Face IT: Only Congress Can Preserve Privacy from the Pervasive Use of Facial Recognition Technology by Police

JOHN ZENS*

TABLE OF CONTENTS

 J.D. Candidate 2021, University of San Diego School of Law. I would like to thank Nicole Zens, for her contribution to my selection of the topic of this Comment; Erica Zens for her love and support throughout the writing process; Michele Brower for her keen editorial eye; and Professor Kevin Cole for his oversight and guidance. I also extend my gratitude to the *San Diego Law Review* editorial board and members for their dedicated efforts.

I. INTRODUCTION

A young person in a hooded sweatshirt saunters down a suburban sidewalk. When a police cruiser rounds the corner, they duck their head, avoiding eye contact. Normally, the officer behind the wheel would chance a glance at this relatively inconspicuous person. Perhaps the officer would feel a twinge of suspicion due to the person's attire or somewhat elusive behavior. Absent additional indicia of criminal activity,[1] the officer's interest would wane almost immediately: an officer patrolling a crime hotspot would wait for a hot lead, and even a bored officer in a low-crime area has more important things to do. The encounter would barely amount to a blip.

1. The "reasonable suspicion" standard is an "elusive" one. Margaret Raymond, *Down on the Corner, Out in the Street: Considering the Character of the Neighborhood in Evaluating Reasonable Suspicion*, 60 OHIO ST. L.J. 99, 102 (1999). An officer must determine the probability that criminal activity is afoot based on factual observations that "in light of the officer's experience, demonstrate a sufficient quantum of probability that an individual is involved in criminal activity." *Id.* at 104. The suspicion must also be particularized, and thus based on the behavior of the individual. *See id.* at 105–06. Here, an officer could not express the requisite "specific and articulable facts which, taken together with the rational inferences from those facts," established reasonable suspicion. *See* Terry v. Ohio, 392 U.S. 1, 21 (1968). However, the *Terry* "reasonable suspicion" doctrine has been stretched thin since the case was decided. *See, e.g.*, Illinois v. Wardlow, 528 U.S. 119, 124 (2000) (finding a stop legal when the individual was in a "high crime area" and exhibited "nervous, evasive behavior" (quoting Adams v. Williams, 407 U.S. 143, 147 (1972))); Whren v. United States, 517 U.S. 806, 818–19 (1996) (allowing stop and frisk following even minor violations of traffic laws); *Adams*, 407 U.S. at 147–48 (blurring the distinction between stops and protective frisks).

However, this police cruiser has cameras equipped with facial recognition technology (FRT). As soon as the vehicle rounds the corner, an FRT camera scans the person's face, maps their facial features, and converts that data into a numerical "faceprint."[2] Before the person ducks their head, the FRT software identifies them by comparing that faceprint to a database of "known faces."[3] The facial recognition system instantly provides the officer the person's name, address, criminal history, and other personal information.[4] The officer notes several factors that, in combination with the elusive conduct, lead the officer to form an articulable, reasonable suspicion that the young person is involved in criminal activity.[5] The officer asks them to stop, which they do. The officer conducts a protective frisk, running their hands along the person's body, squeezing to ensure they possess no concealed weapons.[6] The officer asks a barrage of questions about who the person is, where they are going, and what they are doing. All the while, the person's reputation in the community suffers due to the stigma attached to a subject of a police investigation in public view.[7]

Depending on what flagged the officer's attention, the public reaction is likely to vary. If the officer discovered an open warrant for the person's arrest related to a violent felony charge, technology enhanced policing is the hero of the day, enhancing public safety.[8] However, the public might

---

2. *See infra* Section II.A.

3. *See infra* note 20 and accompanying text.

4. Hypothetically, the officer could even access social media posts. *See, e.g.*, Olivia Solon, *Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent*, NBC NEWS (Mar. 12, 2019, 1:32 AM), https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921 [https://perma.cc/GQS3-NARY].

5. *See Wardlow*, 528 U.S. at 123–24 ("The officer must be able to articulate more than an 'inchoate and unparticularized suspicion or "hunch"' of criminal activity." (quoting *Terry*, 392 U.S. at 27)). *See generally* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 331 (2015) (analyzing the shift from traditional reasonable suspicion to "big data" enhanced policing that "undermines the protection that reasonable suspicion provides against police stops" and noting that the same reasonable suspicion standard might justify stops proscribed by predictive policing software).

6. The law allows this type of protective frisk if the officer can articulate some reason for fearing for their safety. *See Terry*, 392 U.S. at 30–31.

7. *See* Joel S. Johnson, Comment, *Benefits of Error in Criminal Justice*, 102 VA. L. REV. 237, 272–75 (2016) (discussing how the stigma of arrest attaches irrespective of guilt or conviction).

8. *See* Tracey Maclin, *When the Cure for the Fourth Amendment is Worse than the Disease*, 68 S. CAL. L. REV. 1, 56 (1994) ("[U]nreasonable searches and seizures rarely

be less enthused if the grounds for the officer's suspicion were less menacing: a conviction for theft; several delinquent parking tickets; a prior FRT identification near a crime scene a day, month, or year prior to the encounter; a student visa about to expire;[9] the person's distasteful associates on Facebook; membership in an unsavory political or religious organization; anti-establishment, anti-police, or "suspicious" social media posts; or identification as a government whistleblower. The more private and less threatening the stimulus, the more likely an objective observer is to cry foul.[10]

---

attract media attention or arouse the community—'no other constitutional guarantee is so openly flouted with so little public outcry'—that courts should not rely on 'other methods' of enforcement when the search and seizure guarantee is flouted. [Society needs a Fourth Amendment b]ecause the people who are illegally arrested and illegally searched are often despised, and because they are usually 'unrepresentative of the larger class of law-abiding citizens.'" (quoting Yale Kamisar, *Does (Did) (Should) the Exclusionary Rule Rest on a "Principled Basis" Rather than an "Empirical Proposition"?*, 16 CREIGHTON L. REV. 565, 613 (1983))).

9. It is important to note that the law allows law enforcement to stop individuals for a variety of reasons without much justification already. Harvey Gee, *Almost Gone: The Vanishing Fourth Amendment's Allowance of Stingray Surveillance in a Post-*Carpenter *Age*, 28 S. CAL. REV. L. & SOC. JUST. 409, 410 (2019). Police can stop drivers for "just about any reason under the pretext" of a traffic violation. *Id.* Individuals may "be stopped while . . . walking down the street in a 'high crime area' and checked for an active arrest warrant." *Id.* (citing *Wardlow*, 528 U.S. at 124).

10. Public outcry has been at the precipice of many developments in Fourth Amendment law, including the Fourth Amendment itself. *See, e.g.*, Buritica v. United States, 8 F. Supp. 2d 1188, 1194 (1998) (noting that a cash incentive program employed by U.S. Customs bore a "striking resemblance to British colonial practices that helped to spark the American Revolution and led to the adoption of the Fourth Amendment"); Eric Blumenson & Eva Nilsen, *Policing for Profit: The Drug War's Hidden Economic Agenda*, 65 U. CHI. L. REV. 35, 75 n.143 (1998) ("John Adams . . . wrote that *public outcry* against the writs of assistance was one of the sparks leading to American independence." (emphasis added)). When government surveillance and policing practices invade further upon "innocent" citizens' privacy rights, public outcry is amplified. *See, e.g.*, Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 322 (2016) ("[W]hen the TSA started to use x-ray machines that were too revealing of people's bodies, there was an immediate outcry and the practice was stopped."); Jonathan Weisman, *Momentum Builds Against N.S.A. Surveillance*, N.Y. TIMES (July 28, 2013), https://www.nytimes.com/2013/07/29/us/politics/momentum-builds-against-nsa-surveillance.html?pagewanted=all [https://perma.cc/5P8L-LSZ8]. However, the public also reacts negatively to the Fourth Amendment's remedy—the Exclusionary Rule. For example, when police gather evidence without following Fourth Amendment guidelines, critics have called the subsequent exclusion of the "tainted" evidence from use against the criminal defendant as a "windfall" for that defendant. *See* Margareth Etienne, *Remorse, Responsibility, and Regulating Advocacy*, 78 N.Y.U. L. REV. 2103, 2151 & n.213 (2003) (describing one case in which public pressure was exerted on a judge who followed the rule—United States v. Bayless, 913 F. Supp. 232 (S.D.N.Y.), *vacated by* 921 F. Supp. 211 (S.D.N.Y. 1996)).

This scenario should be ringing the "Big Brother" bell. In George Orwell's classic novel *Nineteen Eighty-Four*, the state reminds its citizens that "Big Brother is watching you."[11] The novel explores a dystopian future in which government surveillance is constant, and the "Thought Police" attempt to root out politically subversive citizens.[12] Themes of intrusive government surveillance and overly invasive police procedures are common in science-fiction and conspiracy-based entertainment.[13]

Facial recognition technology is no longer stuff of science fiction nor of prognostication; it is a modern reality. FRT enables cameras to scan a face, analyze its facial geometry, and compare that mathematical formulation with databases of known faces to determine a match.[14] In China, the government uses FRT to identify and fine jaywalkers and capture drivers violating traffic rules.[15] In the United States, Customs and Border Protection uses FRT at domestic airports to verify the identity of international passengers, streamlining the customs departure process.[16] For well over a decade, police departments across the country have been attaching live-scanning devices to police vehicles to read license plates and instantly identify if a vehicle is stolen, has a lapsed registration, or has delinquent parking tickets.[17]

---

11. GEORGE ORWELL, NINETEEN-EIGHTY-FOUR 2 (1949).

12. *Id.* at 59. Sophisticated artificial intelligence (AI), which can predict human behaviors based on data inputs, could become Orwell's "Thought Police." *See generally* ARMANDO VIEIRA, REDZEBRA ANALYTICS PREDICTING ONLINE USER BEHAVIOR USING DEEP LEARNING ALGORITHMS (2016), https://arxiv.org/pdf/1511.06247.pdf [https://perma.cc/9D4Q-Y2CA] (discussing how machine learning facilitates predicting people's future e-commerce behaviors).

13. *See, e.g.*, DAVID EGGERS, THE CIRCLE (2013); EAGLE EYE (K/O Paper Products 2008); ENEMY OF THE STATE (Touchstone Pictures 1998); MINORITY REPORT (20th Century Fox 2002).

14. For a detailed description of how facial recognition technology works, see *How Does Facial Recognition Work?*, NORTON BY SYMANTEC, https://us.norton.com/internet security-iot-how-facial-recognition-software-works.html [https://perma.cc/V5FZ-X7LX].

15. Christina Zhao, *Jaywalking in China: Facial Recognition Surveillance Will Soon Fine Citizens via Text Message*, NEWSWEEK (Mar. 27, 2018, 9:34 AM), https://www.newsweek.com/jaywalking-china-facial-recognition-surveillance-will-soon-fine-citizens-text-861401 [https://perma.cc/9WJ4-8FGX]. The Chinese government also equips law enforcement with FRT-enabled sunglasses, facilitating the instant identification of criminals and other targets. *Id.*

16. Michael Kirkham, *Airport Facial Recognition Technology Runs into Privacy Fears*, L.A. TIMES (Aug. 23, 2019, 5:00 AM), https://www.latimes.com/travel/story/2019-08-22/facial-recognition-biometrics-at-airports-proliferating [https://perma.cc/52U3-L4RY].

17. POLICE EXEC. RSCH. F., HOW ARE INNOVATIONS IN TECHNOLOGY TRANSFORMING POLICING? 1–2 (2012), https://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%20201

In addition to the deployment of live-scanning FRT cameras, private companies and the government are compiling immense databases of personal information at a feverous pace.[18] The FBI compiles biometric information—unique physical characteristics like DNA, fingerprints, and facial images[19]—from other law enforcement agencies and from agencies to which citizens submitted their biometric data for licensing or employment.[20] Private companies collect demographic and behavioral data to improve targeted advertising.[21] Almost 70% of Americans use Facebook,[22] which collects and shares personal information with third parties in addition to maintaining records of every activity ever conducted by its users on the site.[23] As our society continues its trend toward digitization, the personal

---

2.pdf [https://perma.cc/89PW-5YJZ]. Another technology that police departments across the country have widely deployed in the last couple of decades is the automated license plate scanner. *See* Julia M. Brooks, *Drawing the Lines: Regulation of Automatic License Plate Readers in Virginia*, 25 RICHMOND J.L. & TECH. 1, 4 (2019). License plate scanning implicates the same privacy concerns—law enforcement's ability to track the movements of individuals over time—as described by the D.C. Court of Appeals in *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010). Brooks, *supra*, at 8.

18. Richie Koch, *Massive Corporate Databases Become Government Tools of Surveillance*, PROTONMAIL (June 16, 2020), https://protonmail.com/blog/privacy-user-data-requests/ [https://perma.cc/TAV2-LJDY].

19. *See infra* notes 34–36 and accompanying text.

20. *Fingerprints and Other Biometrics*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics [https://perma.cc/LH8Y-6HUM]. The FBI categorizes these into two datasets: one set accumulated from photos acquired by law enforcement and another set of photos acquired by other governmental agencies for civil purposes. *See* Ernest J. Babcock, *Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System*, FBI, https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/interstate-photo-system [https://perma.cc/ZA9F-PSH6]. The FBI maintains a database of biometric identifiers acquired via criminal proceedings, which includes fingerprints, DNA, and photos—such as mugshots—obtained incident to arrest or pursuant to criminal investigations. *See id.* The civil database includes photos, fingerprints, and other information acquired by the government related to employment, licensing applications, and other civil processes. *Id.* Currently, the FBI prohibits law enforcement users from searching the civil database; however, individuals who have a criminal profile in the system will have their civil biometric information added to their criminal profile, making that information searchable. *Id.* There is a third database maintained by the FBI that is handled separately and with which restrictions are far less stringent: the Unsolved Photo File (UPF). *See infra* notes 79–82 and accompanying text.

21. *See* Max Freedman, *How Businesses Are Collecting Data (And What They're Doing with It)*, BUS. NEWS DAILY (June 17, 2020), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://perma.cc/B6WQ-RPVT].

22. John Gramlich, *10 Facts About Facebook*, PEW RSCH. CTR. (May 16, 2019), https://www.pewresearch.org/fact-tank/2019/05/16/facts-about-americans-and-facebook [https://perma.cc/6436-WWND].

23. Kristen Korosec, *This Is the Personal Data that Facebook Collects—And Sometimes Sells*, FORTUNE (Mar. 21, 2018, 7:32 AM), https://fortune.com/2018/03/21/facebook-personal-data-cambridge-analytica [https://perma.cc/AE9N-R8K2].

information captured within various databases will continue to grow exponentially.

The combination of improving FRT with massive databases inevitably leads to infringement upon the First Amendment rights of millions of Americans.[24] If the faces of Americans on social media become part of FRT databases used by law enforcement, American citizens will be less likely to post their images online or to use social media at all.[25] Those who wish to maintain a measure of anonymity when in public will be

---

24. *See* Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, A.B.A.: CRIM. JUST. MAG., Spring 2019, at 9, 12, https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology [https://perma.cc/8M7D-AVNN] ("Critics also have argued that FRT may implicate the First Amendment right to freedom of association and right to privacy."). Several cases have "upheld the right to anonymous speech and association," which allows individuals to advocate for minority causes without fear of retaliation. *Id*. at 13 (citing NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 466 (1958)); *see also, e.g.*, McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995); Talley v. California, 362 U.S. 60, 64 (1960).

> Without these protections, the use of FRT could have a chilling effect on individuals' behaviors and lead to self-censorship. Nevertheless, some courts have considered law enforcement's use of photography at public demonstrations as not violating the First Amendment right to freedom of association. On the other hand, specific, targeted surveillance of a group may cross the line and violate First Amendment association protections. For example, the Second Circuit in *Hassan v. City of New York* determined that the NYPD's targeted use of pervasive video, photographic, and undercover surveillance of Muslim Americans may have caused those individuals "direct, ongoing, and immediate harm," and it may have created a chilling effect. Privacy advocates have been particularly critical of the use of FRT in widespread surveillance. The FRT program that was used to monitor the protestors in Baltimore during the Freddie Gray protests were widely criticized for many reasons, including a fear that African Americans were overrepresented in the facial recognition repository.

