Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations

September 24, 2020

Congressional Research Service
https://crsreports.congress.gov
R46541

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46541

September 24, 2020

Kelsey Y. Santamaria
Legislative Attorney

Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations

Facial recognition technology (FRT) is a biometric technology that compares two or more images of faces to determine whether they represent the same individual. Automated FRT is increasingly used by law enforcement to help identify criminal suspects and other persons of interest. Law enforcement may use FRT and associated image databases to compare and match face images taken from a diverse range of sources, including mugshots, driver's licenses, images from police body cameras, and video stills taken from public surveillance footage. Images might also be compared to nongovernment sources, such as those posted on social media.

Currently, there is no overarching federal framework regulating the use of FRT, though a number of federal statutes addressing privacy or data collection and storage may be relevant. Some federal statutes also address or encourage the use of biometrics more specifically, including those calling for the collection of biometric data from foreign travelers entering or exiting the United States. At the state level, most regulation has been focused on the collection and storage of biometric information by private industry. Regulation of law enforcement use of FRT varies among states and localities. While FRT is used by many state and municipal law enforcement agencies, some states and localities have placed restrictions on its use.

The Constitution provides baseline parameters governing FRT's use by government actors. For example, law enforcement's use of FRT, in combination with photographic or video surveillance, may raise Fourth Amendment considerations. The Fourth Amendment protects against unreasonable searches and seizures. Government observation of individuals in public generally is not a "search" under the Fourth Amendment. But the Supreme Court recently indicated in *Carpenter v. United States* that the use of advanced technologies to engage in the prolonged and sustained surveillance of a person's public activities may prompt Fourth Amendment concerns, when such surveillance becomes so pervasive as to provide "an intimate window into a person's life." *Carpenter* suggests some constraints on the ability of the government to engage in continuous and prolonged FRT-enhanced surveillance of a person's public movements, even while more limited use of FRT may be permitted. There also may be Fourth Amendment implications if an FRT system is unreliable and leads to the mistaken arrest of misidentified persons. To date, it seems that few courts have considered probable cause challenges to purportedly unreliable FRT. But other situations involving potentially unreliable sources, such as informants and canine alerts, suggest that the reliability of a specific FRT system may be subject to scrutiny by a reviewing court when assessing the basis for a law enforcement search or arrest. For example, a court may consider whether the system's accuracy was meaningfully affected by factors that could result in misidentification.

Some commentators have suggested that FRT-enhanced public surveillance may impermissibly chill the exercise of free speech and other rights protected by the First Amendment, if, for example, such surveillance enables the government to easily identify those participating in public demonstrations. The Supreme Court has held that government surveillance of speech, without more, may not provide a plaintiff with standing to bring suit alleging a First Amendment violation, meaning that any claim that surveillance infringed a plaintiff's First Amendment rights would need to claim such surveillance was connected to additional government action causing injury.

Equal protection concerns under the Fifth and Fourteenth Amendments might also be implicated. While FRT has the potential to reduce the likelihood that human error leads to mistaken arrest, some contend that algorithmic biases or other factors may lead to the erroneous matching of images of persons belonging to certain racial and ethnic groups. This misidentification, critics contend, may lead law enforcement to wrongfully target those persons for investigation or arrest. Under current case law, a claim of racially selective law enforcement requires a showing that law enforcement action had a discriminatory *effect* and was taken with a discriminatory *purpose*. This framework does not translate easily to automated, algorithmic-based systems like those frequently employed by FRT, which make independent determinations without close human involvement.

Several bills have been introduced in the 116th Congress that address FRT, with most bills focused on constraining its use by law enforcement or private entities.

Contents

Introduction 1
Background on Facial Recognition 4
What Is Facial Recognition Technology? 4
Use by Law Enforcement 5
Current Law 7
Constitutional Considerations 10
The Fourth Amendment 11
General Overview of the Fourth Amendment 11
Surveillance 12
Searches at International Borders 16
Wrongful Arrests and Other Potential Criminal Consequences 18
The First Amendment 21
Equal Protection 23
Proposed Legislation in the 116th Congress 27

Contacts

Author Information 28

Introduction

Automated facial recognition systems compare two or more images of faces to determine whether they represent the same individual.[1] Facial recognition technology (FRT) falls within the larger categories of biometric technology[2] used to varying degrees by the government and private entities to identify persons. FRT is increasingly used by law enforcement to help identify criminal suspects and other persons of interest, often without those persons' knowledge or consent. Law enforcement may use FRT in conjunction with associated image databases to compare and match face images from a diverse range of sources, including mugshots, driver's licenses, images from police body cameras, and video stills taken from public surveillance footage.[3] Images might also be compared to nongovernment sources, such as those posted on social media.[4]

FRT can be a powerful tool for law enforcement in protecting public safety—potentially assisting law enforcement in identifying a criminal suspect, crime victim, or other person of interest.[5] The adoption of FRT can also increase the efficiency of certain government processes. FRT is deployed, for instance, at international borders to verify individuals' claimed identities, reducing the need to manually check paper travel documents.[6] Private industry also implements FRT for

[1] *See generally* U.S. GOV'T. ACCOUNTABILITY OFFICE, FACIAL RECOGNITION TECHNOLOGY: PRIVACY AND ACCURACY ISSUES RELATED TO COMMERCIAL USES, GAO-20-522 4–7 (2020) [hereinafter 2020 GAO REPORT].

[2] Facial geometry (obtained through facial recognition) falls within the larger category of "biometric data," which generally refers to unique personal identifiers such as a person's fingerprints, DNA sample, iris or retinal scan, voice recording, walking gait, and facial geometry. *See* Carra Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & POL'Y 769, 773–74 (2018).

[3] *See* Clare Garvie, Alvaro Bedoya, & Jonathan Frankle, THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA, GEO. LAW CTR. ON PRIVACY & TECH 10–12 (Oct. 18, 2016) [hereinafter THE PERPETUAL LINE-UP], https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf.

[4] *See id.* at 11; *see also* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (last updated Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (discussing state and local law enforcement use of FRT systems); U.S. Dep't of Homeland Sec., PRIVACY IMPACT ASSESSMENT FOR THE ICE USE OF FACIAL RECOGNITION SERVICES, DHS/ICE/PIA-054 6 (May 13, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf (describing Homeland Security Investigations' use of facial recognition services, including images obtained through social media, in its investigation of criminal activity).

[5] *See, e.g.*, THE PERPETUAL LINE-UP, *supra* note 3, at 10–12; Info. Tech. & Innovation Found., *ITIF Technology Explainer: What Is Facial Recognition* (Apr. 8, 2020), https://itif.org/publications/2020/04/08/itif-technology-explainer-what-facial-recognition ("Facial recognition helps police identify victims, suspects, and witnesses to crimes. For example, it has helped authorities find and rescue human trafficking victims, and identified individuals committing crimes ranging from shoplifting and check forgery to armed robbery and murder."); Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html. For example, Maryland's facial recognition system identified the suspect taken into custody in the mass shooting at the *Capital Gazette* newspaper headquarters in Annapolis on June 28, 2018. Justin Jouvenal, *Police Used Facial-Recognition Software to Identity Suspect in Newspaper Shooting*, WASH. POST (June 29, 2018), https://www.washingtonpost.com/local/public-safety/police-used-facial-recognition-software-to-identify-suspect-in-newspaper-shooting/2018/06/29/6dc9d212-7bba-11e8-aeee-4d04c8ac6158_story.html.

[6] U.S. Dep't of Homeland Sec., PRIVACY IMPACT ASSESSMENT FOR TRAVELER VERIFICATION SERVICE, DHS/CBP/PIA-056 (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-january2020_0.pdf ("CBP has successfully operationalized and deployed facial recognition technology, now known as the Traveler Verification Service (TVS), to support comprehensive biometric entry and exit procedures in the air, land, and sea environments."); *see also* U.S. DEP'T OF HOMELAND SEC., TRANSPORTATION SECURITY ADMINISTRATION AND U.S. CUSTOMS AND BORDER PROTECTION: DEPLOYMENT OF BIOMETRIC TECHNOLOGIES 4 (Aug. 30, 2019), https://www.tsa.gov/sites/default/files/biometricsreport.pdf (report required by Section 1919 of the FAA

various purposes, such as providing users convenient access to personal electronic devices and reducing the likelihood of unauthorized access by third parties to protected information.[7]

But some observers have voiced concern about the current and prospective use of FRT, particularly by government entities. While the reliability of FRT has improved over time,[8] the accuracy rates of FRT systems vary, particularly in the identification of persons in certain demographic groups.[9] A 2020 report by the Government Accountability Office (GAO), for instance, observed that the Department of Commerce's National Institute of Technology's evaluation of various FRT systems concluded that they "generally perform[] better on lighter-skin men and worse on darker-skin women, and do[] not perform as well on children and elderly adults."[10] Some contend that certain racial or ethnic groups may be disproportionately affected by FRT misidentification.[11] According to GAO, there appears to be no clear consensus regarding how various factors precisely contribute to these differing accuracy rates, nor consensus on the appropriate method to assess the size and significance of resulting error rates.[12]

Some commentators have raised more generalized criticisms about FRT as a law enforcement tool. Some critics, for example, have expressed concern that FRT—when paired with other surveillance tools and databases that may provide law enforcement with access to many millions of face images—will enable large-scale surveillance of the general populace in a manner that encroaches on personal privacy and civil liberties.[13] Others contend that this concern is overly

Reauthorization Act of 2018, Pub. L. No. 115-254).

[7] *See generally* 2020 GAO REPORT, *supra* note 1, at 11–13; *Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy, Hearing Before the Committee on Oversight and Reform*, 116th Cong. (2020) (statement of Dr. Charles Romine, Director of the National Institute of Standards and Technology) (observing the growing use of FRT by private industry).

[8] *See, e.g.*, 2020 GAO REPORT, *supra* note 1, at 24 (observing that the NIST "found significant improvements in the accuracy of facial recognition technology"); PATRICK GROTHER, MEI NGAN, & KAYEE HANAOKA, FACE RECOGNITION VENDOR TEST (FRVT), PART 2: IDENTIFICATION, NISTIR 8271 DRAFT SUPPLEMENT 4 (Mar. 27, 2020), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf (stating that "massive gains in accuracy have been achieved in the years 2013 to 2018 and these far exceed improvements made in the prior period, 2010 to 2013"); U.S. FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES 3–4 (Oct. 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf (discussing significant improvements made in FRT between 1993 and 2011 that led to its growing use).

[9] *See generally* 2020 GAO REPORT, *supra* note 1, at 24–32 (discussing findings based on interviews with various stakeholders and review of literature and studies produced by NIST, academic institutions, and other entities).

[10] *Id.* at "GAO Highlights."

[11] *See, e.g.*, Op-Ed, *We Now Have Evidence of Facial Recognition's Harm. Time for Lawmakers to Act.*, WASH. POST (July 5, 2020), https://www.washingtonpost.com/opinions/we-now-have-evidence-of-facial-recognitions-harm-time-for-lawmakers-to-act/2020/07/05/e62ee8d0-baf8-11ea-80b9-40ece9a701dc_story.html; Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, ELEC. FRONTIER FOUND. (Feb. 12, 2018), https://www.eff.org/wp/law-enforcement-use-face-recognition.

[12] *See* 2020 GAO REPORT, *supra* note 1, at 32 ("According to stakeholders we spoke with or literature we reviewed from NIST, academics, independent evaluators, and industry representatives, the performance of a facial recognition technology system depends on physical factors and algorithm factors . . . . However, while these groups note factors that may account for performance differences, they have not determined the magnitude of each factor or root causes of performance differences."); *id*. at 33 (discussing some of the reasons for the difficulty in assessing the reasons for and size of discrepancies in FRT accuracy rates, including the developers' reluctance to share proprietary algorithmic code with evaluators and differences in the methodology and purpose of FRT accuracy evaluations). Though beyond the scope of this report, these topics may be explored in other CRS products.

