lillo, *Open Face: Striking the Balance Between Privacy and Security with the FBI's Next Generation Identification System*, 41 J. Legis. 264, 265 (2014–15).) However, when it released NGI, the FBI issued a caveat that the system was to be used for investigatory purposes only, and it could not serve as the sole basis for an arrest. (See Pagliery, *supra*.) Nevertheless, as the

technology improves, FRT's role in law enforcement investigations will undoubtedly continue to grow.

Legal Issues

Fourth Amendment Concerns Generally

The Fourth Amendment prohibits an unlawful search of a place where a person has a reasonable expectation of privacy. In *Katz v. United States*, the Supreme Court announced a two-part test to determine whether a person has a reasonable expectation of privacy, which assesses (1) whether the person exhibited an actual, subjective expectation of privacy and (2) whether that expectation is one that society recognizes as reasonable. (389 U.S. 347 (1967).) The *Katz* test provides a framework for analyzing Fourth Amendment issues.

On June 22, 2018, the US Supreme Court decided *Carpenter v. United States*. (138 S. Ct. 2206 (2018).) In *Carpenter*, the Court ruled on whether a person's expectation of privacy covered the records of historical cell phone data (historical CSLI), which could reveal the person's physical location or movements. Relying on *Katz*, *Carpenter* held that a person's Fourth Amendment rights were violated when the government received historical CSLI from cell phone companies without first obtaining a search warrant. (*Id.*)

Before the *Carpenter* opinion, government agencies could obtain historical cell phone location records with only a court order by explaining to a judge that the information was necessary to an investigation and that the information was in the possession of a third party. However, *Carpenter* ruled that the government must be put to a higher standard and must obtain a judicial search warrant based on sworn facts that probable cause exists to search for the requested items. Thus, law enforcement agencies must now seek a search warrant for individual, personal historical CSLI from phone companies in these specific situations: where no exigent circumstances exist and for date ranges of more than six days.

The *Carpenter* decision was quite narrow, so many questions remain regarding how the Court will address the government's access to other forms of technology that can track an individual's physical location or movement. The Court, however, clearly outlined that as forms of technology develop and enhance the government's ability to encroach on private areas, the courts will be required to work to preserve an individual's privacy from the government intrusion. The Carpenter Court has found that an individual has an expectation of privacy in his or her personal information acquired in large quantities over an extended period of time even when possessed by third parties. This ruling will shape how courts view other forms of technology.

Possible Legal Issues Raised by FRT Specifically

In light of *Katz* and *Carpenter*, FRT that is used on a limited, short-term basis with strictly public systems should not implicate the Fourth Amendment because an individual's face is open to the public. (*Katz*, 389 U.S. at 351–52; United States v. Dionisio, 410 U.S. 1, 14 (1973). *See, e.g.*, De Lillo, *supra*, at 282.) Nevertheless, legal arguments against the warrantless use of FRT can be made on a variety of issues, including that the technology can be used to track an individual's movement over an extended period of time, First Amendment rights may be chilled, and the technology is not available for public use and may implicate the Fourth Amendment.

Data Aggregation Issues

When a suspect has been identified and law enforcement wishes to track the suspect's movement, the use of FRT together with other technologies could also raise a Fourth Amendment issue. (*Carpenter,* 138 S. Ct. at 2212–21. *See* United States v. Jones, 564 U.S. 400 (2012) (Sotomayor, J., concurring).) As discussed, in *Carpenter,* the Court held that the government's warrantless access to an extensive compilation of cell phone user data violated the Fourth Amendment. (138 S. Ct. at 2219.) The Supreme Court declined to address whether short-term, limited, or real-time access had equal concerns under the Fourth Amendment. (*Id.* at 2220.) As for FRT, *Carpenter* suggests that an individual's public movements captured by FRT in an isolated incident do not implicate the Fourth Amendment. However, the same individual's public movements viewed using FRT over an extended timeframe could reveal intimate details about the individual's personal life that may be found to amount to a Fourth Amendment search, even though everything took place in public. (*See, e.g.,* Riley v. California, 134 S. Ct. 2473 (2014); *Jones*, 565 U.S. 400; United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).) Furthermore, compiling data across various databases (whether public or private), throughout multiple locations over a long period, may also implicate the Fourth Amendment.