Hamann & Smith, *supra*, at 13 (citations omitted) (first citing Laird v. Tatum, 408 U.S. 1 (1972); Phila. Yearly Meeting of Religious Soc'y of Friends v. Tate, 519 F.2d 1335, 1337–38 (3d Cir. 1974); Donohoe v. Duling, 465 F.2d 196, 202 (4th Cir. 1972); then citing Hassan v. City of New York, 804 F.3d 277, 292 (3d Cir. 2015)).

25. The Supreme Court has recognized the importance of social media as an essential tool for the exchange of views and ideas in today's internet-connected world. *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017). "In short, social media users employ these websites to engage in a wide array of protected First Amendment activity on topics 'as diverse as human thought.'" *Id.* at 1735–36 (quoting Reno v. ACLU, 521 U.S. 844, 870 (1997)). However, social media platforms themselves affirmatively act to allow or disallow user-posted content, limiting some expression. *See* VALERIE C. BRANNON, CONG. RSCH. SERV., R45650, FREE SPEECH AND THE REGULATION OF SOCIAL MEDIA CONTENT 1–2 (2019). For an in-depth analysis regarding Congress's ability to regulate such decisions by social media platforms, like Facebook, see generally *id.*

unable to do so if their photo is online or they provided it to a government agency.[26] More importantly, critics of the government could abstain from public speech knowing that every detail of their identity would be known merely by exposing their face. The chilling effect on First Amendment rights is reason enough for lawmakers to deem FRT's use by law enforcement unconstitutional.

Unfortunately, the courts are unlikely to bar law enforcement's use of FRT on the American public. Under current Supreme Court Fourth Amendment doctrine, the Court probably would not classify FRT scans as searches.[27] The ability to challenge a search under the Fourth Amendment rests on whether an individual had a reasonable expectation of privacy in a particular location.[28] In public, a person's reasonable expectation of privacy is almost non-existent.[29] Moreover, even if courts' conception of the Fourth Amendment shifts, the judiciary cannot move quickly enough to prevent unprecedented privacy invasions because the courts are ill-equipped to keep up with new technological developments.[30] Thus, to prevent FRT from eroding the privacy rights of most Americans, Congress must enact federal legislation that directly addresses FRT.[31]

New legislation, instead of the judicial process, offers a more streamlined route to addressing law enforcement's use of FRT. Relying on the legislative process to address emerging issues presents political challenges. However, it offers an avenue to protection that does not require years of litigation. Legislation that considers FRT is sparse, but some states have passed laws to address aspects of its use.[32] However, there is no all-encompassing legislative provision that addresses FRT head on. To limit law enforcement's development of databases that include the faces of

---

26. The government requires individuals to submit photographs of their faces for a wide range of services and for some basic rights. Driver's licenses are the most obtained form of identification, which over 87% of Americans had as of 2009. *Our Nation's Highways: 2011*, FED. HIGHWAY ADMIN., https://www.fhwa.dot.gov/policyinformation/pubs/hf/pl11028/chapter4.cfm [https://perma.cc/DTJ5-366Q] (last updated Nov. 7, 2014). To obtain a passport—required for international travel—an American citizen is required to provide a photo to the State Department. *See Photo Identification*, U.S. DEPT. ST., https://travel.state.gov/content/travel/en/passports/how-apply/identification.html [https://perma.cc/4J8N-6RT3].

27. *See infra* Part V. At least as far as the Fourth Amendment is currently conceptualized, the Court's rationale does not provide a clear path to barring FRT.

28. Minnesota v. Carter, 525 U.S. 83, 88–89 (1998); *see also* Minnesota v. Olson, 495 U.S. 91, 100 (1990) (extending Fourth Amendment protection to an overnight guest).

29. *See* Katz v. United States, 389 U.S. 347, 351 (1967); *see also infra* Section V.B.1.

30. *See infra* Section V.C.

31. *See infra* Part VI.

32. *See infra* Part IV.

most Americans, to provide some modicum of protection for public anonymity, and to protect the privacy of the innocent, Congress must act.

This Comment implores Congress to limit the development of law enforcement FRT databases. In Part II, the Comment describes facial recognition technology, examining its development and uses. This section describes how law enforcement compiles databases of faces. It concludes by exploring potential future applications of the technology. Part III discusses the privacy rights angle, answering why the American population should be concerned about—and why legislators should act to prevent—unchecked FRT-equipped law enforcement.

Part IV addresses the current statutory framework that governs law enforcement's use of FRT. In this section, the Comment points out the general lack of enacted legislation regarding the use of biometric information by law enforcement. The analysis shows that current statutory law is blind to the potential abuses of FRT-equipped law enforcement agencies, making the technology ripe for exploitation.

In Part V, the Comment reviews Fourth Amendment jurisprudence and its applicability to FRT. Further, this section examines Supreme Court Fourth Amendment jurisprudence and concludes that recent decisions indicate that the Court would be unlikely to hold law enforcement's uninhibited use of FRT unconstitutional. The section concludes that relying on the courts to protect citizens from technology's encroachment on Fourth Amendment rights will result in millions of Americans losing privacy rights, even if the Court eventually changes its conception of what the Fourth Amendment protects.

Part VI proffers a legislative solution to directly address FRT's use by law enforcement. The solution requires congressional action that addresses privacy concerns while still allowing law enforcement to use the cutting-edge technology. The proposed solution has two primary prongs: first, amending the U.S. Code to limit the authorization of the FBI's collection and compilation of facial images to those obtained by law enforcement and correctional entities; second, proposing a new law that vests responsibility for the collection of non-criminal identification information in the Department of Health and Human Services, or another non-law enforcement agency.

II. HOW FRT FUNCTIONS AND LAW ENFORCEMENT'S USE OF BIOMETRIC IDENTIFIERS

A. FRT Basics

Understanding the intricacies of how FRT functions is a critical step towards determining how to regulate its use as a law enforcement search tool. Thinking of FRT as a tool that enhances an officer's natural ability to pick people out of a crowd oversimplifies the issue. FRT is a mechanism that gives law enforcement the power to analyze biometric information of potential suspects in real-time or retrospectively.[33]

1. Biometrics

The Department of Homeland Security (DHS) defines biometrics as "unique physical characteristics, such as fingerprints, that can be used for automated recognition."[34] In addition to fingerprints, biometric identifiers include "DNA, irises, voice patterns, palm prints, and facial patterns."[35] Law enforcement collects this information and submits it to the FBI; the FBI then stores this information in various databases and makes it accessible to law enforcement on a local level.[36] Much like matching DNA records obtained at a crime scene to the DNA of the perpetrator, obtaining the data necessary to run an FRT search involves a complex process to obtain matches.

---

33. *See* Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 429–30 (2014).

34. *Biometrics*, U.S. DEP'T HOMELAND SEC. (July 13, 2020), https://www.dhs.gov/biometrics [https://perma.cc/ZSY6-LLSF].

35. *Fingerprints and Other Biometrics*, *supra* note 20.

36. *Id.* The FBI maintains several databases dedicated to particular types of biometric identification information and has a lengthy history of providing that information to other law enforcement agencies. *See id.* Next Generation Identification is an FBI system geared towards identifying people by their fingerprints, palm prints, irises, and faces. *Id.* The Combined DNA Index System (CODIS) "allows labs to exchange and compare DNA profiles to link" criminals to DNA evidence found in new investigations. *Id.* The Foreign Biometric Exchange (FBE) Program "collect[s] high value biometrics obtained from foreign law enforcement partners [relating to] individuals of interest to partner countries, the United States, or the international law enforcement community, and include individuals associated with or appropriately suspected of terrorist activity, egregious crimes, or transnational criminal activity." *Id.* The Preventing and Combating Serious Crime (PCSC) Initiative requires partner nations, as part of the Visa Waiver Program, "to enter into a PCSC agreement to share criminal and terrorist biometrics with the U.S. The Criminal Justice Information Services Division acts as the technical implementer for the Department of Justice to provide connectivity between U.S. and partner nation biometric systems." *Id.*

2. How FRT Works

Identifying a person with FRT begins with a scan that produces an image.[37] From that image, the FRT system must first recognize that a face is present.[38] Once the system identifies a face, FRT software creates a "faceprint."[39] A faceprint is a numerical code generated by mapping distinguishable facial landmarks, such as the distance between the eyes, the width of the nose, the depth of eye sockets, the shape of the cheekbones, and the length of the jawline.[40] Alternatively, software can generate a faceprint by analyzing the attributes of the skin, such as texture, lines, or by mapping pore locations.[41] This faceprint is then cross-referenced with a database of known faces to identify a match.[42] The software is capable of mapping faces from both photographs or videos, which could be recorded or live-streamed.[43]

3. FRT Shortcomings & Criticisms

One major criticism of FRT is that it cannot consistently identify women and people of color accurately.[44] FRT identifies white males at a

37. *See* Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, HOWSTUFFWORKS, https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition1.htm [https://perma.cc/73A3-D2ZY]. For a brief facial recognition demonstration, see *How Does Facial Recognition Work?*, NBC NEWS (Aug. 21, 2019), https://www.nbcnews.com/now/video/how-does-facial-recognition-work-66901573848 [https://perma.cc/NQ3F-52GS].

38. *See* Bonsor & Johnson, *supra* note 37.

39. *Id*.

40. *Id.*

41. Brown, *supra* note 33, at 427.

42. Bonsor & Johnson, *supra* note 37.

43. *See* Brown, *supra* note 33, at 429–30. Several law enforcement agencies are working with private companies to rapidly analyze "live footage from closed-circuit surveillance cameras." *Id.* at 430. New York City, the District of Columbia, Los Angeles, and some Florida police departments are pursuing enhanced live-video FRT capabilities. *Id.*

44. *See, e.g.*, Queenie Wong, *Why Facial Recognition's Racial Bias Problem Is So Hard to Crack*, CNET (Mar. 27, 2019, 5:00 AM), https://www.cnet.com/news/why-facial-recognitions-racial-bias-problem-is-so-hard-to-crack [https://perma.cc/44PJ-KDNX] (40% of identification errors made by Amazon's facial recognition tool, used by law enforcement, involved people of color). Journalists and scholars have made this FRT issue a well-documented one. *See, e.g.*, Drew Harwell, *Facial Recognition Technology Is Finally More Accurate in Identifying People of Color. Could That Be Used Against Immigrants?*, WASH. POST (June 28, 2018, 6:56 AM), https://www.washingtonpost.com/technology/2018/06/28/facial-recognition-technology-is-finally-more-accurate-identifying-people-color-could-that-be-used-against-immigrants [https://perma.cc/R6RM-K69C]; Steve Lohr, *Facial Recognition*

99% accuracy rate.[45] In contrast, when the target of identification is a dark-skinned woman, the accuracy rate drops to 65%, making it only slightly more effective than a coin flip.[46] In addition to difficulties with identifying people of color, FRT has also produced a significantly higher false-positive identification rate with darker-skinned people.[47] If police use FRT that is deficient in this way, not only will it be ineffective, but it will also result in the inadvertent targeting of innocents—and particularly innocents within the minority population—who are incorrectly identified during law enforcement investigations.[48] Even more concerning is the likelihood that police officers will trust the technology over their own intuition.[49] FRT's identification and false-positive issues begin with the training of the FRT software.[50]

Is Accurate, if You're a White Guy, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [https://perma.cc/9N5D-AFZU].

45. Lohr, *supra* note 44.

46. *Id.*

47. *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1, 9 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf [https://perma.cc/CQT5-VSL8]. In analyzing the ability of three commercially available facial recognition software systems in identifying gender, the false positive rate for light-skinned men and women was between 0% and 1.6%; for dark-skinned women, the false positive rate was between 15.8% and 22.2%. *Id.*

48. *See* Jon Sharman, *Metropolitan Police's Facial Recognition Technology 98% Inaccurate, Figures Show*, INDEP. (May 13, 2018, 1:07 PM), https://www.independent.co.uk/news/uk/home-news/met-police-facial-recognition-success-south-wales-trial-home-office-false-positive-a8345036.html [https://perma.cc/F3QR-2X7E]. The United Kingdom's largest police force used FRT to a 98% false positive rate. *Id.* Of the 104 alerts, only two were accurate. *Id.*

49. Many people can relate to the idea of over-trusting technology because, generally, it produces more accurate results than we can ourselves. *See, e.g.*, Kalev Leetaru, *Why Do We Trust GPS More than We Trust Ourselves?*, FORBES (Apr. 30, 2016, 10:13 AM), https://www.forbes.com/sites/kalevleetaru/2016/04/30/why-do-we-trust-gps-more-than-we-trust-ourselves/#6c92c33b2c42 [https://perma.cc/MAH3-KMPG] (relaying a story about a construction company that demolished the wrong house because Google Maps sent its workers there). Map applications on our mobile devices are merely one example of how this affects us, but there a myriad of other instances exist where we rely on technology to our potential detriment. We rely on spell check to ensure our documents and emails are not littered with typos; we rely on Google to tell us the opening and closing hours of stores and restaurants. When technology fails us, it is generally a frustrating experience. However, if FRT fails in its policing application, the ramifications could be life altering.

50. Joy Buolamwini, *How I'm Fighting Bias in Algorithms*, TED (Nov. 2016), https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms/transcript [https://perma.cc/3NFW-F2ZK].

FRT software is a kind of artificial intelligence (AI) that learns over time, "incorporate[ing] real-world experience in its decision making."[51] FRT programmers train the AI that maps and matches faces using "deep learning networks."[52] This process involves exposing the AI to large data sets, broken up into smaller chunks, repetitively.[53] Over time, the AI learns from feedback given to it by software engineers when it correctly or incorrectly makes an identification.[54]

Programmers train FRT systems by feeding datasets containing images of faces and non-faces to AI so that it can learn what is and what is not a face.[55] When the set of faces used to train the AI lacks diversity—for example, if databases used to train FRT AI contain mostly lighter-skinned faces[56]—the AI does not learn to differentiate a dark-skinned face from a non-face.[57] Exacerbating the bias created in FRT AI in its applications to policing is the fact that the databases used by law enforcement—mostly from mugshots—have a disproportionate composition of African American

---

51. Darrell M. West, *What Is Artificial Intelligence?*, BROOKINGS (Oct. 4, 2018), https://www.brookings.edu/research/what-is-artificial-intelligence/ [https://perma.cc/7HSR-QV7Y]. AI systems simulate human responses to stimuli, "given the human capacity for contemplation, judgment, and intention." *Id.* "[T]hese software systems 'make decisions which normally require [a] human level of expertise' and help people anticipate problems or deal with issues as they come up." *Id.*

52. *See* Matt Shipman, *New Technique Cuts AI Training Time by More than 60 Percent*, N.C. ST. U. (Apr. 8, 2019), https://news.ncsu.edu/2019/04/new-technique-cuts-ai-training-time-by-more-than-60-percent [https://perma.cc/F736-KSPP].

> Deep learning networks are at the heart of AI applications used in everything from self-driving cars to computer vision technologies," says Xipeng Shen, a professor of computer science at NC State and co-author of a paper on the work. [¶] "One of the biggest challenges facing the development of new AI tools is the amount of time and computing power it takes to train deep learning networks to identify and respond to the data patterns that are relevant to their applications.

Id.

53. *Id.*

54. *See* Buolamwini, *supra* note 50.

55. *Id.*

56. *See* Rachel Siegel, *Rashida Tlaib Isn't the Only One Who Thinks Race Biases Facial Recognition Results*, WASH. POST (Oct. 4, 2019, 2:27 PM), https://www.washingtonpost.com/technology/2019/10/04/rashida-tlaib-isnt-only-one-who-thinks-race-biases-facial-recognition-results [https://perma.cc/V8NP-PQEX]. Programmers are probably not creating bias in AI intentionally. Instead, the issue is that the racial disparity in the facial images used for training FRT systems could mirror the demographic makeup of the country; over three-quarters of the American population is white, and less than 14% identify as solely black or African American. *See QuickFacts*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/fact/table/US/PST045218 [https://perma.cc/7P94-46H8].