[13] *See, e.g.*, Abdullah Hasan, *2019 Proved We Can Stop Face Recognition Surveillance*, AM. C.L. UNION (Jan. 17, 2020), https://www.aclu.org/news/privacy-technology/2019-was-the-year-we-proved-face-recognition-surveillance-isnt-inevitable/ ("Face recognition offers governments a surveillance capability unlike any other technology in the past .

speculative and, at least at present, does not provide a justification for ending law enforcement's use of a valuable tool to identify criminal suspects and assist victims of crime.[14]

To date, there is no federal framework specifically directed at the development and use of FRT by government and private entities, though some generally applicable laws may apply in certain circumstances.[15] At the state level, police use of FRT is widespread,[16] and regulation is primarily focused on the collection and storage of biometric information by private industry.[17] A few states and municipalities have barred or limited law enforcement from using FRT because of concerns about reliability or potential for misuse.[18] Earlier this year, for example, a three-year moratorium on the use of FRT in police body cameras went into effect in California.[19]

The Constitution may provide some restrictions on government use of FRT. One constitutional consideration concerns the applicability of the Fourth Amendment to law enforcement's use of FRT in criminal investigations.[20] Although the Fourth Amendment's protections against unreasonable searches and seizures do not generally bar surveillance by law enforcement, the Supreme Court has expressed concern over technologically enhanced extended surveillance.[21] FRT-enhanced surveillance also raises novel questions under the First Amendment to the extent that FRT is alleged to have a "chilling effect" on the exercise of free speech.[22] And if a particular FRT system results in the disproportionate misidentification of persons of particular demographic groups, there may be constitutional considerations under equal protection principles in the Fifth and Fourteenth Amendments.[23] While the Constitution provides a baseline for government use of

. . . [FRT] threatens to forever alter our free society, eroding the little remaining semblance of privacy guaranteed under the Fourth Amendment and turning us all into subjects to be monitored, tracked, and scrutinized wherever we go.")

[14] *See, e.g.*, Daniel Castro, *Banning Facial Recognition Will Not Advance Efforts at Police Reform*, INFO. TECH. & INNOVATION FOUND. (June 16, 2020), https://itif.org/publications/2020/06/16/banning-facial-recognition-will-not-advance-efforts-police-reform ("[C]ritics miss the fact that the benefits of law enforcement use of facial recognition are well-proven—they are used today to help solve crimes, identify victims, and find witnesses—and most of the concerns about the technology remain hypothetical. In fact, critics of the technology almost always make a "slippery slope" argument about the potential threat of expanding police surveillance, rather than pointing to specific instances of harm. Banning the technology now would do more harm than good.").

[15] *See infra* "Current Law."

[16] U.S. GOV'T ACCOUNTABILITY OFFICE, FACE RECOGNITION TECHNOLOGY: DOJ AND FBI HAVE TAKEN SOME ACTIONS IN RESPONSE TO GAO RECOMMENDATIONS TO ENSURE PRIVACY AND ACCURACY, BUT ADDITIONAL WORK REMAINS, GAO-19-579T 3–6 (2019) [hereinafter 2019 GAO REPORT].

[17] *See infra* "Current Law."

[18] *See, e.g.*, S.F., CAL. ADMIN. CODE § 19B.2(d) ("[I]t shall be unlawful for any Department to obtain, retain, access, or use: 1) any Face Recognition Technology on City-issued software or a City-issued product or device; or 2) any information obtained from Face Recognition Technology on City-issued software or a City-issued product or device."); Rachel Mentz, *Portland Passes Broadest Facial Recognition Ban in the US*, CNN BUS. (Sept. 9, 2020), https://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html (banning use of FRT "by city departments—including local police—as well as public-facing businesses such as stores, restaurants and hotels"); Matthew Guariglia, *Victory! Boston Bans Government Use of Face Surveillance*, ELEC. FRONTIER FOUND. (June 24, 2020), https://www.eff.org/deeplinks/2020/06/victory-boston-bans-government-use-face-surveillance. Of special note, FRT may be used in San Francisco under exigent circumstances. *See* S.F., CAL. ADMIN. CODE § 19B.7 (permitting law enforcement to use FRT in exigent circumstances).

[19] CAL. PENAL CODE § 832.19.

[20] *See infra* "The Fourth Amendment."

[21] Carpenter v. United States, 138 S. Ct. 2206, 2215 (2018) (citing United States v. Knotts, 460 U.S. 276, 284–85 (1983)).

[22] *See infra* "The First Amendment."

[23] *See infra* "Equal Protection."

FRT, Congress may consider legislation to promote or constrain the technology's use within those parameters.

This report surveys the constitutional implications of the use of FRT by law enforcement. It begins by providing background on FRT and relevant laws. The report then examines some of the constitutional considerations potentially raised by government actors' use of FRT, particularly in the law enforcement context. The report concludes with a brief discussion of legislation introduced in the 116th Congress that specifically addresses FRT.

Background on Facial Recognition

What Is Facial Recognition Technology?

Biometric technology uses automated processes to identify an individual through unique physical characteristics, such a fingerprints, speech patterns, or facial features.[24] FRT can perform several functions, with the most common being (1) *face identification*—the comparison of an unknown person's face against a gallery of known persons—and (2) *face verification*—confirmation of someone's claimed identity.[25] When an image of an unknown person is compared to a database, the technology may determine that an image in the database is sufficiently similar to register as a likely match.[26] One or more likely matches may be identified.[27] If no images are found to be sufficiently similar, the system will return no matches.[28] Face identification can be used for surveillance, to find a person of interest, or for the identification of subjects who are either unable or unwilling to respond.[29] Verification can confirm an individual's claimed identity by comparing a current image with a database of images to determine whether the images match.[30]

Several private companies offer FRT with differing error rates, depending on each company's proprietary techniques for identifying images.[31] Many face recognition algorithms determine which facial features matter most through training.[32] During training, an algorithm is given pairs of face images of the same person.[33] Over time, the algorithm learns to pay more attention to the features that most reliably signaled that the two images contained the same person.[34]

---

[24] JOY BUOLAMWINI, VICENTE ORDÓÑEZ, JAMIE MORGENSTERN, & ERIK LEARNED-MILLER, FACIAL RECOGNITION TECHNOLOGIES: A PRIMER 8 (2020).

[25] 2020 GAO REPORT, *supra* note 1, at 6.

[26] *Id.* at 6–7; *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY, GAO-16-267 5 (2016) [hereinafter 2016 GAO REPORT]. For further discussion on face matching and specific matching (a true match, a true mismatch, a false positive, and a false negative), see BUOLAMWINI ET AL., *supra* note 24, at 12–14.

[27] BUOLAMWINI ET AL., *supra* note 24, at 6.

[28] *Id.*

[29] *Id.*

[30] *Id.* at 6–7. A common use for face verification is access control, such as unlocking a cellphone. *Id.* at 5.

[31] *See generally Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy, Hearing Before the Committee on Oversight and Reform*, 116th Cong. (2020) (statement of Dr. Charles Romine, Director of the National Institute of Standards and Technology) (discussing NIST's review and evaluation of prototype and commercially available facial recognition algorithms).

[32] THE PERPETUAL LINE-UP, *supra* note 3, at 9.

[33] *Id.*

[34] *Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy, Hearing Before the Committee on Oversight and Reform*, 116th Cong. (2020) (statement of Dr. Charles Romine, Director of the National

The successful use of FRT depends on the reliability of the FRT system. Algorithmic factors are determinative of the accuracy of an FRT system, including the algorithm's purpose, its sophistication and sensitivity to false positives, and the data used to "train" the system to compare and match images (e.g., the amount of images used; the demographics of the persons in the images compared; and whether the composition of images in the training data set is representative of the population whose images may be compared using the system once deployed).[35] Physical conditions of use may also affect the accuracy of the FRT. For example, lighting, image quality, and camera motion can affect an FRT system's performance.[36] Performance may also be affected by physical characteristics of the person or persons whose images are captured and compared by an FRT system (e.g., the age of the person in the compared images; changes in facial expression or hairstyle).[37]

Use by Law Enforcement

Law enforcement increasingly uses FRT as a tool to identify persons. When a person is arrested, police may employ FRT and associated databases to compare the arrestee's mugshot with other images to determine the person's identity and criminal history.[38] Law enforcement may also use FRT to help identify persons in other contexts, such as during an encounter in a noncustodial setting.[39] FRT may also be a tool for ongoing criminal investigations. For instance, an FRT system may extract face images from the video feeds of security cameras and compare these images to a "hot list" of suspects.[40] FRT may also be used for many other law enforcement and security purposes, such as to identify international travelers as they enter or exit the United States,[41] or to help ensure that applicants for government-issued identification (e.g., driver's licenses or passports) have not already been issued documents under a pseudonym.[42] Moreover, images taken in the course of any of these law enforcement activities may potentially be added to image databases for future use.[43]

Many state and local law enforcement agencies share data through the FBI's Next Generation Identification system (NGI), a biometric database that includes unique personal identifiers, such as fingerprints and iris scans.[44] NGI allows law enforcement agencies to search a database of

---

Institute of Standards and Technology) ("The process of training a face recognition algorithm (or any machine learning algorithm) involves providing a machine learning algorithm with training data to learn from. The training data shall contain the correct answer, which is known as ground-truth label, or a target. The learning algorithm finds patterns in the training data that map the input data attributes to the target and builds a machine-learning model that captures these patterns. This model can then be used to get predictions on new data for which the target is unknown.").

[35] THE PERPETUAL LINE-UP, *supra* note 3, at 9–15. If a training set skews toward photos of persons with certain attributes, such as persons of a certain race or gender, different FRT systems may be better at identifying members of a group with those common characteristics. 2020 GAO REPORT, *supra* note 1, at 32.

[36] 2020 GAO REPORT, *supra* note 1, at 32; THE PERPETUAL LINE-UP, *supra* note 3, at 47.

[37] 2020 GAO REPORT, *supra* note 1, at 32.

[38] THE PERPETUAL LINE-UP, *supra* note 3, at 11.

[39] *Id.*

[40] *Id.* at 12.

[41] *See, e.g.*, 8 U.S.C. § 1379 (directing the Attorney General or the Secretary of State to consult with Congress to "develop and certify a technology standard, including appropriate biometric identifier standards, that can be used to verify the identity of persons" applying for a visa or seeking admission using a visa).

[42] THE PERPETUAL LINE-UP, *supra* note 3, at 12.

[43] *Id.* at 11.

[44] 2019 GAO REPORT, *supra* note 16, at 2.

criminal photos that accompanied fingerprint submissions.[45] The Interstate Photo System (IPS), a component of NGI, contains photographs searchable by FRT.[46] The FBI also has an internal unit called Facial Analysis, Comparison, and Evaluation (FACE) Services that provides face recognition capabilities to support active FBI investigations.[47] Some states collaborate with the FBI through the sharing of face images (e.g., state-issued driver's license photos, mugshots) with the Next Generation Identification Interstate Photo System (NGI-IPS), accessible for use by both federal authorities and select state or local law enforcement agencies.[48] In addition, the Department of Homeland Security's Office of Biometric Identity Management (OBIM) maintains a biometric database called the Automated Biometric Identification System (IDENT)—holding more than 260 million unique identifiers—that is "used to detect and prevent illegal entry into the United States, grant and administer proper immigration benefits, []vet[] and credential[], facilitat[e] legitimate travel and trade, enforc[e] federal laws, and enabl[e] verification for visa applications to the U.S."[49] DHS also shares biometric information "to support homeland security, defense, and justice missions."[50] The Department of Homeland Security is in a multiyear transition to replace IDENT with the Homeland Advanced Recognition Technology System (HART). That system will likewise store and process biometric data, including face images.[51]

State and local governments may also maintain databases. For example, some states have their own facial recognition systems that compare images to those acquired from mugshots and driver's license photos.[52] Some law enforcement agencies employ facial recognition software that screens databases that contain not only government-issued photos, but also publicly posted photos from sources such as YouTube, Facebook, and Venmo.[53]

As noted above, FRT is also implemented in private industry for a variety of purposes.[54] FRT may be embedded into cellphones and other devices to provide users quick and secure access, thereby protecting personal information and providing the user convenience when accessing their device.[55] Another common use is photo identification on social media to identify and "tag" friends in an image.[56] And some commercial entities use FRT for safety and security purposes,

[45] *Id.*

[46] *Id.* at 3.