First Amendment Issues

Critics also have argued that FRT may implicate the First Amendment right to freedom of association and right to privacy. (*The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on Privacy & Tech. 42–44 (Oct. 18, 2016); Rector & Knezevich, *supra.*)

Courts have upheld the right to anonymous speech and association. (NAACP v. Alabama, 357 U.S. 449, 466 (1958); *see also* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995); Talley v. California, 362 U.S. 60, 64 (1960).) These rights protect an individual's ability to associate freely and advocate for minority positions. Without these protections, the use of FRT could have a chilling effect on individuals' behaviors and lead to self-censorship. (*See The Perpetual Line-Up, supra.*) Nevertheless, some courts have considered law enforcement's use of photography at public demonstrations as not violating the First Amendment right to freedom of association. (Laird v. Tatum, 408 U.S. 1 (1972); Phila. Yearly Meeting of Religious Soc'y of Friends v. Tate, 519 F.2d 1335, 1337–38 (3d Cir. 1974); Donohoe v. Duling, 465 F.2d 196, 202 (4th Cir. 1972).) On the other hand, specific, targeted surveillance of a group may cross the line and violate First Amendment association protections. For example, the Second Circuit in *Hassan v. City of New York* determined that the NYPD's targeted use of pervasive video, photographic, and undercover surveillance of Muslim Americans may have caused those individuals "direct, ongoing, and immediate harm," and it may have created a chilling effect. (*See* 804 F.3d 277, 292 (2d Cir. 2015).) Privacy advocates have been particularly critical of the use of FRT in widespread surveillance. The FRT program that was used to monitor the protestors in Baltimore during the Freddie Gray protests were widely criticized for many reasons, including a fear that African Americans were overrepresented in the facial recognition repository. (Stephen Babcock, *Report Raises Troubling Questions About Facial Recognition Technology in Maryland,* Technical.ly (Oct. 19, 2016); Rector & Knezevich, *supra*; *ACLU Letter to Principal Deputy Assistant Attorney General Vanita Gupta*, Leadership Conference (Oct. 18, 2016).)

Use of Technology That Is Not in the General Public Use

Under the *Katz* test, an individual would not have an automatic expectation of privacy with respect to his or her face because it is exposed to the public. (Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting Katz v. United States, 389 U.S. 347, 351–352 (1967)), and United States v. Jones, 565 U.S. 400, 430 (2012)).) In some instances, however, law enforcement's use of FRT that is not yet available for use generally has been deemed a search. The theory is that such technology is "sense-enhancing" and enables law enforcement to do more than ordinary surveillance by a police officer. For example, in *Kyllo v. United States*, the Supreme Court determined that law enforcement's use of thermal imaging technology to obtain information from the inside of a home constituted a search. (533 U.S. 27, 33 (2001).) Even though law enforcement was on a public street at the time, the use of the thermal imaging to obtain information that would otherwise have required law enforcement to enter the home concerned the Court. (*Id.* at 34.) In part because law enforcement in *Kyllo* relied on technology that was not in the general public use, the use of that technology constituted a search. (*Id.*) Though *Kyllo* addressed a technology that could reach into someone's home, which (unlike FRT) is clearly a private area, some scholars have considered the application of *Kyllo* in terms of the limited availability of the technology to FRT. (*See* Nat'l Research Council, Biometric Recognition: Challenges and Opportunities 106–107 (Nat'l Acads. Press, 2010); *Kyllo*, 533 U.S. at 34.) How the courts will interpret privacy interests in light of FRT technology has yet to be seen and will turn on how the technology is used, how much data are sought, how many locations are requested, how long the tracking of the face continues, the exigency of the need, and the actual method used to "capture" the image. (*Dep't of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, Sept. 3, 2015, at 5.)

Conclusion

Technology permeates almost every aspect of our daily lives. For law enforcement, technology comes with many benefits, but also drawbacks and questions. On the positive side, technology has benefited law enforcement in innumerable ways, such as creating reliable evidence, enabling efficient investigations, and helping to accumulate data that allow law enforcement to react quickly and effectively. On the other hand, this technology impacts peoples' privacy in many ways and will trigger many debates on the parameters of privacy.

It will be up to the courts and policymakers to strike the right balance between the need for information and the right to privacy. The debate about the proper balance between privacy and public safety will continue to play out in the courts, as well as in public discourse, for many years to come. Federal, state, and local law enforcement officials will have to be mindful of this debate when developing the rules and regulations that must ensure citizens' privacy protections, while still enabling law enforcement to make use of surveillance's tremendous investigatory and crime-fighting tools. In the meantime, technology will advance and evolve in ways that cannot be anticipated.