57. *See* Buolamwini, *supra* note 50.

faces.[58] Thus, the databases of faces used to train FRT differ significantly from criminal facial databases. Although this issue is problematic, fixing it only requires that programmers train FRT systems with a higher proportion of women and minority faces. However, even if programmers eliminate racial and gender bias from FRT systems, issues regarding the source of facial images in FRT databases remain.

FRT databases consist of faces from a variety of sources. Technology companies have compiled databases of faces to train their FRT AI to improve its recognition capabilities.[59] Once these datasets have been assembled and distributed, the datasets likely exist in perpetuity.[60] Companies compile datasets by pulling publicly available photos from photo-sharing websites, social media,[61] dating services, and surveillance

58. *See* Lohr, *supra* note 44 (noting that African Americans make up a disproportionate percentage of mugshot databases).

59. Cade Metz, *Facial Recognition Tech Is Growing Stronger, Thanks to Your Face*, N.Y. TIMES (July 13, 2019), https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html [https://perma.cc/QMX3-GVX5]. Microsoft deleted its massive database of approximately 10 million images because government regulation of FRT fell short of Microsoft's standards. *Microsoft Deletes Massive Face Recognition Database*, BBC NEWS (June 7, 2019), https://www.bbc.com/news/technology-48555149 [https://perma.cc/SJQ4-TWXB] ("The deletion comes after Microsoft called on US politicians to do a better job of regulating recognition systems."). Microsoft has been leading the charge in calls to more closely regulate FRT because of its "potential . . . to erode civil liberties." *See* Nicole Lindsey, *Microsoft Deletes Massive Facial Recognition Database*, CPO MAG. (July 2, 2019), https://www.cpomagazine.com/data-privacy/microsoft-deletes-massive-facial-recognition-database/ [https://perma.cc/H7MF-LGLG]. *But see* Melissa Locker, *Microsoft, Duke, and Stanford Quietly Delete Databases with Millions of Faces*, FAST CO. (June 6, 2019), https://www.fastcompany.com/90360490/ms-celeb-microsoft-deletes-10m-faces-from-face-database [https://perma.cc/YE3L-KJ8Q] ("While it's good that someone is stepping up to lead, don't hurt your hands applauding Microsoft too hard. The company may claim it wants regulations for facial recognition, but it also wants to use facial recognition technology to sell you stuff at Kroger through Minority Report-like ads—and it has eluded privacy-related scrutiny for years.").

60. *Id.*

61. Facebook presents unique issues. Seven in ten American adults use Facebook. Gramlich, *supra* note 22. Facebook claims its facial recognition is accurate 97.35% of the time. Yaniv Taigman et al., *DeepFace: Closing the Gap to Human-level Performance in Face Verification*, 2014 PROC. IEEE CONF. COMPUT. VISION & PATTERN RECOGNITION 1701, 1701, 1705–06 (2014), https://research.fb.com/wp-content/uploads/2016/11/deepface-closing-the-gap-to-human-level-performance-in-face-verification.pdf [https://perma.cc/8HLZ-AJXR]. Facebook users are familiar with Facebook's version of FRT: whenever they post pictures of or with other users when the platform suggests "tagging" the other person in the photo or when Facebook notifies a user that they may be in a photo posted by someone else. *See* Srinivas Narayanan, *An Update About Face Recognition on Facebook*, FACEBOOK (Sept. 3, 2019), https://newsroom.fb.com/news/2019/09/update-face-recognition [https://perma.cc/7G86-QE65]. However, on September 3, 2019, Facebook changed how it implements its FRT, allowing users to opt-in. *Id.* The unparalleled extent of Facebook's userbase, all with pictures, combined with Facebook's exceptional facial recognition capabilities—notably, the large dataset of photographs likely shortened the learning curve for Facebook

systems.[62] In other words, private companies use the faces of American citizens without their consent to strengthen their FRT systems.[63] Although many of these private companies have declined to provide these databases to law enforcement agencies amid privacy concerns,[64] at least one company has sold its FRT system and database of faces to hundreds of American law enforcement agencies recently.[65] In lieu of commercially available databases, law enforcement has assembled FRT databases of its own.

AI—gives it immense influence on FRT's future development. *See* April Glaser, *Facebook's Face-ID Database Could Be the Biggest in the World. Yes, It Should Worry Us*, SLATE (July 9, 2019, 7:20 PM), https://slate.com/technology/2019/07/facebook-facial-recognition-ice-bad.html [https://perma.cc/6B4H-ZRYN]. Facebook vows that it will not share its FRT and has designed its FRT template so that other FRT software cannot use it. *Id.* However, until it is legally bound to keep its FRT in-house, it is under no legal obligation to do so. Political winds may shift in such a way that Facebook decides to share its FRT or grant access to its databases to law enforcement or other organizations wishing to exploit the technology for gain, politically or otherwise.

62. Metz, *supra* note 59.

63. *See id.*

64. Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/4UM4-3LUC].

> Until now, technology that readily identifies everyone based on his or her face has been taboo because of its radical erosion of privacy. Tech companies capable of releasing such a tool have refrained from doing so; in 2011, Google's chairman at the time said it was the one technology the company had held back because it could be used "in a very bad way."

Id.

65. *See id.* Clearview AI developed an app that can find other publicly posted images of an individual from one provided. *Id.* The system includes over three billion facial images, taken from sources like "Facebook, YouTube, Venmo, and millions of other websites." *Id.* "[M]ore than 600 law enforcement agencies have started using Clearview in the past year." *Id.* Law enforcement has utilized the "app to help solve shoplifting, identity theft, credit card fraud, murder and child sexual exploitation cases." *Id.* More frightening still, Clearview can monitor law enforcement's use of the app—allowing it to look in on who police officers are targeting. *Id.* However, the company has recently been named as a defendant in several legal actions, including a class action complaint for "collecting, storing and using their and other similarly situated individuals' biometric identifiers and biometric information without informed written consent in direct violation of Illinois' Biometric Information Privacy Act (BIPA)." Kirsten Errick, *Clearview AI Faces Fourth Lawsuit in a Month*, LAW ST. (Feb. 14, 2020), https://lawstreetmedia.com/tech/clearview-ai-faces-fourth-lawsuit-in-a-month/ [https://perma.cc/D34L-CSY4] (quoting Class Action Complaint at 1–2, Calderon v. Clearview AI, Inc., No. 20-cv-01296, (S.D.N.Y. Feb. 13, 2020), ECF No. 1).

B. Law Enforcement's Compilation of Biometric Data

Law enforcement databases are estimated to contain the faces of 117 million Americans, about half of the American adult population.[66] The DHS biometric identification system—the Automated Biometrics Identification System or IDENT—contains over 260 million identities and processes hundreds of thousands of biometric identifications every day.[67] However, the most significant player in biometrics and facial recognition within the law enforcement community is the FBI.

1. The FBI's Biometric Identification Data and Systems

The FBI has a long history of maintaining databases of biometric identifiers. Most notably, the FBI assumed management of the national fingerprint collection in 1924.[68] The FBI developed the collection of fingerprints into the Integrated Automated Fingerprint Identification System (IAFIS), which became the world's largest "person-centric" database.[69] The FBI shares fingerprint data with local, federal, and international criminal justice agencies.[70]

Recently, the FBI developed its Next Generation Identification System (NGI).[71] NGI boasts the "largest and most efficient electronic repository of biometric and criminal history information."[72] This system has two components related to FRT. First, the Interstate Photo System (IPS) is the FBI's database of face records; the source of the photos are FBI files and "bulk submissions" from state repositories.[73] Second, the Facial Recognition Search allows law enforcement to search that database to generate matches.[74]

---

66. Claire Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org [https://perma.cc/2DMW-2G9P].

67. *Biometrics*, *supra* note 34.

68. *Fingerprints and Other Biometrics*, *supra* note 20.

69. *Next Generation Identification (NGI)*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi [https://perma.cc/Q94M-X726].

70. *Does the FBI Exchange Fingerprint or Arrest Information with Domestic and Foreign Police Agencies?*, FBI, https://www.fbi.gov/about/faqs/does-the-fbi-exchange-fingerprint-or-arrest-information-with-domestic-and-foreign-police-agencies [https://perma.cc/PR95-SEXS].

71. *See* Timothy O. Lenz, *21st-Century Developments in Fourth Amendment Privacy Law*, *in* 1 PRIVACY IN THE DIGITAL AGE: 21ST-CENTURY CHALLENGES TO THE FOURTH AMENDMENT 267, 293 (Nancy S. Lind & Erik Rankin eds., 2015). "The FBI maintains that its efforts to develop the [NGI] is driven by technology, customer (that is, police department) requirements, and growing demand for [IAFS] services." *Id*.

72. *Next Generation Identification (NGI)*, *supra* note 69.

73. *Id.*

74. *Id.*

The details of the source of the photos within the IPS are unclear. The FBI maintains separate databases of photos obtained by criminal and civil means.[75] The criminal database consists of arrest records—at state, local, and federal levels—and biometric information obtained at crime scenes and related to missing or unidentified persons.[76] The civil database holds biometric information obtained from military service records, immigration applications, background checks, and licensing applications for many job types, required in some states to be a "dentist, accountant, teacher, geologist, realtor, lawyer, or optometrist."[77] Civil photos associated with individuals in the criminal database are added to that individual's profile, making those civil photos searchable.[78] However, the FBI only authorizes law enforcement agencies to search the criminal database and refuses access to the civil database.[79] Nonetheless, the civil photos may find their

75. Ernest J. Babcock, *Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System*, FBI, https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/interstate-photo-system [https://perma.cc/ZA9F-PSH6].

76. 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 [https://perma.cc/764U-YV96].

77. *Id.*

78. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY 11 (2016), https://www.gao.gov/assets/680/677098.pdf [https://perma.cc/YRB9-C5TW].

79. *Id.* at 12 & n.29; *see also* Babcock, *supra* note 75. According to FBI officials, the FBI "only allows users to conduct face recognition searches in the criminal identities part of the database; no searches are permitted in the civil identities part of the database." U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-267, *supra* note 78, at 12. However, there is another database, the Unsolved Photo File (UPF), that contains photos of subjects of criminal investigations with no known identity match. Babcock, *supra* note 75. The addition of the UPF is a relatively new addition to the FBI's databases of faces. *See id.* "[T]he FBI concedes that civil photos are searched against the unsolved photo file, where photos of unknown perpetrators of 'felony crimes against persons' are stored." Elizabeth Snyder, *"Faceprints" and the Fourth Amendment: How the FBI Uses Facial Recognition Technology to Conduct Unlawful Searches*, 68 SYRACUSE L. REV. 255, 260 (2018) (citing Babcock, *supra* note 75).

> An additional search capability the FBI is exploring for NGI-IPS is the inclusion of the Unsolved Photo File (UPF). While not enrolled in the civil or criminal databases, the NGI-IPS Policy and Implementation Guide states that authorized law enforcement users, such as states, may place probe photos of an unknown individual that is lawfully obtained as part of an authorized criminal investigation of a felony in a separate part of NGI-IPS, called the unsolved photo file. However, as of August 2015, CJIS has not enabled this feature in NGI-IPS.

U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-267, *supra* note 78, at 12 n.29.

way into search results through some limited exceptions, loopholes, and manipulation of the FBI's interconnected systems.[80]

Another prong of the FBI's NGI system is its Facial Analysis, Comparison, and Evaluation (FACE) Services Unit.[81] The FACE unit runs provided images through FRT software and compares images against databases of face photos.[82] Notably, FACE does not limit its searches to the NGI-IPS database.[83] It searches other federal databases, including the Department of State's Visa Photo File, Automated Biometric Identification System, and Passport Photo File.[84] It also searches state repositories, including DMV records, mugshots, and correctional photos.[85] Federal law authorizes law enforcement's access to all of these sources.[86] Nonetheless, accessing these sources for criminal searches appears to run afoul of the FBI's standard of making its NGI-IPS civil database unsearchable. This marks a contradiction within the FBI's compartmentalization policy,[87] highlighting an issue with a self-policing law enforcement agency.

Furthermore, the FBI's facial recognition capabilities are far from perfect. "Simply stated, the most advanced and sophisticated user or facial-recognition technology could not validate the accuracy of the system."[88] The system has an 86% rate of correct identification when requesting fifty

---

80. The FBI claims that when a UPF search results in a match with a photo in its civil database, the "response will be suppressed in most instances and the law enforcement officer [who submitted the photo to the UPF] will not receive the candidate photo." Babcock, *supra* note 75. This policy is vague and contradictory. It creates privacy concerns and a question as to whether the FBI maintains separately administrated databases. For example, if an agent submits a photo to the FBI and the initial search draws no results from the known criminal database, the agent could then submit the photo for addition to the UPF. The administrator of the UPF would then compare the submitted image to those within the civil database. The FBI claims that it suppresses a response because "searches generally do not return civil photos." *Id.* This contradictory explanation seems to allow the FBI to provide identification to the submitting agent if the search returns a match. The logic is circular: the FBI will not return a match if there is no match.

81. *Facial Recognition Technology: Ensuring Transparency in Government Use: Hearing Before the H. Oversight & Reform Comm.*, 116th Cong. (2019) [hereinafter *Hearing*] (statement of Kimberly J. Del Greco, Deputy Assistant Director, Crim. Just. Info. Servs. Div., FBI), https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use [https://perma.cc/K2DW-BXCP].

82. *Id.*

83. *Id.* Notably, most photos searchable by FACE are civil photos. *See* Snyder, *supra* note 79, at 260.

84. *Hearing*, *supra* note 81 (statement of Kimberly J. Del Greco).

85. *Id.*

86. *Id.*; *see also* Driver Privacy Protection Act, 18 U.S.C. § 2721(b)(1); 28 U.S.C. §§ 533 & 534; 42 U.S.C. § 3771; 28 C.F.R. § 0.85 (2019).

87. *See generally* Babcock, *supra* note 75 (detailing the FBI's policy on restricting searches in the civil database).

88. ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 97 (2017).

potential matches.[89] The FBI has not, however, indicated the rate of false positives produced by its system.[90] Although a failure to identify a match 14% of the time is problematic, the potential for incorrect identification presents even greater risks.

The FBI's internal policies are the agency's only limitations regarding which databases are subject to search. Self-policing measures open wide the potential for privacy invasions; the FBI exacerbates this vulnerability by making exceptions to its internal privacy protection policies.[91] For example, the FBI allows law enforcement requests to run FRT searches through the FBI's non-criminal database for certain images when identification is problematic.[92] The privacy concerns related to tapping into state DMV records and other civil databases are readily apparent for all Americans.

2. State DMV Records

Allowing law enforcement access to DMV records without significant hurdles creates privacy concerns for the majority of American adults. State DMV databases contain photographs of most American adults,[93] and Congress has afforded law enforcement almost limitless access to these state databases.[94] Twenty-one states and the District of Columbia allow federal agencies to access their driver's license photo databases.[95] The

89. U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-579T, FACE RECOGNITION TECHNOLOGY: DOJ AND FBI HAVE TAKEN SOME ACTIONS IN RESPONSE TO GAO RECOMMENDATIONS TO ENSURE PRIVACY AND ACCURACY, BUT ADDITIONAL WORK REMAINS 14 (2019), https://www.gao.gov/assets/700/699489.pdf [https://perma.cc/2D76-CT8Z] (statement of Gretta L. Goodwin, Director Homeland Security & Justice). Requesting fewer than fifty matches results in a lower success rate, because the system might exclude the correct match from results. *Id.*

90. *Id.* The report indicates that false positives waste law enforcement time and resources. *Id.* Moreover, the report admits that false positives could result in violations of the civil liberties of U.S. citizens. *Id.*

91. *See supra* notes 79–88 and accompanying text.

92. *See supra* note 80.