[47] *Id.*

[48] *See id.* at 2–5.

[49] U.S. DEP'T OF HOMELAND SEC., *Biometrics*, https://www.dhs.gov/biometrics (last visited Sept. 24, 2020).

[50] *Id.*

[51] *See generally* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1 PIA, DHS/OBIM/PIA-004 (Feb. 24, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf.

[52] *See* THE PERPETUAL LINE-UP, *supra* note 3, at 132 (discussing Maryland's Image Repository System); *see also* Kevin Rector & Alison Knezevich, *Maryland's Use of Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates*, BALT. SUN (Oct. 18, 2016), https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html (same).

[53] *See* Allison Ross, Malena Carollo & Kathryn Varn, *Florida Cops Use This Facial Recognition Tech That Could Be Pulling Your Pics*, TAMPA BAY TIMES (Feb. 11, 2020), https://www.tampabay.com/florida-politics/buzz/2020/02/11/florida-cops-use-this-facial-recognition-tech-that-could-be-pulling-your-pics/; Tom Schuba, *CPD Using Controversial Facial Recognition Program that Scans Billions of Photos from Facebook, Other Sites*, CHI. SUN TIMES (Jan. 29, 2020), https://chicago.suntimes.com/crime/2020/1/29/21080729/clearview-ai-facial-recognition-chicago-police-cpd; Hill, *supra* note 4.

[54] For a discussion on the use of FRT for commercial applications, see 2020 GAO REPORT, *supra* note 1, at 11–13.

[55] *See id.*

[56] *Id.* at 11–12.

including the use of FRT by stores for loss prevention purposes or even by casinos to identify known or suspected gambling cheaters or members of crime networks.[57] At least one FRT developer provides users with access to an associated image database that reportedly contains more than three billion images from millions of websites.[58] Some police departments acquire commercially available FRT for law enforcement purposes.[59] Recently, a few prominent companies have announced that they will limit the sale of FRT to law enforcement.[60]

Current Law

To date, there is no federal framework specifically directed at the use of FRT by government and private entities. But some federal laws of general applicability that address the use of biometrics in particular contexts may be relevant.

A 2020 report by the Government Accountability Office (GAO) noted that the agency could "not identify any federal laws that expressly regulate commercial uses of facial recognition technology in particular."[61] GAO observed, however, that several federal laws that address the collection, use, and storage of personal information may apply to FRT use by private entities.[62] These include

- the Driver's Privacy Protection Act,[63] which limits the use of information contained in state motor vehicle records (including driver's license photographs) for commercial purposes;
- the Health Insurance Portability and Accountability Act,[64] which generally requires covered health entities to adhere to certain data privacy and security requirements in their treatment of certain medical information;
- the Fair Credit Reporting Act,[65] which covers the collection and use of information bearing on a consumer's creditworthiness, and has implementing regulations that treat "unique biometric data" as identifying information;
- the Family Educational Rights and Privacy Act,[66] which establishes privacy protections for student education records (including, by implementing regulation, relevant biometric records);
- the Computer Fraud and Abuse Act,[67] which imposes liability when a person "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer";

[57] *Id.* at 11.

[58] *Id.*

[59] *See id*.; Jay Greene, *Microsoft Won't Sell Police its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM*, WASH. POST (June 11, 2020), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/

[60] *See* Greene, *supra* note 59.

[61] *See* 2020 GAO REPORT, *supra* note 1, at 38 (quoting U.S. GOV'T. ACCOUNTABILITY OFFICE, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY, AND APPLICABLE FEDERAL LAW, GAO-15-621 28 (2015)).

[62] *Id.* at 39.

[63] 18 U.S.C. §§ 2721–25.

[64] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

[65] 15 U.S.C. §§ 1681 *et seq.*; 12 C.F.R. § 1022.3(g)(2).

[66] 20 U.S.C. § 122g; 34 C.F.R. § 99.3.

[67] 18 U.S.C. § 1030(a)(2)(c).

- the Children's Online Privacy Protection Act,[68] which regulates the online collection and use of children's information; and
- Section 5 of the Federal Trade Commission Act,[69] which bars unfair or deceptive practices in or affecting commerce.[70]

Several other federal statutes address the collection and use of biometric data by government entities, which may involve the use of FRT. Most of these statutes involve the screening of arriving or departing international travelers and other border security measures, rather than the use of such technology in the interior of the United States.[71] For example, 8 U.S.C. § 1365b requires the Department of Homeland Security (DHS) to establish an integrated, automated biometric entry and exit system that records the arrival and departure of foreign nationals, collects biometric data of foreign nationals to verify their identity, and authenticates travel documents through the comparison of biometrics.[72] Another statute, 6 U.S.C. § 1118, requires two DHS components—U.S. Customs and Border Protection (CBP) and the Transportation Security Administration—to consult on the deployment of biometric technologies, and further requires DHS to assess the impacts of biometric technology use and submit a report to Congress.[73]

Some generally applicable federal laws may regulate federal agencies' collection and storage of personal data obtained through FRT. Federal agency collection and use of personal information, including face images, is governed mainly by two laws: the Privacy Act of 1974[74] and provisions of the E-Government Act of 2002.[75] The Privacy Act limits agencies' collection, disclosure, and use of personal information maintained in agency records and requires agencies to notify the public when they establish or alter a system of records.[76] The E-Government Act of 2002 requires agencies to conduct "Privacy Impact Assessments" before developing or procuring information technology that collects, maintains, or disseminates personal information.[77] This requirement helps agencies examine the risks and effects on individual privacy when changes are put into place that, for example, alter the way personal information is stored. In addition, agencies must analyze methods to mitigate potential privacy risks.[78] Although these generally applicable

[68] 15 U.S.C. §§ 6501–06.

[69] *Id.* § 45.

[70] 2020 GAO REPORT, *supra* note 1, at 39. For more detailed discussion of these and other federal laws applicable to data privacy, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh.

[71] *See, e.g.*, 8 U.S.C. § 1379 (mandating the Attorney General or the Secretary of State to consult with Congress to "develop and certify a technology standard, including appropriate biometric identifier standards, that can be used to verify the identity of persons" applying for a visa or seeking admission using a visa); *id.* § 1731 (directing the development of an integrated entry and exit data system); *id.* § 1732 (calling for machine-readable, tamper-resistant entry and exit documents).

[72] *Id.* § 1365b.

[73] 6 U.S.C. § 1118(c).

[74] Pub. L. No. 93-579, 88 Stat 1896 (1974); 5 U.S.C. § 552a.

[75] Pub. L. No. 107-347, 116 Stat 2899 (2002); *see also* 2019 GAO REPORT, *supra* note 16, at 6.

[76] 5 U.S.C. § 552a. "Record" is defined in the Privacy Act as "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." *Id.* § 552a(a)(4).

[77] Pub. L. No. 107-347, § 208; 44 U.S.C. § 3501.

[78] *Id.*

regulatory schemes protect an individual's information, neither act directly addresses FRT or the reliability of algorithms employed to compare compiled photographs.

Privacy protections at the state level vary in scope and application, though most states have generally applicable privacy protections.[79] Some states expressly prohibit or limit the use of FRT by government entities.[80]

A handful of states have enacted laws regulating biometric data collection, thereby limiting private industry's collection and use of biometric information.[81] These state laws generally require private entities to notify individuals that their biometric information is being collected, obtain informed consent, and destroy biometric information within a certain time frame.[82] Some states also prohibit private entities from profiting off a consumer's biometric or genetic information and require them to maintain publicly available written policies on biometric data retention and destruction.[83]

Perhaps the most commonly cited state law addressing FRT and related technologies is the Illinois Biometric Information Privacy Act (BIPA).[84] Enacted in 2008, BIPA regulates "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[85] BIPA defines "biometric identifier" to mean "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[86] BIPA provides a private right of action to enforce its provisions.[87] In one notable BIPA case, a plaintiff, who had been required to provide a fingerprint before purchasing items from a vending machine, alleged the company failed to abide by BIPA provisions that required the company to first obtain written consent and publicly disclose the retention schedule and guidelines for permanently destroying the collected biometric identifiers.[88] More recently, other high-profile suits have been filed under BIPA against Macy's

[79] *See generally* E. Casey Lide, *Balancing the Benefits and Privacy Concerns of Municipal Broadband Applications*, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 467, 487 (2008) ("Virtually all states have statutory provisions that impose duties on state government agencies and political subdivisions with regard to the collection, maintenance, accuracy, use, and disclosure of personal information. In some states, the laws are part of an overarching statutory scheme analogous to the federal Privacy Act of 1974 and address the government's use of 'personal information' or 'personal records,' while other states attend to such issues in piecemeal fashion with context-specific laws . . . .").

[80] *See, e.g.*, N.H. REV. STAT. § 263:40-b ("The department [of motor vehicles] is prohibited from using any facial recognition technology in connection with taking or retaining any photograph or digital image for purposes of this chapter."); OR. REV. STAT. § 133.741 (barring "the use of facial recognition or other biometric matching technology to analyze recordings obtained" via body cameras worn by state and local police); WASH. REV. CODE ANN. § 43.003.0011 (effective July 21, 2021) (limiting the use of FRT by state or local governments "to engage in ongoing surveillance, conduct real-time or near real-time identification, or start persistent tracking" except in enumerated circumstances). *See generally* 2019 GAO REPORT, *supra* note 16, at 2–5 (identifying numerous states that limit FRT use).

[81] *See, e.g.*, 740 ILL. COMP. STAT. 14/1; TEX. BUS. & COM. CODE § 503.001; *see also, e.g.*, ALASKA STAT. § 18.12.010 (genetic privacy law limiting genetic testing and access to, storage of, and disclosure of genetic data).

[82] *See, e.g.*, 740 ILL. COMP. STAT. 14/1 § 5(g).

[83] *See, e.g.*, CAL. CIV. CODE §§ 1798.100–1798.199; TEX. BUS. & COM. CODE § 503.001; WASH. REV. CODE §§ 19.375 *et seq.*

[84] 740 ILL. COMP. STAT. 14/1 *et seq.*

[85] *Id.* § 5(g); *see also* Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1203 (Ill. 2019).

[86] 740 ILL. COMP. STAT. 14/10 § 10.

[87] *Id.* § 20.

[88] Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 619 (7th Cir. 2020). Notably, the court has not yet addressed the merits of the claim, as the question before the Seventh Circuit on appeal was whether plaintiff's claimed injury constituted an injury sufficient to confer standing to sue. *See generally id.* The Seventh Circuit held that the collection of the fingerprint without consent was a concrete injury, but that the failure to publicly disclose retention schedule and destruction guidelines was not sufficient to confer standing. *Id.* at 626–27.

department store and Facebook for alleged misuse of biometric data purported to be collected by FRT.[89]

A few other states—Texas,[90] Washington,[91] and California[92]—have adopted biometric privacy laws similar to BIPA.[93]

Constitutional Considerations

The Constitution provides baseline parameters for the government's use of FRT. Some observers have suggested that law enforcement's use of FRT may, in certain circumstances, raise a variety of constitutional considerations. These include the applicability of the Fourth Amendment if FRT is used for law enforcement investigations; possible issues raised under the First Amendment to the extent that FRT is alleged to have a "chilling effect" on free speech; and claims rooted in equal protection principles if a particular FRT uses an algorithm that results in the disproportionate misidentification of persons of particular demographic groups.[94]

Two important considerations inform the scope of this report's discussion of these issues. First, there has been very little federal case law analyzing constitutional issues raised by the government's use of FRT. Accordingly, this report frequently considers how general legal principles might apply, sometimes as a matter of first impression. Second, the significance of these constitutional considerations hinges on the circumstances in which FRT is used and the particular characteristics of that usage. For instance, the legal issues associated with using FRT to monitor the entry and exit of foreign travelers to the United States would be different than those raised in a hypothetical situation where FRT was widely deployed by law enforcement to monitor the daily activities of the general U.S. populace.[95] Additionally, constitutional issues prompted by the alleged misidentification of a criminal suspect through FRT would turn on a number of fact-specific considerations, including not only the reliability of the FRT system employed but also the degree that other evidence informed law enforcement's decisions.