93. *See* I. Wagner, *Total Number of Licensed Drivers in the U.S. in 2018, by State*, STATISTA (Feb. 26, 2020), https://www.statista.com/statistics/198029/total-number-of-us-licensed-drivers-by-state/ [https://perma.cc/G5E4-JGQX] ("In 2018, there were about 227.5 million licensed drivers in the United States."); *see also Our Nation's Highways: 2011*, *supra* note 26.

94. *See, e.g.*, 18 U.S.C. § 2721 (allowing federal law enforcement agents to obtain information—such as driver's license photos—from state DMV records).

95. Drew Harwell, *FBI, ICE Find State Driver's License Photos Are Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019, 12:54 PM), https://www.

FBI and Immigration and Customs Enforcement (ICE) have established working relationships with state DMV officials to more easily obtain access to their license-holders' information.[96] Access is granted without formal process, authorization from the state legislature, or the consent of the individual driver's license holder.[97] The FBI's access to these DMV records has effectively expanded the FBI's searchable database of faces to 641 million photos.[98]

Law enforcement typically taps into these databases when it has obtained an image of an unidentified suspect.[99] When they have a clear image of a suspect, they are able to ascertain the subject's identity and pursue that lead.[100] Law enforcement has used FRT with DMV records to solve even low-level offenses, such as stolen checks and petty theft.[101] ICE takes advantage of lax state regulations to gain access to records contained in DMV databases.[102] Because many states allow undocumented immigrants to obtain driver's licenses or driving privilege cards issued by the local DMV,[103] ICE is able to use these state records to target individuals

---

washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches [https://perma.cc/3MGZ-53DA].

96. *Id.* However, some states have enacted legislation to prevent ICE from getting this kind of direct access to state DMV records. *See, e.g.*, Noelle C. Evans, *New State Law Safeguards Against ICE Facial Recognition Searches Through DMV Databases*, WXXI NEWS (July 9, 2019), https://www.wxxinews.org/post/new-state-law-safeguards-against-ice-facial-recognition-searches-through-dmv-databases [https://perma.cc/5N3D-4G6B] (discussing New York state's Green Light Law, also called the Driver's License Access and Privacy Act, which went into effect on December 16, 2019).

97. Harwell, *supra* note 95. State DMV officials often grant the FBI access to the DMV databases with nothing more than an email. *Id.* From 2011 to mid-2019, the FBI has logged more than 390,000 facial recognition searches using state DMV databases. *Hearing*, *supra* note 81 (statement of Kimberly J. Del Greco).

98. U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-579T, *supra* note 89, at 5–6 (statement of Gretta L. Goodwin, Director Homeland Security & Justice).

99. *See* Lynch, *supra* note 76.

100. *See* 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 [https://perma.cc/G2HZ-LTE5]. However, when the images are unclear, FRT has proven ineffective for some departments. *Id.* (describing FRT as "no magic bullet" because "only a small percentage of [FRT] queries break open investigation of unknown subjects").

101. Harwell, *supra* note 95.

102. *See* Acacia Coronado, *New York Bill Would Grant Undocumented Immigrants Driver's Licenses*, WALL ST. J. (June 16, 2019, 5:34 PM), https://www.wsj.com/articles/new-york-bill-would-grant-undocumented-immigrants-drivers-licenses-11560603600 [https://perma.cc/HG3E-JE6A].

103. *See* Harwell, *supra* note 95. The benefits of licensing undocumented immigrants extend to the states and American citizens. Recurring fees generate millions of dollars in revenue. *See* Coronado, *supra* note 102. Licensing undocumented immigrants also reduces the obstacles for obtaining car insurance. *See id.* Combined with the legality of driving,

who are illegally in the country. ICE runs facial recognition searches through DMV databases of some of these states.[104] Making the voluntarily provided information and photographs available to ICE deters immigrants from obtaining a driver's license.[105] Moreover, policies that operate as a bait and switch—offering undocumented immigrants driving privileges and then providing their voluntarily provided personal information to assist in their deportation—breach the trust of those who, in good faith, obtained identification.[106]

C. Law Enforcement's Use of FRT

1. Current Use of FRT by Law Enforcement Agencies

State and federal law enforcement agencies use FRT for a variety of identification purposes. DHS uses biometrics to regulate immigration, enforce federal laws, and verify visa applicants.[107] The FBI uses FRT to ascertain the identity of unknown criminal actors whose images law enforcement obtained pursuant to investigations.[108] ICE uses FRT to find those who have remained in the country illegally.[109] Customs and Border

---

allowing undocumented immigrants to obtain insurance results in fewer hit-and-run accidents. *See id.*

104. Harwell, *supra* note 95. Vermont, Utah, and Washington have granted access to ICE agents, and all three states offer identification to undocumented immigrants. *Id.*

105. *See supra* note 103 and accompanying text.

106. Harwell, *supra* note 95 ("The state has told [undocumented immigrants], has encouraged them, to submit that information. To me, it's an insane breach of trust to then turn around and allow ICE access to that[.]").

107. *Biometrics*, *supra* note 34. The House of Representatives Committee on Homeland Security has expressed concerns regarding the privacy implications of DHS's use of FRT. *See About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies: Hearing Before the Comm. on Homeland Sec.*, 116th Cong. (2019), https://homeland.house.gov/imo/media/doc/071019BGTOpenStatement.pdf [https://perma.cc/MD8D-4K6R] (statement of Chairman Bennie G. Thompson).

108. *See* Lynch, *supra* note 76. Lynch identifies three reasons for the use of FRT:

> First, a system may be set up to *identify* an unknown person. For example, a police officer would use this type of system to try to identify an unknown person in footage from a surveillance camera. The second type of face recognition system is set up to *verify the identity* of a known person. Smartphones rely on this type of system to allow you to use face recognition to unlock your phone. A third type, which operates similarly to a verification system, is designed to *look for multiple specific, previously-identified faces*.

Id.

109. *See* Coronado, *supra* note 102.

Protection (CBP) uses it to verify who is entering and exiting the country.[110] Most law enforcement agencies are using FRT retroactively—to identify a subject after their image has been captured.[111] However, law enforcement has begun to employ FRT "live" under certain circumstances.[112] CBP has begun to use live FRT in airports and at the border.[113] It is the live application of FRT that previews the extensive potential applications of the technology by law enforcement.

China is implementing a series of FRT measures to track and assess[114]

---

110. *See* Christopher Reynolds, *At Some Airports, Your Face Is Your ID. But Does That Put Your Privacy at Risk?*, L.A. TIMES (Aug. 23, 2019, 5:00 AM), https://www.latimes.com/travel/story/2019-08-22/facial-recognition-biometrics-at-airports-proliferating [https://perma.cc/Q6V4-3JSZ].

111. For an example of how the NYPD used FRT to quickly find the owner of a "suspicious appliance" thought to be a bomb in the New York subway system, see Lane Brown, *There Will Be No Turning Back on Facial Recognition*, INTELLIGENCER (Nov. 12, 2019), https://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html [https://perma.cc/3CXM-WN27]. Brown also notes several additional current uses of FRT: (1) by airlines to replace boarding passes; (2) in sports arenas; (3) by Taylor Swift's security to weed out known stalkers; (4) as replacements for key fobs at an apartment complex; (5) by schools to recognize suspended students who venture onto school grounds; and (6) by retailers to prevent theft and identify known shoplifters. *Id.*

112. For example, police may even compel individuals to open their phones—with facial recognition lock—for search by holding the phone to their face. For a detailed analysis of the Fourth Amendment implications of forcing a suspect to unlock a phone with their face compared to requiring a suspect to provide their passcode, see Richard G. Cole III, *The Constitutional Insecurity of Secured Smartphones: "Unlocking" the Current Fourth and Fifth Amendment Safeguards Protecting Secured Smartphones from Law Enforcement Searches*, 39 U. LA VERNE L. REV. 173, 194–95, 215, 216, 222 (2018).

113. *See* Reynolds, *supra* note 110.

114. *See, e.g.*, Brown, *supra* note 111; Zhao, *supra* note 15. China is attempting to build the world's most powerful facial recognition system. Stephen Chen, *China to Build Giant Facial Recognition Database to Identify Any Citizen Within Seconds*, S. CHINA MORNING POST (Oct. 12, 2017, 9:00 PM), https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any [https://perma.cc/ZQ4X-559T]. Its goal: identify any of its 1.3 billion citizens within three seconds. *Id.*

> The worst-case scenario for facial recognition might look like something like China's forthcoming "social credit system." When the system is fully operational next year, the government will use all surveillance methods at its disposal, including facial recognition and 200 million cameras, to track citizens' behavior and assign each of them a social score, which will have a variety of consequences. Infractions such as jaywalking and buying too many video games could make it harder to rent an apartment or get a loan from a bank. That probably isn't likely in the U.S., but a more ordinary kind of surveillance is almost inevitable.

Brown, *supra* note 111. The Chinese government is also using FRT to track and control a predominantly Muslim minority group within its borders. 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 [https://perma.cc/AD3Z-JSM7].

its 1.4 billion citizens.[115] Facial scanning technology has been implemented into sunglasses,[116] which law enforcement agencies could couple with robust facial databases to make almost every visible person identifiable.[117] "The tool could identify activists at a protest or an attractive stranger on the subway, revealing not just their names but where they lived, what they did and whom they knew."[118] This highlights just one use of FRT that could have nefarious consequences to privacy and free speech rights. Lack of imagination may be the only limit to further development and application of FRT.[119]

2. Potential Future Implications of FRT's Use by Law Enforcement

FRT has been portrayed in science fiction, in various forms, for decades.[120] Many of these portrayals involved innocuous applications of the technology that mirror today's uses, such as unlocking devices and making payments.[121] However, many others show FRT as a tool of the "surveillance state"[122] or authoritarian oppressive governments.[123] The

115. *Population, Total – China*, WORLD BANK, https://data.worldbank.org/indicator/SP.POP.TOTL?locations=CN [https://perma.cc/S2P2-LYQS].

116. Zhao, *supra* note 15.

117. *See* Hill, *supra* note 64.

118. *Id.*

119. Some planned implementations of FRT include: a gas station chain's plans to read customers' age and gender to tailor ads on pump-based screens; an app called Finding Rover that uses FRT to reunite lost pets with their owners; an app to identify lost children and family members; and as a method of preventing theft by identifying known shoplifters. Sandeep Raut, *Facial Recognition in the Digital Age*, INNOVATION ENTER. (Feb. 12, 2018), https://channels.theinnovationenterprise.com/articles/facial-recognition-in-digital-age [https://perma.cc/BPX9-77JM].

120. *See* Rowena Bonnette, *Biometrics in Movies Sci-Fi Security*, AVATIER (Jan. 31, 2017), https://www.avatier.com/blog/biometrics-in-sci-fi-movies/ [https://perma.cc/VD6E-DH69].

121. *See* Shaun Raviv, *The Secret History of Facial Recognition*, WIRED (Jan. 21, 2020, 6:00 AM), https://www.wired.com/story/secret-history-facial-recognition/ [https://perma.cc/U7U6-7XLG] ("Today, facial recognition has become a security feature of choice for phones, laptops, passports, and payment apps. It promises to revolutionize the business of targeted advertising and speed the diagnosis of certain illnesses. It makes tagging friends on Instagram a breeze.").

122. Examples of the "surveillance state" abound in dystopian literature. *See, e.g.*, JOHN BRUNNER, THE SHOCKWAVE RIDER (1975); PHILIP K. DICK, THE MINORITY REPORT (1987); JOHN TWELVE HAWKS, THE TRAVELER (2005); STANISLAW LEM, MEMOIRS FOUND IN A BATHTUB (1961); ORWELL, *supra* note 11.

123. *See, e.g.*, ORWELL, *supra* note 11.

creative machinations of some of the writers of such works are merely the tip of the iceberg. The telescreen of *Nineteen Eighty-Four* read emotions to identify non-compliant citizens.[124] Recently, a Stanford professor used FRT and AI to determine the sexual orientation of subjects from an image of their face alone.[125] Under a justification of protecting the population, the government could use FRT to root out undesirable ideologies, putting democracy at risk.

But "over-surveillance" could protect law-abiding citizens by deterring crime and making the apprehension of wrongdoers easier.[126] More than just catching criminals after they have committed their crimes, FRT could be deployed to deter crime in the first place.[127] With the explosion of surveillance cameras in both public and private settings,[128] American

---

124. Ferran Esteve, *Orwell in Times of Facial Recognition*, CCCB LAB (June 18, 2019), http://lab.cccb.org/en/orwell-in-times-of-facial-recognition/ [https://perma.cc/HED5-NAPG]. "The telescreen of *1984* . . . captures the most subtle of sounds and facial expressions. . . . [T]hey register everything from an 'unconscious look of anxiety' to a nervous tic or even a rumbling stomach." *Id.*

125. Heather Murphy, *Why Stanford Researchers Tried to Create a 'Gaydar' Machine*, N.Y. TIMES (Oct. 9, 2017), https://www.nytimes.com/2017/10/09/science/stanford-sexual-orientation-study.html [https://perma.cc/JX6D-EFJU]. The release of this study was very controversial. *See id.* The vast moral implications of FRT able to detect more than a person's identity are troubling. Scanning that facilitates the discovery of a person's attributes that are more than skin deep further ripens the potential for abuse by those in power. When a particular feeling or train of thought becomes associated with illegal conduct, the police may use technology to detect those thoughts and feelings to persecute those who have them.

126. For arguments supporting the implementation of FRT by the security industry, see generally SEC. INDUS. ASS'N, FACE FACTS: DISPELLING COMMON MYTHS ASSOCIATED WITH FACIAL RECOGNITION TECHNOLOGY (2019), https://www.securityindustry.org/wp-content/uploads/2019/06/facial-recognition-20193.pdf [https://perma.cc/TQ8M-UV8C]. For counterarguments from a leading civil liberties organization, see Hayley Tsukayama & Adam Schwartz, *Governments Must Face the Facts About Face Surveillance, and Stop Using It*, ELEC. FRONTIER FOUND. (Feb. 25, 2019), https://www.eff.org/deeplinks/2019/02/governments-must-face-facts-about-face-surveillance-and-stop-using-it [https://perma.cc/XX6P-PBA5].

127. *See* Nick Coult, *Shoplifting Deterrent: Facial Recognition Software*, CHAIN STORE AGE (June 7, 2018), https://chainstoreage.com/operations/shoplifting-deterrent-facial-recognition-software [https://perma.cc/29KN-LPFL] (discussing how the deployment of FRT in stores deters shoplifters).

128. *See* Liza Lin & Newley Purnell, *A World with a Billion Cameras Watching You Is Just Around the Corner*, WALL ST. J. (Dec. 6, 2019, 1:00 AM), https://www.wsj.com/articles/a-billion-surveillance-cameras-forecast-to-be-watching-within-two-years-11575565402 [https://perma.cc/N6JY-YU3X]. The improvements in FRT play a factor in the decisions of businesses to add surveillance cameras. *See id.* The integration of technologies, such as FRT, into video surveillance provides cross-functionality that is fueling hypergrowth in the global video surveillance industry. *See* Tim A. Scally, *State of the Market: Video Surveillance 2019*, SDM (Feb. 4, 2019), https://www.sdmmag.com/articles/96179-state-of-the-market-video-surveillance-2019 [https://perma.cc/9BWY-FRNG].

citizens are caught on camera more than ever.[129] Not all crimes will be caught by a surveillance camera, and even those that are may not produce a facial image that can be recognized even by advanced FRT.[130] Nevertheless, the possibility of being identified by enhanced FRT by one of the millions of cameras positioned throughout the country may reduce crime and help to apprehend dangerous perpetrators—something many would regard as justification for the widespread adoption of FRT surveillance.[131]

Most Americans would likely see a nationwide network of FRT surveillance, with its crime deterrent and enforcement effects, as a positive.[132] In fact, a recent study found that more than half of the population trusts law enforcement to use FRT responsibly.[133] However, those respondents may

129. *See* Drew Engelbart, *Caught on Camera: Americans Are Captured on an Estimated 70 Security Cameras Each Day*, KDVR (Feb. 11, 2018, 1:54 PM), https://kdvr.com/news/trending/caught-on-camera-americans-are-captured-an-estimated-70-security-cameras-each-day/ [https://perma.cc/ST4Z-L7K5].

130. *See* Valentino-DeVries, *supra* note 100.

131. Video recording serves another benefit to American citizens that has been highlighted recently by videos depicting police brutality. *See, e.g.*, Sarah Almukhtar et al., *Black Lives Upended by Policing: The Raw Videos Sparking Outrage*, N.Y. TIMES (Apr. 19, 2018), https://www.nytimes.com/interactive/2017/08/19/us/police-videos-race.html [https://perma.cc/F3UX-25JC]. None have sparked the reaction quite like the video of a Minneapolis police officer kneeling on the neck of George Floyd. *See* Evan Hill et al., *How George Floyd Was Killed in Police Custody*, N.Y. TIMES (May 31, 2020), https://www.nytimes.com/2020/05/31/us/george-floyd-investigation.html [https://perma.cc/7KB8-WELV]. Without videos like the ones showing George Floyd's last minutes, the calls for change and justice would be without the fervor demonstrated in the protests that raged across the country. However, videos of police violence are not new; perhaps the most well-known example of police violence against a citizen before George Floyd was the video of the 1991 beating of Rodney King in Los Angeles. *See* Anjuli Sastry & Karen Grigsby Bates, *When LA Erupted in Anger: A Look Back at the Rodney King Riots*, NPR (Apr. 26, 2017, 1:21 PM), https://www.npr.org/2017/04/26/524744989/when-la-erupted-in-anger-a-look-back-at-the-rodney-king-riots [https://perma.cc/57L8-ZKK5]. Unfortunately, the increased instances of police "caught-in-the-act" videos has not deterred police misconduct. The officer who killed George Floyd continued his assault despite the obvious presence of people recording the entire incident. *See* Farhad Manjoo, *Cameras Won't Stop Police from Killing*, N.Y. TIMES (June 3, 2020), https://www.nytimes.com/2020/06/03/opinion/george-floyd-video-police.html [https://perma.cc/ZP2S-KZVR]. The officer "ma[de] smirking eye contact with the camera . . . [and] halfheartedly reache[d] for what look[ed] like pepper spray when the phone-wielding bystanders g[o]t a bit rowdy in their insistence that Floyd [wa]s dying before their eyes." *Id.*

132. *See* Aaron Smith, *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, PEW RSCH. CTR. (Sept. 5, 2019), https://www.pewinternet.org/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly [https://perma.cc/PBL6-RUL8].

133. *Id.*

have failed to consider the big picture privacy implications of comprehensive state sponsored surveillance. Weighing privacy rights against effective policing creates a tension, which the law has struggled to address with any semblance of consistency.

III. PRIVACY VERSUS EFFECTIVE POLICING

With changes in technology, the role of police, police practices, and the culture of policing have changed, blurring the lines drawn in the law and weakening the constitutional protections those lines were meant to guarantee.[134] Technology has enabled police to be more proactive in their policing measures.[135] However, the potential uses of FRT by law enforcement could remove any expectation of privacy when one is in public.[136] Although over-surveillance and facial recognition may catch "wrongdoers," it does open the door for selective enforcement.[137] Those who have access to the technology would have tremendous power to choose how they use the information.[138] As Justice Sotomayor warned in her concurring opinion in *United States v. Jones*,[139]

> I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power and prevent "a too permeating police surveillance."[140]

---

134. FERGUSON, *supra* note 88, at 140.

135. BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 18 (2017). Police will likely continue to incorporate surveillance technology into their everyday activities.

> In the new policing, departments across the country are ramping up to employ automatic license plate readers and [FRT]—and soon enough drones—to be able to track us everywhere we go. They are utilizing software to predict where crime will occur next, and by whom. . . . Policing today is *regulatory*: it is about shaping behavior on the front end, not capturing crooks after the fact—and we have all become its targets.

Id.

136. FERGUSON, *supra* note 88, at 140. "We simply have no clear answer to whether things like pervasive, high-altitude video surveillance violates the Fourth Amendment. Nor has Congress stepped in to provide statutory clarity." *Id.*; *see also* MARIA HELEN MURPHY, SURVEILLANCE AND THE LAW: LANGUAGE, POWER, AND PRIVACY 31 (2019) (noting the lack of definitive direction to lower courts and police from the Court in *Carpenter*).

137. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013).

138. *Id.* at 1961 ("[W]atchers would have increased power to blackmail, selectively prosecute, coerce, persuade, and sort individuals.").

139. 565 U.S. 400 (2012).

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

A world in which an officer could type in a name and see that person's movements and actions, even if only to enforce the law, should be problematic to everyone.[141]

The rampant, unchecked use of FRT by law enforcement exposes all Americans to potential abuses by police officers equipped with FRT. An officer who can immediately identify any person on the street could create a myriad of more worrisome privacy invasions.[142] People should have the freedom to maintain some anonymity when outside their home.[143] If a judge would not sign off on a warrant to allow investigators to obtain the

141. For example, an officer types a name into their system and can see everywhere that person drove—and how fast; they could see where the person parked—and for how long; every time that person inadvertently dropped something—the officer would see. How many tickets for speeding, parking, and littering could one accumulate in a week? What if the officer was that person's neighbor and they had an ongoing property dispute?

142. For one, police officers—like all other citizens—are susceptible to poor decision making. A jealous officer could use the technology to instantly know intimate details about their spouse's acquaintances, which could lead to inappropriate interactions, or worse. However, more problematic would be an officer who is suspicious of a person, potentially based on the officer's biases. Instead of following that person to determine if there is any basis for suspicion, with FRT the officer would instantly know who that person is, where they live, and a whole slew of additional information. The officer might then check in regularly on persons that the officer decided were suspicious, which could rise to the level of harassment.

143. Eoin O'Carroll, *Face Off? Americans Fear Privacy Loss to Recognition Software*, CHRISTIAN SCI. MONITOR (June 20, 2019), https://www.csmonitor.com/Technology/2019/0620/Face-off-Americans-fear-privacy-loss-to-recognition-software [https://perma.cc/BJF7-ZG2T]. The Supreme Court has also found that anonymity is a protected First Amendment right. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995).

> Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society. The right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse.

Id. (citations omitted) (citing Abrams v. United States, 250 U.S. 616, 630–31 (1919) (Holmes, J., dissenting)). Moreover, "live" FRT could destroy anonymity, which would redefine how people behave in public space. Katelyn Ringrose, Essay, *Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns*, 105 VA. L. REV. ONLINE 57, 62–63 (2019). Those who might otherwise be critical of law enforcement could be subjected to abusive treatment "[a]nd, based on current technology, over time these burdens would disproportionately fall on minorities." *Id.* at 63.

information FRT would put at law enforcement's fingertips, the law should not allow technology to circumvent the warrant system.

Furthermore, due to the lack of reliability of FRT,[144] the potential for misidentification could expose the innocent to unwarranted police attention.[145] FRT may render a match that a police officer will act upon without verifying the accuracy of the identification.[146] This "black box data" is, almost by design, unverifiable.[147] The speed with which identification occurs combined with the immediacy to act on the identification makes mistaken identity by FRT even more dangerous.[148] A 95% match is likely to be good enough for most officers to act upon; yet a rate of one false arrest out of twenty is a frightening prospect.

To privacy advocates, FRT implemented as a law enforcement search tool creates issues that justify banning the technology altogether.[149] Even the general population—that does not take privacy as seriously as privacy advocates[150]—views personal information obtained for surveillance purposes as highly sensitive.[151] Unchecked, FRT could have drastic implications for our freedoms. As Justice Sotomayor further explained in *Jones*,

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. . . . [M]aking available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion,

144. *See supra* notes 44–58 and accompanying text.

145. *See* FERGUSON, *supra* note 88, at 96.

146. *Id.* at 97. When FRT confirms an officer's preexisting bias, they will be more emboldened to react strongly. *See* Shahram Heshmat, *What Is Confirmation Bias?*, PSYCH. TODAY (Apr. 23, 2015), https://www.psychologytoday.com/us/blog/science-choice/201504/what-is-confirmation-bias [https://perma.cc/9M7R-N473] (describing that confirmation bias leads individuals to neglect additional information gathering because evidence supports their underlying prejudices).

147. FERGUSON, *supra* note 88, at 97.

148. *Id.*

149. See Evan Selinger & Woodrow Hartzog, *What Happens when Employers Can Read Your Facial Expressions?*, N.Y. TIMES (Oct. 17, 2019), https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html [https://perma.cc/W8JX-RPDG], for the opinion from the perspective of two members of the Privacy Project.

150. *See* Liesbet van Zoonen, *Privacy Concerns in Smart Cities*, 33 GOV'T INFO. Q. 472, 475 (2016). A recent survey found that 56% of Americans trust law enforcement agencies to use FRT responsibly and 59% support its use to assess security threats in public spaces. Smith, *supra* note 132. However, almost three-quarters of those surveyed believed FRT could effectively identify individuals with a—perplexingly—slightly lower percentage believing FRT could accurately identify a person's race or gender. *Id.* So, although a majority does favor FRT's use by law enforcement, an even greater majority does not comprehend its current shortcomings. *See supra* notes 137–48 and accompanying text.

151. *See* van Zoonen, *supra* note 150, at 475.

> chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."[152]

An outright ban on a developing technology also has an impact on at least one of our freedoms—namely, our freedom to innovate.[153] Although rulings on FRT could impact other areas of the law—such as intellectual property rights and free speech, when it comes to FRT's use by law enforcement, the Court's analysis must begin with the Fourth Amendment.[154]

In its Fourth Amendment cases, the Court has attempted to balance privacy against government power—both with legitimate and important considerations.[155] The rights of privacy must be weighed against the legitimate government powers of fighting crime and protecting national security.[156] The development of new technology combined with the national security model of law enforcement will force the judiciary to confront the challenge of accommodating change while continuing to uphold the privacy rights afforded by the Fourth Amendment.[157] The core concept of privacy as a Fourth Amendment right evolved out of the Court's broad interpretation

---

152. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas–Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

153. The Constitution grants Congress the power "[t]o promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries." U.S. CONST. art. I, § 8, cl. 8. Limiting innovation by restricting the use of FRT could impact innovation and reduce the ability of Congress to promote scientific progress. By no means should this drive judicial decision making regarding FRT, but it is another example of how the Court's decisions in one area of the law can indirectly affect seemingly unrelated Constitutional rights and mandates.

154. Any action by law enforcement that could be construed as a search must survive Fourth Amendment scrutiny. *See generally* Thomas K. Clancy, *What Is a "Search" Within the Meaning of the Fourth Amendment?*, 70 ALB. L. REV. 1 (2006) (discussing the "two-sided inquiry" of Fourth Amendment search analysis defined as "governmental actions [that] must invade a protected interest of the individual").

155. Lenz, *supra* note 71, at 272. However, justices have different conceptions of privacy, which can be separated into two camps. *Id.* at 277. The first is that "privacy applies to an act that a person does alone or that has no impact on anyone else." *Id.* The second "is based on the distinction between acts that government has a legitimate interest in regulating, which are therefore public, and acts the government does not have a legitimate interest in regulating, which are therefore private even if the action involves more than one person." *Id.* This second notion of privacy is more adaptable to the digital age, when "private communications" travel through third-party intermediaries and a person's "personal photo album" exists on a third-party's website. *See id.* at 277–78.

156. *Id.*

157. *Id.* at 302–03.

of the four things—persons, houses, papers, and effects[158]—specifically identified in the Fourth Amendment.[159] This reading of the amendment interprets the intent of the drafters "to guarantee limited government by protecting the right to privacy."[160]

"To protect [privacy] rights, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[161] However, courts may be willing to relax constitutional protections as a practical matter when FRT identifies a potential suspect or "bad actor" by finding suspicion based on the FRT result alone.[162] How intrusive FRT becomes is dependent upon what the law allows.

IV. THE STATUTORY FRAMEWORK GOVERNING FRT

Statutory law that directly addresses the use of FRT is sparse.[163] In the United States, some potential uses of FRT have been anticipated and

---

158. U.S. CONST. amend. IV. Defining each of the enumerated items has been the subject of considerable scholarly debate. *See, e.g.*, H. Brian Holland, *A Cognitive Theory of the Third-Party Doctrine and Digital Papers*, 91 TEMP. L. REV. 55, 63 (2019) (arguing that the digital equivalents of papers should receive Fourth Amendment protection); Alexander Porro, Comment, *Dwelling in Doubt: Do Tenants Have a Reasonable Expectation of Privacy in the Common Areas of Their Apartment Buildings?*, 2018 U. CHI. L.F. 333, 334 (arguing that Fourth Amendment rights should be extended to common areas of apartment buildings).

159. *See* Lenz, *supra* note 71, at 272.

160. *Id.*

161. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). Although Justice Brandeis was on the losing side of the decision in *Olmstead*, his dissent laid the foundation for the evolution of Fourth Amendment jurisprudence. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 839 (2004). Some scholars have singled out Brandeis's dissent "as a model for how to interpret the Fourth Amendment in light of technological change." *Id.* at 858 (citing LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 116 (1999)). However, Kerr has disagreed with the entire notion of judicial rulemaking in the context of technology and the Fourth Amendment. *See id.* at 858–59.

162. *See* FERGUSON, *supra* note 88, at 140–41. Combining predictive AI technology with FRT will only serve to further justify this kind of stop and seizure by police. Society might accept some reduction to privacy rights if the result is not only better law enforcement, but statistically supported crime prevention.

> [Q]uestions of probabilistic suspicion will bedevil courts. Precise algorithms providing accurate but generalized suspicion will make decision on probable cause very difficult. Metadata will provide actionable clues that police will want to act on in real time. Courts will have a difficult time saying highly predictive, pure-probability suspicion is not good enough.

Id. at 141. There is substantial skepticism regarding the use of big data searches for preventative policing. *See* Lenz, *supra* note 71, at 279.

163. *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 414–15 (2012)

addressed by legislation at the state level.[164] Illinois addressed the use of FRT by private enterprise, primarily aimed at online media companies like Facebook and Google.[165] New Hampshire bars state agencies from using FRT in conjunction with its driver's license photo databases[166] and body-worn cameras.[167] A Vermont law bans law enforcement from equipping drones with FRT.[168] California is the most recent to take legislative action in addressing the use of FRT. On September 12, 2019, the California legislature sent AB 1215 to the governor,[169] and on October 7, 2019, Governor Gavin Newsom signed it into law.[170] The law bans the use of FRT incorporated into law enforcement body-worn cameras.[171] However, it is limited to a duration of three years, and proposed provisions to apply the ban to all surveillance cameras were removed before the bill's

(noting that despite an increase in federal FRT identification initiatives, Congress has yet to pass legislation that directly addresses the use of FRT by law enforcement or by intelligence agencies).

164. *See, e.g.*, CAL. PENAL CODE § 832.19 (West 2020); N.H. REV. STAT. ANN. §§ 105-D:2, 263:40-b (2019); VT. STAT. ANN. tit. 20, § 4622 (2019).

165. *See* Illinois Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14/1–/25 (2018) (limiting private enterprise use of "facial geometry"). *See generally In re* Facebook Biometric Info. Priv. Litig., 326 F.R.D. 535 (N.D. Cal. 2018) (certifying "a class consisting of Facebook users located in Illinois for whom Facebook created and stored a face template" under the common questions of whether "Facebook's facial recognition technology harvest[ed] biometric identifiers" and whether "Facebook g[a]ve users prior notice of these practices and obtain[ed] their consent").

166. N.H. REV. STAT. ANN. § 263:40-b.

167. *Id.* § 105-D:2.