[89] *See* Class Action Complaint, Carmine v. Macy's Retail Holdings, Inc., No. 20-cv-4589 (N.D. Ill. Aug. 5, 2020); Class Action Complaint, Whalen v. Facebook, Inc., No. 20-CIV-03346 (Cal. Superior Court, San Mateo Aug. 10, 2020) (alleging that Facebook obtained biometric data through Instagram in violation of BIPA).

[90] TEX. BUS. & COM. CODE § 503.001.

[91] WASH. REV. CODE §§ 19.375.010–19.375.900.

[92] CAL. CIV. CODE §§ 1798.100–1798.199.

[93] One notable difference between these state provisions are their mechanisms of enforcement. BIPA and the California Consumer Privacy Act provide a private right of action to enforce its provisions. 740 ILL. COMP. STAT. 14/10 § 20; CAL. CIV. CODE § 1798.150(a)(1). But Texas's biometric privacy law and Washington's biometric privacy law do not allow for a private right of action, instead leaving enforcement to their respective attorneys general. TEX. BUS. & COM. CODE § 503.001(d) ("The attorney general may bring an action to recover the civil penalty."); WASH. REV. CODE § 19.375.030 (providing that "[t]his chapter may be enforced solely by the attorney general under the consumer protection act" as codified in Chapter 19.86 in the Washington Code).

[94] FRT CIVIL RIGHTS CONG. HEARING, *See Facial Recognition Technology (I): Its Impact on Our Civil Rights and Liberties: Hearing Before the Committee on Oversight and Reform*, 116th Cong., at 5–6 (2019) [hereinafter FRT CIVIL RIGHTS CONG. HEARING] (statement of Andrew G. Ferguson, Professor of Law, University of the District of Columbia, David A. Clarke School of Law); *id.* at 7–9 (statement of Clare Garvie, Senior Associate, Georgetown University Law Center, Center on Privacy & Technology); *id.* at 9–11 (statement of Neema Singh Guliani, Senior Legislative Counsel, American Civil Liberties Union).

[95] *See infra* "Searches at International Borders."

The Fourth Amendment

General Overview of the Fourth Amendment

The Fourth Amendment protects against unreasonable government searches and seizures.[96] Whether a "search" has occurred within the meaning of the Fourth Amendment depends primarily on whether one has a "reasonable expectation of privacy" in the area searched.[97] Courts often apply a two-part test set forth in Justice Harlan's concurring opinion in *Katz v. United States*: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[98] A search may also occur on a trespass theory—where the government obtains information by physically intruding on a constitutionally protected area, such as a home or even the human body.[99]

The Fourth Amendment also guards against seizures of the person.[100] A person has been seized if, in view of all the circumstances surrounding the incident, that person has an objective reason to believe that he or she is not free to leave.[101] As the Supreme Court has explained, an arrest—"the quintessential 'seizure of a person'"[102]—"requires *either* physical force . . . *or*, where that is absent, *submission* to the assertion of authority."[103]

Once a search or seizure subject to Fourth Amendment scrutiny has occurred, the Fourth Amendment requires a determination of whether the search itself was "reasonable."[104] The Supreme Court has explained that "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"[105] Reasonableness generally means obtaining a warrant supported by probable cause before conducting a search or arrest.[106] To evince probable cause, the government must present facts establishing a reasonable belief that an individual has likely committed a criminal

---

[96] Mapp v. Ohio, 367 U.S. 643, 655 (1961); *see also* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized.").

[97] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (ruling that the bugging of a phone booth violated Katz's Fourth Amendment right to be free from an unreasonable search).

[98] *Id.*

[99] *See* Maryland v. King, 569 U.S. 435, 446 (2013) (collection of DNA sample by buccal swab on inner cheek was a search under the Fourth Amendment).

[100] *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 16 (1968) ("It is quite plain that the Fourth Amendment governs 'seizures' of the person which do not eventuate in a trip to the station house and prosecution for crime—'arrests' in traditional terminology.").

[101] Michigan v. Chesternut, 486 U.S. 567, 573 (1988); *see also* United States v. Mendenhall, 446 U.S. 544, 553–54 ("We adhere to the view that a person is 'seized' only when, by means of physical force or a show of authority, his freedom of movement is restrained.").

[102] California v. Hodari D., 499 U.S. 621, 624 (1991).

[103] *Id.* at 626 (rejecting argument that an arrest "effected by the slightest application of physical force, despite the arrestee's escape" constitutes a seizure). Other forms of detention, such as field detentions for investigation, may also be subject to Fourth Amendment scrutiny. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 4–6 (1968). Courts generally conclude that if an individual is approached by an officer and asked questions without the use of force, the individual is only "seized" if a reasonable person would not feel free to disregard the police and walk away. *Mendenhall*, 446 U.S. at 553–54.

[104] Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995).

[105] Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

[106] *Vernonia Sch. Dist. 47J*, 515 U.S. at 653.

offense.[107] But the Supreme Court has held that, in certain circumstances, the government may conduct a warrantless arrest (such as when an officer has observed a person commit a crime)[108] or a warrantless search (such as when a search is incident to a lawful arrest).[109]

Surveillance

In combination with photographic and video surveillance, law enforcement may use FRT to identify and track criminal suspects.[110] As a general principle, government observation of individuals in public is not a "search" under the Fourth Amendment.[111] In *Katz v. United States*, the Supreme Court explained that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[112] For example, the Court has observed that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[113] In addition, a person generally does not have a Fourth Amendment interest in "physical characteristics . . . constantly exposed to the public," such as the tone of one's voice or his or her facial features.[114] Accordingly, a person's Fourth Amendment rights typically are not infringed if photographed by law enforcement.[115]

---

[107] Maryland v. Pringle, 540 U.S. 366, 371 (2003) ("To determine whether an officer had probable cause for an arrest, the court examines the events leading up to the arrest, and then decides whether these historical facts, viewed from the standpoint of an objectively reasonable police officer, amount to probable cause.").

[108] *See, e.g.*, Atwater v. City of Lago Vista, 532 U.S. 318, 354 (2001).

[109] *See, e.g.*, Mincey v. Arizona, 437 U.S. 385, 390 (1978).

[110] *See supra* "Use by Law Enforcement." *See, e.g.*, 2016 GAO REPORT, *supra* note 26, at 10–14 (discussing federal, state, and local law enforcement use of NGI-IPS); *id.* at 11 ("FBI officials said that NGI-IPS has been used by law enforcement officers conducting investigations of credit card and identity fraud, bank robberies, and violent crimes, among others. For example, in July 2014 the FBI compared a suspect's images captured through video surveillance with NGI-IPS criminal mug shots, which provided an investigative lead that helped identify a bank robbery suspect who was ultimately convicted.").

[111] *See, e.g.*, United States v. Jones, 565 U.S. 400, 412 (2012); Katz v. United States, 389 U.S. 347, 351 (1967).

[112] *Katz*, 389 U.S. at 351.

[113] United States v. Knotts, 460 U.S. 276, 281–82 (1983).

[114] In *United States v. Dionisio*, 410 U.S. 1 (1973), the Supreme Court held that a grand jury directive for a witness to give a voice exemplar did not constitute an infringement of the witness's Fourth Amendment rights. *Dionisio*, 410 U.S. at 14–15. In so ruling, the Court opined:

> In *Katz* . . . we said that the Fourth Amendment provides no protection for what a person knowingly exposes to the public, even in his own home or office . . . . The physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public. Like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world.

Id. at 14 (internal quotations omitted).

[115] *See, e.g.*, United States v. Farias-Gonzalez, 556 F.3d 1181, 1188 (11th Cir. 2009) ("The police can obtain both photographs and fingerprints without conducting a search under the Fourth Amendment."); United States v. Anthony, No. 4:18-CR-00012, 2019 WL 471984, at *3 (W.D. Va. Feb. 5, 2019) (granting a motion by the government to compel the photographing of the criminal defendants' tattoos on parts of the body commonly exposed to the public as evidence of gang affiliation, but emphasizing that the Fourth Amendment barred photographs of other areas not normally exposed to the public); Rowe v. Burton, 884 F. Supp. 1372, 1381 (D. Alaska 1994), ("Courts have consistently refused to accord Fourth Amendment protection to non-testimonial evidence such as photographs of a person, his or her handwriting, and fingerprints."); Application of Rodgers, 359 F. Supp. 576, 578 (E.D.N.Y. 1973) (holding that grand jury witness seeking destruction of compulsory photograph did not raise a cognizable Fourth Amendment claim).

The fact that law enforcement surveillance of public activity involves more than just visual observation, such as through the use of technological tools, does not necessarily alter Fourth Amendment analysis. In a 1983 decision, *United States v. Knotts*, the Court addressed whether tracking by an electronic device that had been installed in a container transported by the suspect 100 miles away to its delivery exceeded Fourth Amendment limitations.[116] The Court held that the tracking was not a search because it revealed only facts that could have been ascertained by visual surveillance.[117] The Court, though, emphasized the "limited use which the government made of the signals from this particular beeper" during a discrete "automotive journey."[118] *Knotts* suggests that the government may use technology to monitor an individual's movements in public to the extent that the same result could be achieved through visual surveillance.[119]

But in recent years, in cases involving new technologies that have made extended and comprehensive surveillance of a person's public activities far easier, the Court has indicated that such surveillance may raise Fourth Amendment concerns.[120] Indeed, the *Knotts* Court cautioned that "different constitutional principles may be applicable" if "twenty-four hours surveillance of any citizen of this country [were] possible."[121] And in later cases the Court has expressed the view that the aggregation of personal data through technological surveillance of public conduct may prompt Fourth Amendment concerns.[122] When detailed information is collected regarding a person's movements for an extended period, the cumulative nature of the information collected may implicate a privacy interest on the part of the individual being tracked.[123]

In the 2012 case of *United States v. Jones*, in an opinion written by Justice Scalia, the Supreme Court held that tracking a person through a GPS device installed on the person's vehicle constituted a "search" under the Fourth Amendment.[124] The Court grounded this decision on the view that the physical installation of the device onto the vehicle constituted a "trespass" on

[116] United States v. Knotts, 460 U.S. 276, 277 (1983).

[117] *Id.* at 281–82 ("When Petschen travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.").

[118] Carpenter v. United States, 138 S. Ct. 2206, 2215 (2018) (citing *Knotts*, 460 U.S. at 284–285).

[119] *See* United States v. Karo, 468 U.S. 705, 707 (1984) ("In *United States v. Knotts*, we held that the warrantless monitoring of an electronic tracking device ('beeper') inside a container of chemicals did not violate the Fourth Amendment when it revealed no information that could not have been obtained through visual surveillance.") (internal citation omitted). *Cf.* Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (holding that EPA's aerial photography of chemical company's facilities from public airspace with standard photographic equipment was not a "search" for Fourth Amendment purposes).

[120] *See Carpenter*, 138 S. Ct. at 2215.

[121] *Id.*

[122] *See id*. at 2217.

[123] Jones v. United States, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("[W]hen considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements . . . I would ask whether people reasonably expect that their movements will be *recorded and aggregated* in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.") (emphasis added); *see also* United States v. Maynard, 615 F.3d 544, 560 (D.C. Cir. 2010) (holding that the use of a GPS tracking device was a search under the Fourth Amendment and observing that "the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil"). *Cf. Karo*, 468 U.S. at 714–17 (beeper installed in can of ether without a warrant was subject to Fourth Amendment constraints once the can was carried into a private residence—revealing personal information that would not have been obtained through visual surveillance alone).