168. VT. STAT. ANN. tit. 20, § 4622. The issue of drone-enhanced policing is another that needs more consideration by lawmakers. Experts predicted that the government and private companies could launch as many as thirty thousand drones by the early 2020s. *See* Brown, *supra* note 33, at 431. "Equipped with powerful FRT cameras, the drones 'will be capable of capturing minute details, including every mundane action performed by every person in an entire city simultaneously.'" *Id.* (quoting John W. Whitehead, *Smile, the Government Is Watching: Next Generation Identification*, RIGHT SIDE NEWS (Sept. 17, 2012, 12:07 PM), http://www.rightsidenews.com/2012091717049/editorial/us-opinion-and-editorial/smile-the-government-is-watching-next-generation-identification.html [https://perma.cc/A9A2-YET2]).

169. Rachel Metz, *California Lawmakers Ban Facial-Recognition Software from Police Body Cams*, CNN (Sept. 13, 2019, 8:04 AM), https://www.cnn.com/2019/09/12/tech/california-body-cam-facial-recognition-ban/index.html [https://perma.cc/YE8K-YN5X].

170. Evan Symon, *Governor Newsom Signs Bill Banning Facial Recognition Technology in Police Body Cameras*, CAL. GLOBE (Oct. 9, 2019, 8:53 PM), https://californiaglobe.com/section-2/governor-newsom-signs-bill-banning-facial-recognition-technology-in-police-body-cameras [https://perma.cc/ARK7-ZKQG]; *see* CAL. PENAL CODE § 832.19 (West 2020).

171. *See* PENAL § 832.19(b).

passage.[172] Other laws control aspects of FRT's implementation, without any cognizance of the implications it would have on FRT.[173] None of these laws are broad enough to relieve privacy concerns.[174] However, some federal law provides alternative justification for governmental use of FRT outside the law enforcement context.

28 U.S.C. § 534 expressly requires the Attorney General to acquire, preserve, and exchange identification information.[175] The statutory scheme creating the FBI provides that "[t]he Attorney General shall" obtain information related to "criminal identification [and] crime," identifying deceased individuals, and locating missing persons.[176] The statute also requires that the Attorney General share those records with other federal agencies, state agencies, cities, and "penal and other institutions."[177] The statute further provides the Attorney General—who assigned this responsibility to the FBI—broad discretion in how to comply[178] and few legal limitations to the collection of biometric information.[179] Many scholarly works have advocated for the amendment of 28 U.S.C. § 534 to address privacy concerns.[180] However, this Comment advocates for a more thorough overhaul of § 534 and creation of a new statutory provision to address the legitimate government interests in identifying the deceased and locating the missing.

Other statutes aim at assisting law enforcement in identifying people. Many states adopted "stop and identify" statutes by the mid-1970s requiring suspicious persons to identify themselves when asked by police.[181] "[S]top and identify laws exist in 24 states."[182] The Court has struck down

---

172. *Id.* § 832.19(e); *Law Enforcement: Facial Recognition and Other Biometric Surveillance: Hearing on A.B. 1215 Before the Assemb. Comm. on Pub. Safety*, 2019-2020 Leg. Sess. (Cal. 2019) (statement of Nikki Moore, Couns., Cal. State Assemb. Comm. on Pub. Safety); Metz, *supra* note 169.

173. *See, e.g.*, 18 U.S.C. § 2721 (allowing federal law enforcement agents to obtain information—such as driver's license photos—from state DMV records); 28 U.S.C. § 534 (requiring the Attorney General to gather and disseminate information related to crime and identification).

174. *See supra* Part III.

175. 28 U.S.C. § 534 (governing the "[a]cquisition, preservation, and exchange of identification records and information; appointment of officials").

176. *Id.* § 534(a)(1)–(3).

177. *Id.* § 534(a)(4).

178. *See* Christopher DeLillo, *Open Face: Striking the Balance Between Privacy and Security with the FBI's Next Generation Identification System*, 41 NOTRE DAME J. LEGIS. 264, 266 (2015).

179. *See* Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. MARSHALL L. REV. 589, 601 (2018).

180. *See, e.g.*, DeLillo, *supra* note 178, at 266; Snyder, *supra* note 79, at 274.

181. *See* Jonathan Weinberg, *Proving Identity*, 44 PEPP. L. REV. 731, 780 (2017).

182. Charles Montado, *Do I Have to Show the Police My ID?*, THOUGHTCO. (Nov. 2, 2019), https://www.thoughtco.com/show-the-police-my-id-970889 [https://perma.cc/

some aspects of these laws, iterating that the statutes cannot be vague and must require reasonable suspicion.[183] In a typical interaction, though, these concerns are not at issue because most people, when asked for identification by a police officer, will comply without resistance.[184] However, if a person declines the officer's request, the officer cannot demand the citizen's identification without reasonable suspicion.[185] FRT

CL4P-7UCG]. The states that have stop and identify laws are Alabama, Arizona, Arkansas, Colorado, Delaware, Florida, Georgia, Illinois, Indiana, Kansas, Louisiana, Missouri (Kansas City only), Montana, Nebraska, Nevada, New Hampshire, New Mexico, New York, North Dakota, Ohio, Rhode Island, Utah, Vermont, and Wisconsin. *Id.*

183. *See, e.g.*, Kolender v. Lawson, 461 U.S. 352, 357–58 (1983) (striking down California's "stop and identify" statute for vagueness); Brown v. Texas, 443 U.S. 47, 53 (1979) (striking down a Texas "stop and identify" statute because it lacked a reasonable suspicion component). *But see* Hiibel v. Sixth Jud. Dist. Ct. of Nev., 542 U.S. 177, 188 (2004) ("A state law requiring a suspect to disclose his name in the course of a valid *Terry* stop is consistent with Fourth Amendment prohibitions against unreasonable searches and seizures.").

184. *See* Desiree Phair, *Searching for the Appropriate Standard: Stops, Seizure, and the Reasonable Person's Willingness to Walk Away from the Police*, 92 WASH. L. REV. 425, 442 (2017).

> Previous studies have demonstrated that civilians rarely feel free to ignore authority figures. Researchers have conducted a number of queries examining subjects' actions when commanded by an official, responses to requests from those in uniform, behavior adaptions when warned in advance of rights, and willingness to interact with police[.] Electric shock experiments and experiments testing laypersons' reaction to those in uniform show that most people comply with requests from authority figures. Studies covering warnings' effect on voluntary consent further support that civilians tend to acquiesce. Finally, a thorough study testing willingness to refuse police indicates laypersons' discomfort with avoiding officers.

Id. (footnotes omitted).

185. *See* Margaret Raymond, *The Right to Refuse and the Obligation to Comply: Challenging the Gamesmanship Model of Criminal Procedure*, 54 BUFF. L. REV. 1483, 1501 (2007). Professor Raymond goes on to note the practical implications of refusing to comply with an officer's request for identification.

> There is another gamesmanship component to the consensual encounter standard. While the standard presumes that a reasonable person knows when he is free to decline an officer's requests, as a legal matter that freedom turns, in part, on the officer's level of suspicion. If the officer's observations do not amount to reasonable suspicion, then the individual is free to decline the encounter. On the other hand, if the officer has reasonable suspicion, he has the authority to subject the individual to a stop and to require compliance if the individual refuses. But the individual, even assuming he understands the governing legal principles, has no way of knowing how much suspicion the officer has. Walking away may be constitutionally protected, or it may be a criminal act; which it is may prove to

cuts out the request and consensual aspect of the equation, jumping directly to the identification step without gaining consent or having reasonable suspicion.[186]

Another area that has been explored by academia and addressed by some state legislative action is the implementation of FRT into body-worn cameras (BWCs).[187] There has been significant public outcry calling for the required use of BWCs by police officers, and its implementation has been largely considered a positive development in policing practices.[188] However, incorporating FRT into BWCs presents a myriad of potential constitutional issues and negative effects.[189] In a First Amendment context, FRT may deter people from attending public protests, rallies, or other political gatherings knowing that their identity would be instantly known to law enforcement equipped with FRT enabled BWCs.[190]

> be a roll of the dice. At least in some circumstances, the suspect needs not only to be reasonable about the legality of the officer's actions, but to be right.

Id. at 1501–02 (footnotes omitted) (citing N.D. CENT. CODE § 12.1-08-02 (1997)).

186. Congress could mitigate the reasonable suspicion issue with legislation that requires law enforcement to manually operate any FRT search systems. Instead of having FRT actively scanning faces like license plate scanners, *see* POLICE EXEC. RSCH. F., *supra* note 17, at 28–34; *see also supra* note 17 and accompanying text, officers operating a vehicle or monitoring a camera feed could control when an FRT system runs a search. This potential solution presents problems on both sides of the issue. From the perspective of law enforcement, this would seem to be a gross underutilization of the technology. Nonetheless, from those advocating for privacy protections and against overbearing police search tactics, such a limitation would be ripe for exploitation and nearly impossible to oversee. In a certain sense, such a compromise is an attractive option. However, in application, limiting technological advancement does not achieve an optimal result. Also, the ease with which an officer could initiate an FRT search—by pushing a button—decreases the inherent barriers to initiating a traditional search—conducting a stop, engaging with the individual, and requesting identification—increases the likelihood of abuse. *See generally* Wouter Kool et al., *Decision Making and the Avoidance of Cognitive Demand*, 139 J. EXPERIMENTAL PSYCH.: GEN. 665 (2010). Congress should enact legislation that allows for technology's implementation without tempting unconstitutional behavior. *See infra* Part VI.

187. *See, e.g.*, Ringrose, *supra* note 143; Wouter Zwart, *Slow Your Roll Out of Body-Worn Cameras: Privacy Concerns and the Tension Between Transparency and Surveillance in Arizona*, 60 ARIZ. L. REV. 783, 788 (2018).

188. Kelly Blount, *Body Worn Cameras with Facial Recognition Technology: When It Constitutes a Search*, CRIM. L. PRAC., Fall 2017, at 61, 61.

189. Ringrose, *supra* note 143, at 62; *see also supra* notes 20, 24 and accompanying text. The negative effects of BWCs with FRT "include, but are not limited to, disparities in how the technology treats African Americans, chilling free speech, and vulnerability to third-party hacking and misuse of data." Ringrose, *supra* note 143, at 62.

190. *See generally* Julian R. Murphy, *Chilling: The Constitutional Implications of Body-Worn Cameras and Facial Recognition Technology at Public Protests*, 75 WASH. & LEE L. REV. ONLINE 1 (2018) (arguing against incorporating FRT into BWCs, especially in the context of political protests, due to the likely chilling effect on freedom of speech).

Other laws have targeted FRT's commercial uses by non-government entities.[191] These laws sparked an explosion of litigation,[192] which may eventually provide valuable insight into how the courts view FRT outside the law enforcement context. However, the states with these laws have made them applicable to non-public entities only.[193] More comprehensive legislation is necessary to appropriately check law enforcement's use of FRT. This Comment insists that Congress must act to interrupt law enforcement's use of FRT to protect the privacy rights of Americans because the judiciary is unlikely to bar FRT's use or act quickly enough to prevent unprecedented privacy intrusions.

V. THE SUPREME COURT'S FOURTH AMENDMENT SEARCH DOCTRINE

The legality of law enforcement's use of FRT must begin by determining whether the use of FRT constitutes a search. All search analyses begin with the Fourth Amendment to the U.S. Constitution, which reads:

> 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, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[194]

The two clauses of the Fourth Amendment deserve special attention. The first—the "reasonableness clause"—requires that searches and seizures be "reasonable"; the second—the "warrant clause"—explains what is required to obtain a warrant.[195] This distinction is important here because

191. *See, e.g.*, Illinois Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14/10 (2019). This law has already been the subject of recent litigation. *See In re* Facebook Biometric Info. Priv. Litig., 326 F.R.D. 535, 535–36 (N.D. Cal. 2018).

192. Charles N. Insler, *Understanding the Biometric Information Privacy Act Litigation Explosion*, ILL. B.J., Mar. 2018, at 34, 35–36; *see, e.g.*, *In re* Facebook Biometric Info. Priv. Litig., 326 F.R.D. at 535; Rivera v. Google Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017); Gullen v. Facebook.com, Inc., No. 15-cv-7681, 2016 WL 245910 (N.D. Ill. Jan. 21, 2016).

193. *See, e.g.*, 740 ILL. COMP. STAT. 14/10. The Illinois statute only applies to "private entities," defined as "any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof." *Id.*

194. U.S. CONST. amend. IV.

195. *See* Silas J. Wasserstrom, *The Fourth Amendment's Two Clauses*, 26 AM. CRIM. L. REV. 1389, 1389–90 (1988–1989). The first iteration of what became the Fourth Amendment, written by James Madison, related these clauses to one another in the context of barring general warrants. *Id.* at 1391. The original wording was:

this Comment explores the legal framework of warrantless FRT use, analyzing whether that use constitutes a search.[196]

Early case law involving the Fourth Amendment searches is sparse, mostly because criminal prosecutions were in state courts—in which the Fourth Amendment did not apply prior to the ratification of the Fourteenth Amendment—and law enforcement was conducted by state or locally run agencies.[197] Until the enactment of the Fourteenth Amendment, the protections under the Fourth Amendment were only applied to federal law enforcement agencies, very few of which existed before the twentieth century.[198]

In the twentieth century, the Court developed its Fourth Amendment doctrine.[199] The Court has established two approaches to Fourth

---

> The right of the people to be secure in their persons, their houses, their papers, and their other property, from all unreasonable search and seizures, shall not be violated by warrants issued without probable cause, supported by oath or affirmation, or not particularly describing the places to be searched, or the persons or things to be seized.

1 ANNALS OF CONG. 452 (J. Gales ed. 1789).

196. Under the proposed solution of this Comment, *see infra* Part VI, law enforcement would be free to seek a warrant to use FRT to find or identify a suspect. Although this Comment analyzes only warrantless FRT use, a warrant resolves many of the issues identified herein. A warrant must "particularly describ[e] the . . . things to be seized." U.S. CONST. amend. IV. Thus, a warrant resolves the issue of widely deployed FRT that scans and identifies every person's face or scans particular faces on an officer's whim. If law enforcement obtains a warrant to get images contained on social media, there is no inappropriate invasion of privacy.

197. Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 613 (1999); David E. Steinberg, *The Uses and Misuses of Fourth Amendment History*, 10 U. PA. J. CONST. L. 581, 586–87 (2008). Prior to *United States v. Boyd*, 116 U.S. 616 (1886), "constitutional search-and-seizure provisions probably were mentioned in fewer than fifty cases." Steinberg, *supra*, at 586. Although most state constitutions during the eighteenth and early nineteenth century contained search and seizure provisions similar to the language of the Fourth Amendment, published state court opinions rarely referenced these provisions. *Id.* at 587. Instead, courts often treated search and seizure related claims as common law trespass or civil law forfeiture actions. Fabio Arcila, Jr., *A Response to Professor Steinberg's Fourth Amendment Chutzpah*, 10 U. PA. J. CONST. L. 1229, 1251 (2008).

198. *See* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 77 & n.41 (2013); *see also, e.g.*, *A Brief History*, FBI, https://www.fbi.gov/history/brief-history [https://perma.cc/2LSR-GXJE] (describing the formation of the FBI in 1908).

199. In the late nineteenth century, the Court did take on two cases that established the foundation from which the Court built its Fourth Amendment doctrine. *See Boyd*, 116 U.S. 616; *Ex parte* Jackson, 96 U.S. 727 (1877). In *Ex parte Jackson*, the Court held that the Fourth Amendment barred government officials from opening letters and packages transported by the U.S. Postal Service. 96 U.S. at 733. In *Boyd*, the Court noted the close relationship between the Fourth Amendment's protection against unreasonable searches and the Fifth Amendment's right against self-incrimination. 116 U.S. at 633–35. The Court construed the Fourth Amendment liberally and held that complying with a federal law requiring disclosure of documents was equivalent to a search. *Id.* at 634–35.