[124] *Jones*, 565 U.S. at 404.

personal effects protected by the Fourth Amendment.[125] However, several Justices joined opinions that expressed broader concerns with the use of new technologies to surveil persons over extended periods. In a concurring opinion joined by three other members of the Court, Justice Alito concluded that the extended GPS surveillance of a person's public movements implicated a person's reasonable expectation of privacy and therefore constituted a search under the Fourth Amendment.[126] Justice Sotomayor joined Justice Scalia's opinion applying the trespass approach, but wrote a separate concurrence.[127] She agreed with Justice Alito's position but went further to declare that even short-term GPS surveillance could constitute a search under the Fourth Amendment.[128] She observed that GPS surveillance could provide the government with "precise, comprehensive record of a person's public movements," which could be mined "for information years into the future."[129]

More recently in *Carpenter v. United States*, the Court held that the police acquisition of cell phone site location records over a period of 152 days, enabling law enforcement to track a suspect's precise location for an extended period of time, constituted a "search" subject to the Fourth Amendment.[130] The Court reasoned that the acquisition of this data intruded on an individual's reasonable expectation of privacy by potentially revealing a significant amount of personal information.[131]

How this jurisprudence applies to FRT likely depends on how that system is deployed. As a general matter, the limited use of FRT to determine whether a person has traveled to a particular location would not seem to prompt serious concerns under current Fourth Amendment jurisprudence because this information could be gained through visual surveillance alone.[132] And in the *Carpenter* case, it was consequential to the Court that the collection of cell location data provided "near perfect surveillance" capable of producing a "detailed log of [a person's] movements" over an extended time period—not merely a snapshot of the person's location at a particular moment.[133] In short, current Supreme Court jurisprudence holds that surveillance of activities arising in public typically does not raise Fourth Amendment concerns, but surveillance that is *prolonged* and *continuous* may implicate privacy interests protected under the Fourth Amendment.

That said, there may be one notable distinction between the aggregation of cell-site location data and FRT-enhanced surveillance data. It appears unlikely that there is sufficient technological infrastructure for law enforcement to conduct continuous and prolonged FRT-enhanced surveillance to the extent that the Court expressed concern about in *Carpenter*.[134] There may, however, be Fourth Amendment concerns if, for instance, there were cameras throughout a geographic area that allowed law enforcement to capture images of the public, and FRT was then

[125] *Id*.

[126] *Id*. at 429–31 (Alito, J., concurring, joined by Breyer, Ginsburg, and Kagan, JJ.).

[127] *Id.* at 414–15 (Sotomayor, J., concurring).

[128] *Id.* at 415–16.

[129] *Id.*

[130] Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

[131] *Id.*

[132] *See* United States v. Knotts, 460 U.S. 276, 277 (1983) ("[T]here is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin.").

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

[134] *See id.* at 2211; *see also supra* "Use by Law Enforcement."

used to compare those pictures and provide a detailed log of where a particular person had been over an extended period.[135]

In any event, courts have not yet addressed the degree to which *prolonged* FRT-enhanced surveillance implicates the Fourth Amendment. More recently, some circuit courts have held that the surveillance of the front of an individual's home by a pole camera, although not involving FRT, did not constitute a search under the Fourth Amendment because the only information obtained was conduct in front of the home that could be obtained by visual surveillance by law enforcement—not the prolonged and continuous surveillance at issue in *Carpenter*.[136] And one district court held that an aerial surveillance program, which consisted of daily surveillance of the city of Baltimore for approximately 12 hours per day, did not violate the Fourth Amendment.[137] The district court distinguished the aerial surveillance from the surveillance in *Carpenter* on the ground that the aerial surveillance was unable to produce a running log of individuals' movements.[138] In another case, a district court concluded that GPS monitoring was not a search when the tracking only lasted for a period of around twenty-two hours and did not involve trespass onto the suspect's vehicle.[139] The degree of tracking necessary to implicate the Fourth Amendment remains an unresolved question.

It is important to note that law enforcement use of Department of Motor Vehicle (DMV) photos or photos held by other third parties employed in conjunction with a FRT system, in and of itself, likely does not implicate the Fourth Amendment rights of the photo subjects.[140] The Supreme Court has held that, as a general proposition, people have no reasonable expectation of privacy in information that they voluntarily provide to third parties.[141] In the seminal case *United States v. Miller*, the Court concluded that the government's subpoena of a suspect's bank records did not constitute a Fourth Amendment search, as the documents contained "only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[142] The third-party doctrine is based on the rationale that a person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[143] However,

---

[135] There are reports that expansive surveillance is becoming more prevalent in some countries. *See, e.g.*, 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 (reporting that FRT has been "integrated into China's rapidly expanding networks of surveillance cameras, looks exclusively for Uighurs [a Muslim minority in China] based on their appearance and keeps records of their comings and goings for search and review").

[136] United States v. Trice, 966 F.3d 506, 520 (6th Cir. 2020) (ruling there was no reasonable expectation of privacy where a camera monitored the defendant entering and exiting his apartment); United States v. Moore-Bush, 963 F.3d 29, 40 (1st Cir. 2020) (holding defendants had no reasonable expectation of privacy in conduct at the front of their home, which was recorded by a pole camera).

[137] Leaders of a Beautiful Struggle v. Balt. Police Dep't, No. RDB-20-0929, 2020 WL 1975380, at *12 (D. Md. Apr. 24, 2020), *appeal filed*, No. 20-1495 (4th Cir. Apr. 28, 2020).

[138] *Id.*

[139] United States v. Howard, 426 F. Supp. 3d 1247, 1256–57 (M.D. Ala. 2019).

[140] *See, e.g.*, Phillips v. Bailey, 337 F. Supp. 2d 804, 806 (W.D. Va. 2004) (explaining that the plaintiff had "no legitimate expectation of privacy in information voluntarily shared to a third party, such as certain information maintained by the DMV").

[141] Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[142] United States v. Miller, 425 U.S. 435, 442–43 (1976).

[143] *Id.* at 443. Although *Miller* and *Smith* both involve private entities as third parties, the general principle that an individual does not have a reasonable expectation of privacy if he or she has voluntarily provided that information to a third party may still apply when that third party is a government agency. *See, e.g.*, *Phillips*, 337 F. Supp. 2d at 806. But *Carpenter* does suggest that the acquisition of certain information from third parties that provides significant detail into

in *Carpenter*, which also included the issue of whether the criminal defendant had a reasonable expectation of privacy in cell records maintained by a private third party, the Court distinguished *Miller* and its progeny in holding that law enforcement acquisition of cell phone location records held by third-party companies is in fact a "search" for purposes of the Fourth Amendment.[144] The *Carpenter* Court explained that the compelled disclosure by wireless carriers of cell-site location information "provides an intimate window into a person's life."[145] Although *Carpenter* renders the third-party doctrine inapplicable to cell-site location information, the case would not appear likely to disturb the doctrine's applicability to law enforcement acquisition of driver's license photos from the DMV.[146]

Searches at International Borders

The federal government makes use of FRT to identify international travelers coming to and departing from the United States. But under current jurisprudence, this use seems unlikely to trigger serious Fourth Amendment concerns.

Congress has broad authority to regulate persons or property entering the United States—an authority that is rooted in its power to regulate foreign commerce and to protect the integrity of the nation's borders.[147] Under federal statutes, government officers may inspect and search individuals, merchandise, vehicles, and vessels that are attempting to enter the United States or are found further within the interior of the country shortly after entry.[148] Additionally, government officers have statutory authority to investigate potential violations of federal immigration laws at the border and surrounding areas.[149]

Federal law requires DHS to develop and deploy a biometric entry and exit system.[150] CBP has used a form of FRT, known as Traveler Verification Service (TVS), to support biometric entry and exit systems at air, sea, and land environments.[151] CBP also uses facial recognition and iris-scanning technology for pedestrian travelers at some land ports of entry, as well as facial recognition of occupants in moving vehicles entering and exiting the United States.[152] In addition,

---

an individual's life may constitute a search subject to Fourth Amendment scrutiny, regardless of whether the third party is a public or private entity. Carpenter v. United States, 138 S. Ct. 2206, 2217–19 (2018).

[144] *Carpenter*, 138 S. Ct. at 2217–19.

[145] *Id.* at 2217.

[146] *See id.* ("We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his [captured] physical movements . . . .").

[147] *See* United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985) (recognizing "Congress' power to protect the Nation by stopping and examining persons entering this country"); United States v. 12,200-Foot Reels of Super 8mm. Film, 413 U.S. 123, 125 (1973) ("The Constitution gives Congress broad, comprehensive powers 'to regulate Commerce with foreign Nations.' Historically such broad powers have been necessary to prevent smuggling and to prevent prohibited articles from entry.") (quoting U.S. CONST. art. I, § 8, cl. 3.).

[148] 14 U.S.C. § 522; 19 U.S.C. §§ 482, 1467, 1496, 1581, 1583.

[149] 8 U.S.C. § 1357.

[150] *See id*. §§ 1365a, 1365b.

[151] U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR TRAVELER VERIFICATION SERVICE, DHS/CBP/PIA-056 (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-january2020_0.pdf.

[152] *See, e.g.*, Agency Information Collection Activities: Biometric Identity, 83 Fed. Reg. 24,326 (Mar. 25, 2018); Test to Collect Biometric Information at the Otay Mesa Port-of-Entry, 80 Fed. Reg. 70,241 (Nov. 13, 2015); *see also* Test to

CBP collects biometric information of persons interdicted when illegally crossing the international border.[153]

The Supreme Court has recognized searches and seizures at international borders as unique cases for Fourth Amendment purposes.[154] Under the border search exception, searches performed at international borders in relation to an actual or attempted border crossing[155] do not generally require a warrant, probable cause, or reasonable suspicion.[156]

But the border search exception has limits. The Supreme Court has stated that *routine* searches at the border "are reasonable simply by virtue of the fact that they occur at the border."[157] That said, not *all* searches at the border are per se reasonable under the Fourth Amendment. Some border searches conducted in a particularly intrusive manner—such as a body cavity search—may still be limited by the Fourth Amendment.[158] Simply stated, the reasonableness of a border search depends on the circumstances of the search itself.[159]

Depending on the level of intrusion, some searches performed at the international border may require reasonable suspicion of unlawful activity.[160] When determining whether a search is reasonable, Fourth Amendment jurisprudence generally categorizes searches at the border into two categories: routine searches and nonroutine searches, with the latter requiring a level of particularized suspicion of illegal activity. Routine searches generally include searches of

Collect Facial Images from Occupants in Moving Vehicles at the Anzalduas Port of Entry (Anzalduas Biometric Test), 83 Fed. Reg. 56,862 (Nov. 14, 2018).

[153] U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/NPPD/PIA-002 2–5 (Dec. 7, 2012), https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf (discussing the data shared and stored in DHS's biometric database IDENT); U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1 PIA, DHS/OBIM/PIA-004 16–17 (Feb. 24, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf (identifying data collected and stored in the HART system that replaces IDENT as DHS's central biometric database).

[154] United States v. Ramsey, 431 U.S. 606, 617–19 (1977).

[155] Stops and searches may also be conducted at the "functional equivalent" of the border. Almeida-Sanchez v. United States, 413 U.S. 266, 272–73 (1973). Because people can enter the country at points other than along the border, courts have concluded that stops and searches conducted at the first point at which an entrant may practically be detained to be the functional equivalent of the border. *See, e.g.*, United States v. Cardenas, 9 F.3d 1139, 1147 (5th Cir. 1993); United States v. Beras, 183 F.3d 22, 26 (1st Cir. 1999). This includes an airport where an international flight lands. *See, e.g.*, United States v. Yang, 286 F.3d 940 (7th Cir. 2002) (explaining "even though Chicago is not an international border, searches at customs at O'Hare are permissible under the functional equivalent doctrine."). This may also include the port where a ship docks after having been to a foreign port. *See, e.g.*, United States v. Prince, 491 F.2d 655 (5th Cir. 1974); United States v. LaFroscia, 485 F.2d 457 (2d Cir. 1973); *Cardenas*, 9 F.3d at 1147; United States v. Victoria-Peguero, 920 F.2d 77, 80 (1st Cir. 1990) (explaining that a warrantless search at the functional equivalent of the sea border was consistent with Fourth Amendment).

[156] *See* United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

[157] *Ramsey*, 431 U.S. at 616; *Montoya de Hernandez*, 473 U.S. at 539–40 n.4 ("The Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border.").

[158] *See Montoya de Hernandez*, 473 U.S. at 540 n.3; *see also* United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006) (explaining that reasonable suspicion would be required for a more invasive search); United States v. Whitted, 541 F.3d 480, 485–86 (contrasting "routine" "patdowns, frisks, luggage searches, and automobile searches" with "non-routine" "body cavity searches, strip searches, and x-ray examinations" that require reasonable suspicion).

[159] *See Montoya de Hernandez*, 473 U.S. at 538 (noting that the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior).

[160] *See id.* at 537–38 (discussing Fourth Amendment reasonableness requirement at the border).

automobiles, baggage, and other goods entering the country.[161] Additionally, an individual seeking to enter the country may be required to submit to a search of his or her outer clothing,[162] which may include an examination of the contents of a purse, wallet, or pockets and a canine sniff.[163] While this is ongoing, the individual may be subject to a brief detention.[164] Nonroutine border searches—such as prolonged detentions, strip searches, body cavity searches, or involuntary x-ray searches—require reasonable suspicion.[165]

Jurisprudence suggests that minimally intrusive collection of biometric data at an international border does not affront the Fourth Amendment. For example, the Second Circuit[166] has noted that collecting fingerprints, another biometric identifier, at a land port of entry was a routine search, meaning that no reasonable suspicion was required.[167] A Fourth Amendment challenge to the collection of nonobtrusive personal identifiers, such as the collection and comparison of facial geometry through FRT at the border, appears unlikely to succeed in court based on current case law.[168] Furthermore, FRT-enhanced surveillance at the international border, for the purpose of monitoring the entry and exit of persons from the United States, likely would not raise the same privacy concerns in cases like *Carpenter* because the monitoring would not aggregate data providing "an intimate window into a person's life" to the extent it did in *Carpenter*.[169] It therefore seems unlikely that a court would conclude that the use of FRT for the sole purpose of monitoring the entry and exit of travelers raises meaningful Fourth Amendment concerns.

Wrongful Arrests and Other Potential Criminal Consequences

Some observers have expressed concern that unreliable FRT may have potentially significant consequences for a misidentified person, such as mistaken arrest.[170]

---

[161] *See, e.g.*, United States v. Sandoval Vargas, 854 F.2d 1132 (9th Cir. 1988) (car); United States v. Flores, 594 F.2d 438 (5th Cir. 1979) (car); *Lafroscia*, 485 F.2d 457 (car); United States v. Gonzalez, 483 F.2d 223 (2d Cir. 1973) (baggage); United States v. Stornini, 443 F.2d 833 (1st Cir. 1971) (baggage).

[162] *See, e.g.*, United States v. Braks, 842 F.2d 509, 515 (1st Cir. 1988) (holding that requiring a female suspect to lift her dress somewhat in a private room with a female inspector present was part of routine border search); United States v. Nieves, 609 F.2d 642, 646 (2d Cir. 1979) (holding that requiring a person to remove a shoe is part of routine border search but drilling into shoes is not routine border search); United States v. Flores, 477 F.2d 608, 609 (1st Cir. 1973) (ruling that search of pockets was justified).

[163] *See, e.g.*, United States v. Kelly, 302 F.3d 291, 294–95 (5th Cir. 2002) (recognizing that a canine sniff was routine border search, reasoning a canine sniff "is no more intrusive than a frisk or a pat-down, both of which clearly qualify as routine border searches.").

[164] *See, e.g.*, United States v. Nava, 363 F.3d 942, 946 (9th Cir. 2004) (individual was not subject to an "arrest" when officer asked him to exit truck, handcuffed him, escorted him to security office to be patted down, and was required to wait while officer inspected pickup truck).

[165] *Montoya de Hernandez*, 473 U.S. at 541 n.4. *See, e.g.*, United States v. Garcia-Garcia, 319 F.3d 726, 730 (5th Cir. 2003) (alert by drug sniffing dog constituted reasonable suspicion supporting detention of bus for time reasonably necessary to investigate the cause of the alert). The reasonable suspicion standard is "considerably less than proof of wrongdoing by a preponderance of the evidence, and obviously less than is necessary for probable cause." Navarette v. California, 572 U.S. 393, 397 (2014) (internal quotation marks omitted) (quoting United States v. Sokolow, 490 U.S. 1, 7 (1989)).

[166] For purposes of brevity, references to a particular circuit in this report (e.g., the Second Circuit) refer to the U.S. Court of Appeals for that particular circuit (e.g., the U.S. Court of Appeals for the Second Circuit).

[167] Tabbaa v. Chertoff, 509 F.3d 89, 99 (2d Cir. 2007).

[168] *See id.*

[169] Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018).

[170] *See, e.g.*, BUOLAMWINI ET AL., *supra* note 24, at 13. A June 2020 *New York Times* article details concerns about the use of facial recognition as an investigatory tool leading to false arrests and false criminal charges. Kashmir Hill,

Reliance on inaccurate FRT when seeking an arrest warrant may raise questions about whether the warrant is supported by probable cause.[171] The probable cause requirement "protects citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime, while giving fair leeway for enforcing the law in the community's protection."[172] The Supreme Court has recognized that probable cause is a concept that is imprecise, fluid, and dependent on the context of the search or seizure.[173] Typically evaluated under a totality-of-the-circumstances test, courts consider all available information, rather than apply bright-line rules, to determine whether probable cause exists.[174] Generally, "[t]o determine whether an officer had probable cause for an arrest, the court examines the events leading up to the arrest, and then decides whether these historical facts, viewed from the standpoint of an objectively reasonable police officer, amount to probable cause."[175]

Although investigatory officers have deployed FRT to identify suspects, a survey of case law suggests that courts have rarely considered probable cause challenges to police work that relied on purportedly unreliable FRT matches.[176] But courts have considered other situations involving potentially unreliable sources, such as informants and canine alerts, which may offer insight into how a court may rule on a probable cause challenge to an arrest or search based on inaccurate or unreliable FRT results. As with FRT, lack of trust in an unreliable informant or a canine alert may raise questions of whether law enforcement had sufficient reason to suspect criminal activity in obtaining a warrant.

Courts often must determine whether an informant's tip sufficiently supports a finding of probable cause.[177] In *Aguilar v. Texas*, the Supreme Court held that a law enforcement affidavit submitted in support of a search warrant, based on information supplied by an unidentified informant, was insufficient to establish probable cause.[178] The Court concluded that the affidavit did not describe underlying circumstances that would provide police with a basis to consider the

---

Wrongfully Accused by Algorithm, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html. There, a man was arrested for larceny after FRT matched a still frame from a store surveillance video with his driver's license photo in a FRT database. *Id.* Reportedly, the officers had relied solely on the photo comparison to obtain a warrant, arrest, and detain the suspect for 30 hours. *Id.*

[171] *See* Illinois v. Gates, 462 U.S. 213, 232 (1983).

[172] Maryland v. Pringle, 540 U.S. 366, 370 (2003) (quoting Brinegar v. United States, 338 U.S. 160, 176 (1949) (internal quotation marks omitted)).

[173] *See Gates*, 462 U.S. at 231–32 ("Perhaps the central teaching of our decisions bearing on the probable cause standard is that it is a 'practical, nontechnical conception.' . . . [P]robable cause is a fluid concept—turning on the assessment of the probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.").

[174] *See* Florida v. Harris, 568 U.S. 237, 244 (2013).

[175] *Pringle*, 540 U.S. at 371.

[176] *See, e.g.*, United States v. Green, No. 08-44, 2011 WL 1877299 (E.D. Penn. May 16, 2011) (defendant did not challenge the use of FRT, but instead raised other arguments challenging his convictions, such as prosecutorial misconduct and court error in admitting certain evidence).

[177] Aguilar v. Texas, 378 U.S. 108, 113–15 (1964).

[178] *Id.* at 115–16 (rejecting officer's statement that "affiants have received reliable information from a credible person and believe" that heroin was stored in home). The *Aguilar* Court established a two-pronged test that was later abandoned in *Illinois v. Gates* for an approach that considers the totality of the circumstances when determining whether probable cause exists. 462 U.S. at 238–39. The prongs enunciated in *Aguilar*—basis-of-knowledge and veracity—remain "highly relevant" in determining the value of an informant's tip. *Gates*, 462 U.S. at 230. The prongs are no longer treated as separate, independent requirements. *Id.* Rather, they are indicia of reliability that may be considered in *Gates'* "totality-of-the-circumstances" test. *Id.*

informant credible or his information reliable.[179] And in *Illinois v. Gates*, the Court held that a reviewing court must consider the *totality of the circumstances* when evaluating whether probable cause exists.[180] The Court explained the following:

> A sworn statement of an affiant that "he has cause to suspect and does believe that" liquor illegally brought into the United States is located on certain premises will not do. *Nathanson v. United States,* 290 U.S. 41 (1933). An affidavit must provide the magistrate with a substantial basis for determining the existence of probable cause, and the wholly conclusory statement at issue in *Nathanson* failed to meet this requirement. An officer's statement that "affiants have received reliable information from a credible person and believe" that heroin is stored in a home, is likewise inadequate. *Aguilar v. Texas,* 378 U.S. 108 (1964). As in *Nathanson,* this is a mere conclusory statement that gives the magistrate virtually no basis at all for making a judgment regarding probable cause. Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others. In order to ensure that such an abdication of the magistrate's duty does not occur, courts must continue to conscientiously review the sufficiency of affidavits on which warrants are issued.[181]

In other words, a reviewing court balances factors like the reliability of the informant, the basis for the informant's information, and the extent to which the police have corroborated the tip.[182] For instance, a judge may at times disregard the fact that a confidential informant's criminal record or drug addiction undermines her reliability if other factors point toward the informant's truthfulness.[183]

In other cases, reviewing courts have evaluated whether a drug-detection dog's positive alert provides law enforcement with probable cause to search an area.[184] The reliability or accuracy of those alerts has been the subject of significant litigation. In *Florida v. Harris*, the Supreme Court considered the standard for determining whether the alert of a drug-detection dog during a traffic stop provided probable cause to search a vehicle.[185] Writing for the Court, Justice Kagan observed that "[t]he question—similar to every inquiry into probable cause—is whether all the facts surrounding a dog's alert, viewed through the lens of common sense, would make a reasonably prudent person think that a search would reveal contraband or evidence of a crime."[186] The Court then concluded that the dog's alert gave the officer probable cause to search the vehicle because

[179] *Aguilar*, 378 U.S. at 113–15.

[180] *Gates*, 462 U.S. at 230–31.

[181] *Id.* at 239.

[182] *Id.* at 230–34.

[183] United States v. McKinney, 919 F.2d 405, 415 (7th Cir. 1990) ("The magistrate was thus presented with specific details of a crime; neither Brown's drug addiction nor criminal record warranted disregarding her report. Although an informant's reliability is a factor to be considered by a court, it is just one relevant consideration in the totality of the circumstances analysis.").

[184] *See, e.g.*, Florida v. Harris, 568 U.S. 237, 247 (2013) ("[A] probable-cause hearing focusing on a dog's alert should proceed much like any other."). There is a separate question of whether a dog sniff is, in itself, a search under the Fourth Amendment. *See, e.g.*, Florida v. Jardines, 569 U.S. 1, 11 (2013) (holding that a dog sniff to investigate home and immediate surrounding was a "search" under the Fourth Amendment); United States v. Place, 462 U.S. 696, 707 (1983) (dog sniff of luggage in public place was not a "search" under the Fourth Amendment). But whether a dog's sniff is itself a search under the Fourth Amendment is a distinct question from whether the dog's positive alert is sufficient evidence to give probable cause supporting a warrant to search or arrest an individual.

[185] *Harris*, 568 U.S. at 240.