Amendment questions: trespass and privacy.[200]

A. Fourth Amendment Trespass Doctrine

In the 1920s, the Court began to evaluate Fourth Amendment issues as trespasses.[201] In *Olmstead v. United States*,[202] the Court departed from the liberal application of Fourth Amendment rights. The Court found that Fourth Amendment protections applied if "there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."[203] This rule became known as the "trespass test" and controlled Fourth Amendment jurisprudence throughout the early twentieth century.[204] However, after establishing the "reasonable expectation of privacy" test in *Katz v. United States*,[205] the Court relegated trespass to one factor in the privacy analysis.[206]

In the twenty-first century, the Court—in a slew of decisions—reestablished the trespass view of the Fourth Amendment.[207] The seminal case restoring the trespass approach is *United States v. Jones*, in which the

200. David Steinberg, Florida v. Jardines*: Privacy, Trespass, and the Fourth Amendment*, 23 TEMP. POL. & C.R.L. REV. 91, 97 (2013) ("[N]either privacy analysis nor trespass analysis has yielded a coherent body of Fourth Amendment doctrine.").

201. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 466 (1928); Hester v. United States, 265 U.S. 57, 58–59 (1924).

202. 277 U.S. 438 (1928).

203. *Id.* at 466. The Court ruled that a wiretap of a building's phone lines was not a "search" or a "seizure" because law enforcement never entered the building to effectuate the wiretap. *Id.*

204. *See* Richard Sobel, Barry Horwitz & Gerald Jenkins, *The Fourth Amendment Beyond* Katz*,* Kyllo *and* Jones*: Reinstating Justifiable Reliance as a More Secure Constitutional Standard for Privacy*, 22 B.U. PUB. INT. L.J. 1, 9 (2013). Notably, Justice Brandeis, in dissent, described the future focus of Supreme Court Fourth Amendment decisional rationale: privacy. *See Olmstead*, 277 U.S. at 475–78 (Brandeis, J., dissenting). Before ascending to the Court, Brandeis along with Samuel Warren argued that "a person has the 'right to be let alone'" in an 1890 article in the *Harvard Law Review*. Meghan E. Leonard, *The Changing Expectation of Privacy in the Digital Age*, *in* 1 PRIVACY IN THE DIGITAL AGE: 21ST-CENTURY CHALLENGES TO THE FOURTH AMENDMENT 307, 308 (Nancy S. Lind & Erik Rankin eds., 2015) (quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890)).

205. 389 U.S. 347, 361 (1967).

206. Steinberg, *supra* note 200, at 107.

207. *See id.* at 107–09.

late Justice Scalia penned the majority opinion.[208] The *Jones* search analysis notes that "[a] trespass on 'houses' or 'effects,' or a *Katz* invasion of privacy, is not alone a search unless it is done to obtain information; and the obtaining of information is not alone a search unless it is achieved by such a trespass or invasion of privacy."[209] However, when the Court applied the *Jones* test in *Florida v. Jardines*[210]—another opinion written by Justice Scalia—the word "trespass" was noticeably absent.[211] Nonetheless, Justice Scalia is credited with returning the Court's Fourth Amendment approach to its traditional roots, which has gained significant support within the academic community.[212]

However, at least one scholar has challenged the notion that the Court has traditionally required trespass as a precursor to finding a Fourth Amendment violation.[213] Orin Kerr noted that early Fourth Amendment cases varied widely in methodology, weighing "a mix of property, privacy, and policy concerns."[214] Further, the Founding Fathers drafted many provisions of the Bill of Rights to protect the rights of suspects and convicted offenders because they had "experienced the political use of the criminal law powers during the colonial era."[215]

Applying the *Jones* test to FRT as a search tool requires determining whether the technology intrudes physically upon the "person."[216] Looking

---

208. 565 U.S. 400, 405 (2012); *see also* Sara M. Corradi, *Be Reasonable! Limit Warrantless Smart Phone Searches to* Gant*'s Justification for Searches Incident to Arrest*, 63 CASE W. RSRV. L. REV. 943, 954 (2013).

209. *Jones*, 565 U.S. at 408 n.5.

210. 569 U.S. 1, 5 (2013).

211. Orin Kerr, *What is the State of the* Jones *Trespass Test After* Florida v. Jardines*?*, VOLOKH CONSPIRACY (Mar. 27, 2013, 2:56 AM), http://volokh.com/2013/03/27/what-is-the-state-of-the-jones-trespass-test-after-florida-v-jardines [https://perma.cc/Z979-DCRX].

212. *See* Sobel, Horwitz & Jenkins, *supra* note 204, at 8–9 (noting that the Supreme Court applied a Fourth Amendment property-based test: "a government-sponsored physical trespass on or of tangible property constituted a Fourth Amendment violation").

213. Kerr, *supra* note 198, at 68–69.

214. *Id.* at 69. Professor Kerr traces the mistaken "common wisdom" that pre-*Katz* search doctrine was based on trespass law to two cases from 1967: *Warden v. Hayden*, 387 U.S. 294 (1967), and *Katz* itself. Kerr, *supra* note 198, at 68–69. "Both cases wrongly claimed that prior law had adopted a trespass standard. Later commentators assumed these claims to be true, cementing the trespass narrative for pre-*Katz* search doctrine." *Id.* at 69. Several nineteenth and early twentieth century cases demonstrate that "early Supreme Court search doctrine was not tied to property law." *Id.* at 77–79 (referencing *Boyd v. United States*, 116 U.S. 616 (1886), *Hale v. Henkel*, 201 U.S. 43 (1906), *Perlman v. United States*, 247 U.S. 7 (1906), and *United States v. Lee*, 274 U.S. 559 (1927)).

215. Lenz, *supra* note 71, at 282.

216. *See* Kerr, *supra* note 211. Under one interpretation, the *Jones* test acts to "protect[] private property from physical intrusion." *Id.* While Professor Kerr notes that the *Jones* Court relied on the text of the Fourth Amendment explicitly to extend its protections to "private property," *see id.*, this Comment posits that the same analysis should yield similar protections to the "person."

first to the scan, FRT has no physical interaction with its subject. It need not touch a person or invade upon their personal space. The logic applied by *Olmstead* was that tapping the phones did not require intrusion into the building, and therefore was not a "trespass" by the government that evoked Fourth Amendment protections.[217] Because *Jones* revived the trespass rationale iterated in *Olmstead*, it must be noted that FRT scans do not fall within the common law's trespass doctrine. Evaluating the databases yields the same result under the *Jones* test. There is no physical intrusion because the acquisition of data requires no physical contact; instead, data is acquired electronically.[218] What is more, the electronic intrusion does not involve property owned by the target; instead, the data resides on servers owned by the agency or company from which the photo was mined to assemble the database.[219]

Lower courts have narrowly interpreted *Jones* as applying only to cases of physical intrusion.[220] So, that provides a definitive result: FRT as a search tool does not violate traditional notions of trespass, neither by the facial scan nor in its assembly of face databases. "Where a search does not involve a physical trespass, the court applies the analysis used in *Katz*."[221]

B. Katz*'s Reasonable Expectation of Privacy*

The privacy view of Fourth Amendment protection was fully adopted by the Court in the 1960s.[222] The Court's Fourth Amendment analysis

---

217. Olmstead v. United States, 277 U.S. 438, 466 (1928).

218. However, the Court applies different analysis to digital-age questions. *See infra* Sections V.B.2 & V.B.3.

219. *See, e.g.*, Krish Bandaru & Kestutis Patiejunas, *Under the Hood: Facebook's Cold Storage System*, FACEBOOK (May 14, 2015), https://engineering.fb.com/core-data/under-the-hood-facebook-s-cold-storage-system [https://perma.cc/H4DF-86W7] (explaining Facebook's innovate approach to data storage to accommodate the more than two billion photos that are shared via the social media site every day); David Mortenson, *2017 Year in Review: Date Centers*, FACEBOOK (Dec. 11, 2017), https://engineering.fb.com/data-center-engineering/2017-year-in-review-data-centers [https://perma.cc/6PY7-PCQ6] (noting that Facebook added four new data centers in 2017 to the eleven already existing across the globe).

220. *See, e.g.*, United States v. Davis, 785 F.3d 498, 513–14 (11th Cir. 2015); United States v. Rogers, 71 F. Supp. 3d 745, 749 (N.D. Ill. 2014), *aff'd*, 901 F.3d 846 (7th Cir. 2018).

221. United States v. Alvarez, No. 14-cr-00120-EMC, 2016 WL 3163005, at *1 (N.D. Cal. June 3, 2016) (citing United States v. Jones, 565 U.S. 400, 411 (2012)).

222. *See* Ber-An Pan, Comment, *The Evolving Fourth Amendment:* United States v. Jones*, the Information Cloud, and the Right to Exclude*, 72 MD. L. REV. 997, 1003 (2013).

shifted away from property rights[223] and focused on a reasonable expectation of privacy test.[224] *Katz v. United States*[225] is the seminal case interpreting the protection against warrantless searches provided by the Constitution.[226] Justice Harlan's concurrence in *Katz*, adopted by the Court in *Smith v. Maryland*,[227] laid out a two-part test: "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.'"[228] Application of the test has typically consisted of only applying the second, objective prong, asking whether an expectation of privacy and protection against warrantless searches is societally reasonable.[229]

The Warren Court of the 1960s was known as a policymaking court, especially in the area of criminal justice. *See* Lenz, *supra* note 71, at 271. The Warren Court did not decide cases narrowly, instead making broad policy rulings with "a clear preference for the due process model of justice." *Id.* The Burger and Rehnquist Courts that followed moved the Court in a conservative direction. *Id.* While the Roberts Court has followed the broad policymaking approach of the Warren Court, "its rulings reflect the values and policies associated with the crime control model of justice" that is more deferential to police and prosecutors, supporting executive discretion. *Id.*

223. Martin McKown, *Fifty Years of* Katz*: A Look Back—and Forward—at the Influence of Justice Harlan's Concurring Opinion on the Reasonable Expectation of Privacy*, 85 GEO. WASH. L. REV. ARGUENDO 140, 142 (2017).

> In a single footnote, Justice Harlan also declared that the Court's decision effectively overruled the property-based approach in *Olmstead*. This was a significant proposition because, in his own words, the *Olmstead* decision "essentially rested on the ground that conversations were not subject to the protection of the Fourth Amendment." The footnote served to emphasize the notion that, like his colleagues in the majority, Justice Harlan believed the Fourth Amendment extends beyond physical intrusions to protect conversations that were expected to be safe from the uninvited ear, even when made in a public place like a telephone booth.

Id. at 143–44 (footnotes omitted) (citing and quoting Katz v. United States, 389 U.S. 347, 361, 362 n.* (1967)).

224. *See Katz*, 389 U.S. at 353, 359.

225. 389 U.S. 347 (1967).

226. Charles E. MacLean, Katz *on a Hot Tin Roof: The Reasonable Expectation of Privacy Doctrine is Rudderless in the Digital Age, Unless Congress Continually Resets the Privacy Bar*, 24 ALB. L.J. SCI. & TECH. 47, 55 (2014); McKown, *supra* note 223, at 140; Matthew M. Meacham, *The Perfect Storm How Narrowing of the State Action Doctrine, Inconsistency in Fourth Amendment Caselaw, and Advancing Security Technologies Converge to Erode Our Privacy Rights*, 55 IDAHO L. REV. 309, 321 (2019).

227. 442 U.S. 735, 740 (1979).

228. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

229. Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV.113, 114–16 (2015). Although courts often contend that they are applying both the subjective and objective prongs of the *Katz* analysis, courts overwhelmingly rely upon the objective prong, even in the two percent of decisions that claim to apply subjective analysis exclusively. *Id.* at 117, 120–21.

Courts have struggled to define a "reasonable expectation of privacy," as this concept is dynamic and subjective.[230] Balancing privacy interests of individuals against the reasonableness of law enforcement's tactics[231] and police efficiency has led to perplexing decisions.[232] The bulk of rulings boil down to an unhelpful maxim: "it depends." In determining whether an expectation of privacy is reasonable, the courts examine the totality of the circumstances.[233] Certain classes of people have a reduced

230. Lenz, *supra* note 71, at 270. The reasonableness requirement is malleable in that "it changes with the times" and "its meaning is relative in the sense that it is based on personal expectations." *Id.* Thus, public opinion plays a major role in the Supreme Court's Fourth Amendment jurisprudence. *See id.* The changing expectations of privacy make it difficult for courts to keep pace. More critically, the idea of an evolving concept of privacy rights—especially when the Constitution does not explicitly mention privacy—rings of "living constitutionalism," a concept that makes devoted originalists cringe. *See generally* Thomas Y. Davies, *Can You Handle the Truth? The Framers Preserved Common-Law Criminal Arrest and Search Rules in "Due Process Of Law"—"Fourth Amendment Reasonableness" Is Only a Modern, Destructive, Judicial Myth*, 43 TEX. TECH L. REV. 51 (2010) (arguing against the *Katz* reasonable expectation of privacy test from an originalist perspective). "The historical record shows that the Framers did not write the Fourth Amendment to control criminal arrest and search standards; rather, the primary aim for that Amendment was to prohibit the use of general warrants for revenue searches of houses for untaxed goods." *Id.* at 56.

231. Although technology enhanced policing has resulted in increased safety and less policy-citizen violence, press coverage regarding new enhancements has generally focused on negative implications. *See* Bryce Clayton Newell, *Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information*, 66 ME. L. REV. 397, 398–99 (2014). However, "less attention has been given to balancing these privacy interests with the important societal interest in promoting effective and efficient police work. The tensions between these competing, equally legitimate aims is substantial." *Id.* at 399.

232. *See, e.g.*, Heather Baxter, *Right Result, Wrong Reason: Why the Intent Requirement in* Florida v. Jardines *Trespasses on the Clarity of the Fourth Amendment*, 51 TEX. TECH L. REV. 217, 230 (2019) (noting that the result in *Florida v. Jardines* was surprising). Justice Sotomayor, in her concurring opinion in *Jones*, spelled out the implications on privacy of long-term GPS monitoring:

> 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. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques.

United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

233. *See, e.g.*, Samson v. California, 547 U.S. 843, 848 (2006); United States v. Knights, 534 U.S. 112, 118 (2001); Ohio v. Robinette, 519 U.S. 33, 39 (1996).

expectation of privacy, given their particular environments.[234] A person's locale at the time of the search weighs heavily in determining whether an expectation of privacy was reasonable.[235] Although defining what constitutes a societally acceptable reasonable expectation of privacy is generally impossible, the Court has established several doctrines and revealed certain analytical tendencies that provide some guidance to lower courts and law enforcement.

1. Unprotected Faces: Public Exposure Doctrine

"What a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection."[236] Thus, law enforcement's observations of anything put on public display are not "searches" at all.[237] This rationale naturally leads to the conclusion that a person's uncovered face has no privacy protections, but the Court did not leave this to mere conjecture. In *United States v. Dionisio*, the Court, in dicta, explained that a person has no reasonable expectation of privacy of their face.[238] No one would find it reasonable to preclude a police officer from looking at faces of people on the street nor would anyone bar that

---

234. *See, e.g.*, *Samson*, 547 U.S. at 852 (parolees); *Knights*, 534 U.S. at 119–20 (probationers); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 656–57 (1995) (student-athletes); Hudson v. Palmer, 468 U.S. 517, 525–26 (1984) (prisoners).

235. *See* Michael J. Zydney Mannheimer, *Decentralizing Fourth Amendment Search Doctrine*, 107 KY. L.J. 169, 179 (2018) (citing United States v. Dunn, 480 U.S. 294, 303–04 (1987); Oliver v. United States, 466 U.S. 170, 179–81 (1984)). The Fourth Amendment expressly protects citizens' "persons, houses, papers, and effects" from unreasonable warrantless searches. U.S. CONST. amend. IV. Houses may include hotel rooms, apartments, automobiles, occupied taxis, and business offices. *See* Lanza v. New York, 370 U.S. 139, 143–44 (1962) (finding that a prison cell did not share the attributes of a "house" under the meaning of the Fourth Amendment because official surveillance was the traditional norm but identifying the listed places as being included as "houses" in other cases). However, outside the home, the constrictions on law enforcement searches vanish almost entirely, even if police look into areas close to the home. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 450–52 (1989) (fenced area visible by air from helicopter not protected by Fourth Amendment); California v. Greenwood, 486 U.S. 35, 40 (1988) (no reasonable expectation of privacy of one's trash); California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (fenced area visible from air by airplane not protected by Fourth Amendment).