[186] *Id.* at 248.

substantial evidence of the dog's training and proficiency "provide[d] sufficient reason to trust the alert."[187]

Lower courts have likewise found dog alerts sufficiently reliable to establish probable cause.[188] For instance, in *United States v. Green*, the Fourth Circuit concluded that the totality of the circumstances established a dog's reliability, given the dog's field performance records, performance during training and recertification exercises, and evaluations.[189] The dog's field performance reports reflected an accuracy rate of 25.88%, but the court commented that the dog had a success rate of 43% when considering that the dog alerted for vehicles in which drugs had recently been in the vehicle—even if no drugs were in the vehicle at the time of the alert.[190] According to the Fourth Circuit, this was sufficient under the totality of the circumstances to establish the dog was sufficiently reliable in detecting drugs to justify probable cause to search the vehicle.[191]

Like searches supported by information provided by informants and dog sniffs, the reliability of the specific FRT system may be subject to scrutiny by a reviewing court when assessing the basis for a law enforcement search or arrest of an identified suspect.[192] A court may consider, for example, whether the FRT system's accuracy was affected by physical or algorithmic factors that could result in misidentification.

For these reasons, the Supreme Court's probable cause jurisprudence suggests that a reviewing court would consider the totality of the circumstances surrounding the face match using FRT. This might include, for example, the reported accuracy rate of a particular FRT system, the quality of the image, whether a secondary verification by a human confirmed the selection, and whether additional facts obtained by police support a conclusion that the suspect identified by FRT is the individual who committed the alleged crime.

The First Amendment

In addition, some commentators have suggested that FRT-enhanced surveillance by the government may cause people to self-censor protected speech in violation of the First Amendment.[193] Some claim that the mere threat or fear of monitoring or identifying persons by FRT-enhanced surveillance at a public demonstration could have a "chilling effect" on the exercise of constitutionally protected speech and assembly rights.[194]

---

[187] *Id.* at 246–47.

[188] *See, e.g.*, United States v. Bentley, 795 F.3d 630, 636–37 (7th Cir. 2015) (reliability satisfied with a showing of a 93% alert rate and a 59.5% accuracy rate and training); *see also* United States v. Lozano, 761 F. App'x. 444, 445–48 (5th Cir. 2019) (per curiam) (stating that canine sniff is presumptively reliable).

[189] United States v. Green, 740 F.3d 275, 282 (4th Cir. 2014).

[190] *Id.* at 283.

[191] *Id.* at 283–84.

[192] For instance, one company, which uses an algorithm often sold to police, claims to have an identification rate above 95% as measured by U.S. government-sponsored Face Recognition Vendor Tests. *See* THE PERPETUAL LINE-UP, *supra* note 3, at 46. Critics have claimed that the statistic is outdated and misrepresentative of the accuracy. *Id.* For a further discussion regarding why accuracy rate estimates differ among observers, see 2020 GAO REPORT, *supra* note 1, at 33.

[193] *See* THE PERPETUAL LINE-UP, *supra* note 3, at 42–44.

[194] *See, e.g.*, FRT CIVIL RIGHTS CONG. HEARING, *supra* note 94, at 41 (testimony of Clare Garvie, Senior Associate, Georgetown University Law Center, Center on Privacy & Technology).

The First Amendment protects the freedoms of speech and peaceable assembly.[195] Neither the Supreme Court nor lower federal courts have addressed any First Amendment challenges to the use of FRT-enhanced surveillance. On one hand, as discussed in more detail below, the Supreme Court has held that the First Amendment protects the right to anonymous speech and association.[196] On the other hand, the Court has also held that the mere surveillance of speech, without more, likely does not provide a plaintiff grounds to bring suit alleging a First Amendment violation.[197]

The Supreme Court has long recognized that government investigative activities, including surveillance, may implicate the First Amendment.[198] In *NAACP v. Alabama*, the Supreme Court held that the NAACP could not be compelled by state law to disclose the identities and personal information of its members because that disclosure would likely hinder the ability of those members collectively to advocate their beliefs.[199] The Court explained that there is a "vital relationship between freedom to associate and privacy in one's associations."[200]

But then again, the First Amendment does not guarantee a right to be free from surveillance. In *Laird v. Tatum*, the plaintiffs alleged that military surveillance of public meetings and demonstrations impermissibly chilled their speech in violation of the First Amendment.[201] Declining to rule on the merits, the Court held that Article III standing requirements were not satisfied because the plaintiffs had failed to allege a past harm or immediate danger of direct injury.[202] The Court described the plaintiff's claims as asserting only that "the Army may at some future date misuse the information" gained from their surveillance activities.[203] The Court said that these "speculative" allegations were "not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm."[204] And the Supreme Court's 2013 decision in *Clapper v. Amnesty International*, concerning a challenge to a provision in the Foreign Intelligence Surveillance Act (FISA), reaffirmed *Laird*'s holding.[205] There, the plaintiffs argued there was an objectively reasonable likelihood that their communications with foreign contacts would be intercepted at some point in the future under the FISA provision, which allows surveillance of individuals who are not "United States persons" and are reasonably believed to be located outside the United States.[206] The Supreme Court ruled that the plaintiffs failed to allege an Article III injury that was "certainly impending" or "imminent" to confer standing, because their

[195] U.S. CONST. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.").

[196] *See, e.g.*, NAACP v. Ala. *ex rel.* Patterson, 357 U.S. 449, 466 (1958) (striking down a state order for the NAACP to disclose its membership lists); *see also* Talley v. California, 362 U.S. 60, 64–65 (1960).

[197] *See, e.g.*, Laird v. Tatum, 408 U.S. 1, 2–3, 11–14 (1972) (holding that allegations of a subjective chilling effect by "mere existence, without more, of investigative and data-gathering activity" does not constitute an injury sufficient to confer standing to sue).

[198] *See, e.g.*, *NAACP*, 357 U.S. at 466.

[199] *Id.*

[200] *Id.* at 462.

[201] *Laird*, 408 U.S. at 2.

[202] *Id.* at 13.

[203] *Id.*

[204] *Id.* at 14.

[205] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 417–18 (2013).

[206] *Id.* at 411–12.

asserted injury was "too speculative,"[207] given the lack of evidence suggesting that the government was likely to "imminently target" their communications.[208]

Additionally, First Amendment implications may go beyond preemptive concerns of the chilling of speech by the threat of FRT-enhanced surveillance; the First Amendment also prohibits government officials from retaliating against individuals for engaging in protected speech.[209] If there are allegations of retaliatory arrests, for example, a plaintiff must prove that the arresting officer possessed impermissible animus against the protected speech and that the officer lacked probable cause to make the arrest.[210] If there was probable cause, the claim of retaliatory arrest fails.[211] If there was not probable cause, the plaintiff would then need to show that retaliation was a substantial or motiving factor behind the prosecution and that the prosecution would have been pursued absent a retaliatory motive.[212]

It is important to note that law enforcement has sometimes used FRT-enhanced surveillance of public events to identify suspects for arrest.[213] It is unclear whether or how this might affect a court's analysis of the use of FRT-enhanced photographic surveillance of public gatherings under the First Amendment.[214]

Equal Protection

Even when the government's use of FRT does not implicate the First or Fourth Amendments, it is possible that it could raise equal protection concerns under the Fifth or Fourteenth Amendments. Some allege that algorithmic biases or other factors may lead to persons of some racial or ethnic groups being more likely to be misidentified through FRT and wrongly arrested as a result.[215]

---

[207] *Id.*

[208] *Id.*

[209] Nieves v. Bartlett, 139 S. Ct. 1715, 1722 (2019).

[210] Lozman v. City of Riviera Beach, Fla., 138 S. Ct. 1945, 1952 (2018) (citing Hartman v. Moore, 547 U.S. 250, 265–66 (2006)); *see also Nieves*, 139 S. Ct. at 1726 (applying *Hartman*'s no-probable-cause rule for claims of retaliatory arrests).

[211] *Nieves*, 139 S. Ct. at 1725. *See also*, *e.g.*, Hartman v. Thompson, 931 F.3d 471, 483–85 (6th Cir. 2019) (ruling that that First Amendment retaliation claim failed when protestors were arrested based on probable cause for "causing a disruption" at an event during a state fair); *id.* at 486 (Bush, J., concurring in part and in the judgment) (joining majority opinion in concluding that the defendants had probable cause to arrest plaintiffs); Case v. City of New York, 233 F. Supp. 3d 372, 389 (S.D.N.Y. 2017) (dismissing First Amendment retaliation claim because protestor had pleaded guilty to disorderly conduct).

[212] *Nieves*, 139 S. Ct. at 1725 (citing *Lozman*, 138 S. Ct. at 1952–53).

[213] For example, FRT was used by the Baltimore Police Department to monitor protesters during the unrest following the death of Freddie Gray, reportedly leading to the apprehension and arrest of protestors who had outstanding warrants. *See* Benjamin Powers, *Eyes Over Baltimore: How Police Use Military Technology to Secretly Track You*, ROLLING STONE (Jan. 6, 2018), https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885/.

[214] Although discussed in the Fourth Amendment context in *United States v. Jones*, Justice Sotomayor stressed that anonymity protects against the government keeping track of a person's movements that "reflect[] a wealth of detail about her familial, political, professional, religious, and sexual association." 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

[215] *See*, *e.g.*, FRT CIVIL RIGHTS CONG. HEARING, *supra* note 94, at 37 (testimony of Joy Buolamwini, Founder, Algorithmic Justice League) ("[B]ecause you have the propensity for these systems to misidentify black individuals or brown communities more often and you also have confirmation bias where if I have been said to be a criminal that I am more targeted, so there is a case with Mr. Bah, an 18-year-old African-American man, who was misidentified in Apple stores as a thief and in fact he was. . . falsely arrested multiple times because of this kind of misidentification.").

The Equal Protection Clause, located in the Fourteenth Amendment, provides in part: "No state shall . . . deny to any person within its jurisdiction the equal protection of the laws."[216] The Supreme Court has held that equal protection also applies to the federal government through the Due Process Clause of the Fifth Amendment on the rationale that the Fifth Amendment includes an implicit requirement for equal protection.[217] Simply stated, equal protection generally requires that the government treat people alike.

Under equal protection jurisprudence, "[r]acial and ethnic distinctions of any sort are inherently suspect and thus call for the most exacting examination."[218] One way of establishing an equal protection violation is to show that a seemingly neutral law is enforced in a discriminatory manner.[219] A claim of racially selective law enforcement requires the plaintiff to show that the defendant's actions had a discriminatory *effect and* the defendant acted with a discriminatory *purpose*.[220] Once the plaintiff shows a discriminatory effect and discriminatory purpose, the burden shifts to the government to prove that it would have taken the same action without the discriminatory motivation.[221]

Official action will not be held unconstitutional solely because of a racially disproportionate impact, except perhaps in extreme cases.[222] Two Supreme Court decisions highlight how evidence of disparate impact is has been inadequate, by itself, to establish an equal protection violation. In *Washington v. Davis*, the Court considered an equal protection challenge to a police force application for the Washington, DC police, which black applicants failed significantly more often than white applicants.[223] The Supreme Court held, however, this disproportionate impact did not, by itself, show an improper racial classification.[224] Similarly, in *McCleskey v. Kemp*, the Supreme Court held that proof of disparate frequency in death penalty sentencing could not establish an equal protection violation.[225] There, statistics demonstrated racial inequality in whether a defendant received a death sentence.[226] The Supreme Court, however, explained that for the defendant to demonstrate an equal protection violation, he "must prove that the decision makers in *his* case acted with discriminatory purpose."[227] The Court also stressed that to challenge the law authorizing capital punishment, the defendant "would have to prove that the Georgia Legislature enacted or maintained the death penalty statute *because of* an anticipated racially

[216] U.S. CONST. amend. XIV; *see, e.g.*, Brown v. Board of Ed. of Topeka, 347 U.S. 483, 495 (1954) (holding that segregation in Kansas public schools is a "denial of the equal protection of the laws").

[217] Bolling v. Sharpe, 347 U.S. 497, 498–500 (1954) (holding that the segregation of students in District of Columbia public schools "constitutes an arbitrary deprivation of their liberty in violation of the Due Process Clause").

[218] Univ. of Cal. Regents v. Bakke, 438 U.S. 265, 291 (1978) (plurality opinion).

[219] *See, e.g.*, United States v. Armstrong, 517 U.S. 456, 465 (1996) (claimant challenging prosecution under equal protection was required to show that the "federal prosecutorial policy 'had a discriminatory effect and that it was motivated by a discriminatory purpose.'").

[220] Hunter v. Underwood, 471 U.S. 222, 227–28 (1985) (holding that a provision of the Alabama Constitution of 1901, which disenfranchised persons convicted of crimes involving moral turpitude, violated equal protection because, even though the provision was racially neutral, its enactment was motivated by a desire to discriminate on account of race and had a racially discriminatory effect).

[221] *Id.* at 228.

[222] *See* Vill. of Arlington Heights v. Metro. Hous. Dev. Corp., 429 U.S. 252, 264–65 (1977).

[223] Washington v. Davis, 426 U.S. 229, 229 (1976).

[224] *Id.* at 239.

[225] McCleskey v. Kemp, 481 U.S. 279, 297–99 (1987).

[226] *See id.* at 286.

[227] *Id.* at 292.

discriminatory effect."[228] *Davis* and *McCleskey* demonstrate that a showing of disparate impact likely cannot, by itself, prove an equal protection violation; a plaintiff must also prove a discriminatory purpose.

Proving discriminatory purpose may, however, be a difficult task. "Determining whether invidious discriminatory purpose was a motivating factor demands a sensitive inquiry into such circumstantial and direct evidence of intent as may be available."[229] In *Village of Arlington Heights v. Metropolitan Housing Development Corp.*, the Supreme Court established a multifactor test to determine whether a certain law has a discriminatory purpose.[230] For some cases, a law's impact may be so clearly discriminatory as to allow no other explanation than it was adopted for impermissible purposes.[231] In cases without a clear discriminatory pattern, *Arlington Heights* articulated relevant factors to consider: the historical background of the decision; the specific sequence of events leading up to the challenged decision; departures from normal procedures; and contemporary statements by relevant government decisionmakers and reports or other documents.[232] And in *Personnel Administrator of Massachusetts v. Feeney*, the Court explained that "discriminatory purpose" requires more than "intent as volition or intent as awareness of consequences."[233] "Discriminatory purpose 'implies that the decisionmaker . . . selected or reaffirmed a particular course of action at least in part '*because of*,' not merely 'in spite of,' its adverse effects upon an identifiable group.'"[234]

To date, federal courts have rarely, if ever, confronted equal protection claims involving the use of FRT. It is likely, though, that a plaintiff asserting an equal protection claim would first seek to establish a discriminatory effect arising out of the use of FRT as an identification tool. To do so, the plaintiff may point to aggregated data showing accuracy rates.[235] It is also worth noting that accuracy rates may also depend on the particular FRT system used. A plaintiff would thus likely need to establish that the specific system used caused discriminatory impact.

Current case law suggests that a plaintiff would need to show that not only was there a disparate impact from the use of FRT, but that the defendant had discriminatory purpose. Applying the *Arlington Heights* factors, a claimant would likely face an uphill battle in establishing

---

[228] *Id.* at 298.

[229] Vill. of Arlington Heights v. Metro. Hous. Dev. Corp., 429 U.S. 252, 266 (1977).

[230] *Id.* at 266–68.

[231] *Id.* at 266 ("The impact of the official action—whether it 'bears more heavily on one race than another'—may provide an important starting point. Sometimes a clear pattern, unexplainable on grounds other than race, emerges from the effect of the state action even when the governing legislation appears neutral on its face."); *see also* Yick Wo v. Hopkins, 118 U.S. 356, 373 (1886) (ruling that a pattern of disproportionately denying waivers to laundry owners of Chinese ancestry established an equal protection violation, observing that "[n]o reason for [the discrepancy] is shown, and the conclusion cannot be resisted that no reason for it exists except hostility to the race and nationality to which the petitioners belong, and which, in the eye of the law, is not justified").

[232] *Arlington Heights*, 429 U.S. at 266–68; *see also* Fusilier v. Landry, 963 F.3d 447, 463 (5th Cir. 2020) (reversing district court finding of a discriminatory purpose where the conclusion was based primarily on the discriminatory impact of at-large voting, the sequence of events, and the alleged pretextual arguments).

[233] Pers. Adm'r of Mass. v. Feeney, 442 U.S. 256, 279 (1979).

[234] Congregation Rabbinical Coll. of Tartikov, Inc. v. Vill. of Pomona, 945 F.3d 83, 111 (2d Cir. 2019) (quoting *Feeney*, 442 U.S. at 279 (emphasis added)).

[235] *Cf., e.g.*, Blackwell v. Strain, 496 F. App'x. 836 (2012) (submitting statistical evidence concerning conduct of state police officers stationed at land port of entry). Indeed, courts have found statistics persuasive in proving discriminatory effect, as evidenced in *McCleskey* where statistics showed that the state imposed capital punishment for 22% of black defendants with white victims; for 8% of white defendants with white victims; and for 3% of white defendants with back victims. McCleskey v. Kemp, 481 U.S. 279, 286 (1987).

discriminatory purpose. It seems unlikely that a plaintiff could prevail in the first part of the *Arlington Heights* test—showing that the impact of government action is so clearly discriminatory as to allow no other explanation than it was adopted for impermissible purposes.[236] For example, a defendant may claim that an FRT system permits law enforcement to more efficiently identify potential suspects.[237] It appears unlikely that a court would conclude that there could be no other explanation for implementing FRT besides a discriminatory purpose.[238] Turning to the other *Arlington Heights* factors, a plaintiff may then attempt to prove discriminatory purpose through circumstantial evidence.[239] A court would consider the historical background, events leading up to the decision, departures from normal procedure, and decisionmakers' contemporaneous statements.[240]

The traditional equal protection framework focuses on the intent of human decisionmakers. This framework does not translate easily to automated, algorithmic-based systems like those frequently employed by FRT, which make independent determinations without close human involvement.[241] As mentioned above, a criminal suspect who alleges that he was wrongfully arrested "must prove that the decisionmakers in *his case* acted with discriminatory purpose."[242] But how does this standard apply when a decision to arrest a person is most immediately prompted by an algorithmic determination in an FRT system, rather than personal animus of a human decisionmaker?

It is possible that a reviewing court's inquiry would revolve around the human decisionmaker's decision to deploy FRT generally or in a specific situation. If the decisionmaker was unaware of issues with the FRT system that made it unreliable, thereby resulting in the disproportionate misidentification of certain demographic groups, it seems unlikely that an equal protection violation could be established. But even if the decisionmaker was generally aware that the system's accuracy rate varied for different demographic groups, that awareness might not be sufficient to support an equal protection claim. In *Personnel Administrator of Massachusetts v. Feeney*, the Supreme Court explained that "discriminatory purpose" requires more than "awareness of consequences."[243] Accordingly, a claim against a human decisionmaker would likely need to show not only that the person was aware that the FRT might be more likely to misidentify persons of a particular group, but also that the decisionmaker intended to use the FRT

[236] *See Arlington Heights*, 429 U.S. at 266.

[237] *See, e.g.*, *Facial Recognition Technology: Ensuring Transparency in Government Use: Statement Before the House Oversight and Reform Committee*, FBI NEWS (June 4, 2019), https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use (statement of Kimberly J. Del Greco, Deputy Assistant Director, FBI).

[238] *Cf.* Doe ex rel. Doe v. Lower Merion School Dist., 665 F.3d 524, 552 (2011) (noting insufficient discriminatory impact to establish discriminatory purpose in redistricting schools, pointing to other explanations for the redistricting plan); Hayden v. Paterson, 594 F.3d 150, 168 (2d Cir. 2010) ("Absent any adequately supported factual allegations as to discriminatory intent behind the enactment of the 1894 constitutional provision, we are compelled to find that the New York Constitution's requirement that the legislature pass felon disenfranchisement laws is based on the obvious, noninvidious purpose of disenfranchising felons, not Blacks or Latinos.").

[239] *See Arlington Heights*, 429 U.S. at 266–68.

[240] *See id.*

[241] Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARVARD J. L. & TECH. 889, 891–93 (2018).

[242] *McCleskey*, 481 U.S. at 292 (emphasis in original).

[243] Pers. Adm'r of Mass. v. Feeney, 442 U.S. 256, 279 (1979).

"at least in part 'because of,' not merely 'in spite of,' its adverse effects upon an identifiable group."[244]

In any event, an equal protection analysis is a fact-intensive inquiry. Given that these claims hinge on the specific circumstances and remain untested in the courts, the circumstances in which a plaintiff may pursue an equal protection claim for disparate outcomes arising from inaccurate FRT is an open question.

Proposed Legislation in the 116th Congress

Several bills have been introduced in the 116th Congress to restrict the use of FRT by federal and state governments. For instance, companion bills introduced in the House and Senate (H.R. 7356/S. 4084) would place a moratorium on the use of FRT by federal officers, agents, employees, and contractors, except in situations Congress has specifically authorized the activities.[245] The bills would also require the congressionally authorized activity to satisfy several conditions, including standards for use and management of information derived from the system, "auditing requirements to ensure the accuracy of biometric surveillance system technology, standards for minimum accuracy rates, and accuracy rates by gender, skin color, and age," and "rigorous protections for due process, privacy, free speech and association, and racial, gender, and religious equity."[246]

Several bills include provisions that would ban federal funding to states and local governments if they purchase or use FRT.[247] H.R. 7356/S. 4084, mentioned above, would make a state or local government ineligible for grants under the Edward Byrne Memorial Justice Assistance Grant program[248] if the state or local government acquired, possessed, accessed, or used FRT.[249] The legislation includes a private cause of action, as well as a provision for enforcement by state attorneys general.[250]

Other bills, S. 3284 and S. 2878, would prohibit the use of FRT except in certain situations where a warrant is obtained.[251] Another bill, H.R. 4021, would restrict a federal agency from using FRT systems that incorporate any photo identification obtained by a state or federal government, unless the agency obtained a federal court order determining there is probable cause to use FRT.[252] The bill would also prohibit the sharing of information between federal agencies unless a federal court order has been obtained.[253]

[244] *Id.*

[245] H.R. 7356, 116th Cong. (2020); S. 4084, 116th Cong. (2020).

[246] H.R. 7356, 116th Cong. (2020), at § 3(b).

[247] *See, e.g.*, H.R. 3875, 116th Cong. (2020).

[248] 34 U.S.C. § 10151 *et seq.* This program grants federal funds to states, the District of Columbia, and territories for nonfederal criminal justice initiatives. For further information on this grant program, see CRS In Focus IF10691, *The Edward Byrne Memorial Justice Assistance Grant (JAG) Program* (updated Jan. 2020), by Nathan James.

[249] H.R. 7356, 116th Cong. § 4(a) (2020); *see also* S. 4084, 116th Cong. (2020).

[250] H.R. 7356, 116th Cong. § 3(c)(2) (2020).

[251] *See* S. 3284, 116th Cong. (2020); S. 2878, 116th Cong. (2020).

[252] H.R. 4021, 116th Cong. § 2(a) (2019).

[253] *Id.* § 2(b).

In contrast, S. 847 would regulate private entities' use of FRT.[254] It would prohibit certain nongovernmental entities from using FRT to identify or track a user, as well as sharing facial recognition data with a third party without obtaining the user's consent.[255] A violation would be categorized as an unfair or deceptive act or practice under the Federal Trade Commission Act, and the Federal Trade Commission would have the authority to enforce the act.[256] The bill would also allow a state attorney general to bring a civil action on behalf of a state's residents.[257]

Author Information

Kelsey Y. Santamaria
Legislative Attorney

Disclaimer

[254] S. 847, 116th Cong. (2019).

[255] *Id.* § 3.

[256] *Id.* § 4(a).

[257] S. 847, 116th Cong. § 4(c)(1) (2019).