236. Katz v. United States, 389 U.S. 347, 351 (1967).

237. United States v. Dionisio, 410 U.S. 1, 14 (1973).

238. *Id.* The Court in *Dionisio* found that the Fourth Amendment did not protect from discovery a defendant's voice. *Id.* The Court analogized a person's voice to their face, noting that

> 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.

officer from approaching people they recognized as known or suspected criminals.[239]

Moreover, in a recent civil case, one U.S. district court judge applied the public exposure rationale to FRT. In *Rivera v. Google, Inc.*, a plaintiff attempted to differentiate a face, which it admitted was not "private," from the biometric information of the face, which it contended deserved privacy protections.[240] The court rejected that argument, holding that because the biometric face template was created from "otherwise public information," it was not private.[241]

Nonetheless, the Supreme Court has expressed that "[a] person does not surrender all Fourth Amendment protections by venturing into the public sphere."[242] While the Court has not defined the limits of the exception to the public exposure doctrine, it has repeatedly deferred to what law enforcement would have been able to learn about a suspect without a warrant at the time of the Fourth Amendment's drafting.[243] A person's exposed face would seem to fall within that category, and, therefore, the FRT scan would not constitute a search. More importantly, if taken at face value, the public exposure doctrine would likely extend to photographs shared with the public—on social media, for example. Moreover, the third-party doctrine could expose *any* information shared with a third

239. Courts have consistently treated a face as having no privacy protections under the Fourth Amendment. *See id.*; *see also In re* Melvin, 550 F.2d 674, 676 (1st Cir. 1977) ("[I]t seems clear that one has no more reasonable expectation of privacy in one's face than in one's voice, and that being forced to stand in a lineup does not result in an unconstitutional 'seizure'."); United States v. Anthony, No. 4:18-CR-00012, 2019 WL 471984, at *3 (W.D. Va. Feb. 5, 2019) ("The court holds that defendants have no reasonable expectation of privacy to their heads, faces, necks, arms, and hands.").

240. 366 F. Supp. 3d 998, 1012 (N.D. Ill. 2018).

241. *Id.*

242. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018). The *Carpenter* Court acknowledged that "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* (quoting Katz v. United States, 389 U.S. 347, 351–52 (1967)).

243. *See, e.g.*, *Carpenter*, 138 S. Ct. 2217; Riley v. California, 573 U.S. 373, 403 (2014); United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring); Kyllo v. United States, 533 U.S. 27, 40 (2001); Carroll v. United States, 267 U.S. 132, 149 (1925) ("The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens.").

party—even companies that store photos hidden from public view[244]—reachable without a warrant.

2. Third-Party Doctrine

The third-party doctrine intimates that any information shared with a third-party is obtainable by government agents without a warrant.[245] The Court created the third-party doctrine in *Miller v. United States*[246] and reinforced it three years later in *Smith v. Maryland*.[247] The third-party doctrine provided a clear, bright-line rule within the otherwise murky waters left by *Katz*: information possessed by a third party is not private and has no Fourth Amendment protection.[248] Although the doctrine was a blunt instrument that failed to "acknowledge gradations in the sensitivity of information citizens disclose to others" in modern times,[249] it remained fully in force for over forty years until the Court delivered its holding in *Carpenter v. United States*.[250]

In *Carpenter*, the Court surprised legal scholars by departing from the third-party doctrine.[251] "[T]he majority emphatically rejected the government's argument that people lose their privacy rights when using

---

244. For example, not all photographs on social media are public. *See, e.g.*, Brian Barrett, *The Complete Guide to Facebook Privacy*, WIRED (Mar. 21, 2018, 1:10 PM), https://www.wired.com/story/facebook-privacy-apps-ads-friends-delete-account [https://perma.cc/5RKY-YKFP]. Some are set to private or restricted to friends-only viewing. *See id.* Some users keep information on third-party servers for storage purposes only. *See, e.g.*, DROPBOX, https://www.dropbox.com/out-of-space?oqa=wb_oq_rd_hm [https://perma.cc/9D4E-VRVG].

245. United States v. Miller, 425 U.S. 435, 443 (1976).

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Id. For a detailed discussion of the third-party doctrine, see generally Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

246. 425 U.S. 435 (1976). In *Miller*, the defendant objected to the use of his bank records against him, but the Court ruled "that a person has no 'legitimate expectation of privacy' in information he or she voluntarily provides to third parties." MURPHY, *supra* note 136, at 27 & n.10 (citing *Miller*, 425 U.S. at 442–44).

247. 442 U.S. 735 (1979). *Smith* involved law enforcement's use of a pen register, which allowed law enforcement to learn the numbers dialed by the defendant. *Id.* at 737. The Court held that the defendant had no legitimate expectation of privacy in the numbers he dialed because the telephone company collected that information. *Id.* at 744–45.

248. *See* Michael Gentithes, *The End of* Miller*'s Time: How Sensitivity Can Categorize Third-Party Data After* Carpenter, 53 GA. L. REV. 1039, 1054 (2019).

249. *Id.* at 1053–54.

250. 138 S. Ct. 2206 (2018).

251. *See* Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 363 (2019).

[cellular] technologies, intimating that the third-party doctrine is less of a bright-line rule and more of a fact-specific standard."[252] The Court carefully limited its holding to the facts of the case,[253] which has been interpreted narrowly as applying only to the tracking of an individual's movements over time.[254] The Court did not overrule *Miller* or *Smith* and left the third-party doctrine standing, although on shaky legs.[255] However,

252. Gee, *supra* note 9, at 428–49. On a related note, the use of cell phones as containers of massive amounts of personal information means that they amount to "papers" in the context of the Fourth Amendment as intended by the Framers. *See* Leah Aaronson, *Constitutional Restraints on Warrantless Cell Phone Searches*, 69 U. MIAMI L. REV. 899, 924 (2015). "Papers," at the time of the Framing, included notes, journals, and anything written on a sheet of paper. Jeffrey Bellin, *Fourth Amendment Textualism*, 118 MICH. L. REV. 233, 261 (2019). Today, these types of records are maintained electronically, and these electronically stored records deserve equivalent Fourth Amendment protections. *Id.* "Books and journals are now 'PDF' files and word-processing documents. Emails and text messages are today's letters and notes." *Id.* However, not all electronic information should be classified as Fourth Amendment protected "papers." "[E]lectronic information that is not consciously communicated or stored—such as a notification sound that rings out upon receipt of a text message or an electronic ping emitted by a cell phone, remote control, or door opener—would not constitute one's 'papers.'" *Id.* at 261–62.

253. *Carpenter*, 138 S. Ct. at 2220 ("Our decision today is a narrow one."); *see also* Hamann & Smith, *supra* note 24 at 12. The narrow facts of *Carpenter* are "that an individual maintains a legitimate expectation of privacy in the 'record of his physical movements as captured through [cell site location information (CSLI)].'" MURPHY, *supra* note 136, at 31. The Court "chose not to decide whether there is a limited period for which the Government may obtain an individual's historical CSLI 'free from Fourth Amendment scrutiny' and limited its main finding to declaring that access to seven days of CSLI constitutes a Fourth Amendment search." *Id.* (citing *Carpenter*, 138 S. Ct. at 2266). While the rationale of the majority in *Carpenter* seems ripe for extension to other categories of technology, the opinion fails to provide much in the way of guidance "for citizens, law enforcement, and lower courts" for even matters closely related to the core issues in *Carpenter*. *See id.* at 32. Lower courts have taken this narrowness directive quite literally. *See* Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J.F. 943, 950 (2019).

> For example, one district court has held that *Carpenter* did not apply to grand jury subpoenas sent to an internet service provider (ISP) and an email provider for subscriber information associated with an ISP account and an email address: "The privacy interest in this type of identifying data . . . simply does not rise to the level of the evidence in *Carpenter* such that it would require law enforcement to obtain a search warrant."

Id. at 950 (quoting United States v. Tolbert, 326 F. Supp. 3d 1211, 1225 (D.N.M. 2018)).

254. *See* Hamann & Smith, *supra* note 24, at 12.

255. MURPHY, *supra* note 136, at 31. Although Professor Ohm noted that *Carpenter* nearly killed the third-party doctrine, Ohm, *supra* note 251, at 363, Murphy notes that the Court instead "opted to distinguish *Miller* and *Smith* on the grounds that 'bank records' and 'telephone numbers' are in a 'qualitatively different' category to cell site records."

the four dissenters in *Carpenter* all expressed some type of support for the third-party doctrine.[256]

The Court's departure from the third-party doctrine has tremendous implications for the use of FRT when evaluating the assembly of facial databases. By rejecting the third-party doctrine, the Court opened the door to extending Fourth Amendment protections to photos shared with third-parties, like social media and other websites. The decision offers criminal defendants many opportunities to attack police practices, as noted by Paul Ohm:

> In sum, criminal defendants will test the outer boundaries of *Carpenter*'s reasoning whenever the police use massive databases assembled by private parties that reveal location information, directly or by inference. Other defendants will challenge the collection of data unrelated to location. The broad reasoning of the majority's opinion will give all of them plenty to work with. Anticipating this, risk-averse police departments will err on the side of caution, getting a warrant for data whenever they can, sometimes turning promising leads into dead ends.[257]

But even stretching the *Carpenter* rationale to its furthest bounds, it is unlikely that the Court will restrict law enforcement from tapping into data collected by government agencies.[258] *Carpenter* confronted data collected by non-governmental parties.[259] Simply put, the altered third-party doctrine is inapplicable to government data because the government is not a third-party at all; rather, it is the prosecution, a direct party in criminal litigation. Accordingly, the data willingly provided by millions of Americans to the government exposes them to reduced privacy rights.

Nevertheless, the *Carpenter* decision opened the door not only to further relaxation of the third-party doctrine but also the public exposure doctrine. These doctrines, if applied as they had been pre-*Carpenter*, would snuff out any legal basis for holding the use of FRT unconstitutional under the Fourth Amendment. However, over the past few decades, the Court has demonstrated that the use of technology imposes additional questions on Fourth Amendment analysis.

MURPHY, *supra* note 136, at 31 (citing *Carpenter*, 138 S. Ct. at 2216). Nevertheless, the logic could potentially "be extended to other—non-location based—categories of information that are conveyed to telecommunications and internet service providers in a future case with different facts." *Id.*

256. *Carpenter*, 138 S. Ct. at 2223–24, 2227–33 (Kennedy, J., dissenting); *id.* at 2244 (Thomas, J., dissenting); *id.* at 2247, 2257–61 (Alito, J., dissenting); *id.* at 2262–64, 2268–69 (Gorsuch, J., dissenting).

257. Ohm, *supra* note 251, at 366.

258. *See* Rebecca Lipman, *Protecting Privacy with Fourth Amendment Use Restrictions*, 25 GEO. MASON L. REV. 412, 446 (2018).

259. *See id.*

3. Technology Enhanced Searches

The drafters of the Constitution could never have conceived of a technology that would allow law enforcement to ascertain the identity of millions of Americans instantly on sight. In crafting the Fourth Amendment, the drafters protected the "persons, houses, papers, and effects" of American citizens from warrantless searches.[260] At the time of drafting, this was a relatively all-inclusive list of what citizens had; people's records and information were usually kept in their homes—which included offices, shops, and barns.[261] Today, websites capture and retain enormous amounts of personal information via people's behaviors online.[262] The Framers intended to protect "the privacies of life"[263] and "to place obstacles in the way of a too permeating police surveillance."[264] Technology complicates the analysis because enhancing acceptable surveillance tactics by incorporating new technology makes what was previously private by default ascertainable by police. The Court has shown that it is willing to depart from traditional Fourth Amendment doctrines due to technological developments.

In *Kyllo v. United States*, the Court analyzed the use of sense-enhancing technology by law enforcement under the Fourth Amendment.[265] In that case, a federal agent used thermal imaging to look through the walls of a suspected marijuana grower's home.[266] The Court deemed the use of the

260. U.S. CONST. amend. IV.

261. Collins T. Fitzpatrick, *Protecting the Fourth Amendment So We Do Not Sacrifice Freedom for Security*, 2015 WIS. L. REV. 1, 5.

262. *See* Vito Pilieci, *Just How Much of Your Personal Data Is Actually Online? We Take a Look*, OTTAWA CITIZEN (Apr. 2, 2018), https://ottawacitizen.com/news/national/just-how-much-of-your-personal-data-is-actually-online-we-take-a-look [https://perma.cc/N69S-PG4G]. Facebook, Google, and Twitter alone amassed more than 1.66 gigabytes of information for an individual. *Id.* One gigabyte amounts to thousands of pages of documents. *See* John Tredennick, *How Many Documents in a Gigabyte? An Updated Answer to that Vexing Question*, CATALYST (Jan. 13, 2014), https://catalystsecure.com/blog/2014/01/how-many-documents-in-a-gigabyte-an-updated-answer-to-that-vexing-question [https://perma.cc/PT6M-BBWK] (varying by document type, a gigabyte could contain between 505 and 7,085 documents); LEXISNEXIS DISCOVERY SERVS., HOW MANY PAGES IN A GIGABYTE? 1 (2007), https://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf [https://perma.cc/N69S-PG4G] (a gigabyte could contain between 15,477 to 297,317 pages depending on document type).

263. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

264. *Id.* (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

265. 533 U.S. 27 (2001).

266. *Id.* at 29–30.

thermal imaging camera a Fourth Amendment search because "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use."[267] "This 'general public use' test is now used to determine if information gained by new technology is indeed a search."[268]

Courts are unlikely to find law enforcement's use of FRT a search under *Kyllo*. Unlike thermal imaging cameras, which are not in general public use,[269] FRT is widely available for commercial and public use.[270] Moreover, outside the home, the protections added by *Kyllo* evaporate under most lower court interpretations.[271] Many lower court decisions further limit *Kyllo* to restricting law enforcement's use of technology to peer beyond the walls into the target's home.[272] FRT does not implicate concerns of invasion of privacy into the home. Thus, although FRT is a sense-enhancing technology,[273] courts will likely distinguish the use of FRT from the facts of *Kyllo* and find no search occurred.

---

267. *Id.* at 34–35 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)). "To rule [the use of the thermal imaging camera not a search] would allow the police to evade the Fourth Amendment's intended protection of the interior of a private home from warrantless search." Lenz, *supra* note 71, at 279.

268. Baxter, *supra* note 232, at 226.

269. *Kyllo*, 533 U.S. at 34.

270. *See generally* Brandon Amos, Bartosz Ludwiczuk & Mahadev Satyanarayanan, *OpenFace: A General-Purpose Face Recognition Library with Mobile Applications* (Carnegie Melon Univ., Sch. of Comput. Sci., Technical Report No. CMU-CS-16-118, 2016), http://reports-archive.adm.cs.cmu.edu/anon/anon/usr0/ftp/2016/CMU-CS-16-118.pdf [https://perma.cc/A74D-LQK8] (exploring the qualitative differences between the more widely publicly available FRT systems and private, state-of-the-art FRT systems).

271. *See, e.g.*, United States v. Morales-Zamora, 914 F.2d 200, 205 (10th Cir. 1990) (holding that dog sniffs outside a vehicle are not protected under *Kyllo*); United States v. Broadway, 580 F. Supp. 1179, 1191 (D. Colo. 2008) (noting that odors escaping the home are not revealing of intimate details of home's interior); United States v. Vela, 486 F. Supp. 2d 587, 589 (W.D. Tex. 2005) ("There is a clear distinction between the expectation of privacy behind the walls of one's home and the expectation of privacy behind the windows of a vehicle.").

272. *See, e.g.*, United States v. Lambis, 197 F. Supp. 3d 606, 609–10 (S.D.N.Y. 2016) (determining that the use of a cell site simulator to locate a phone within a residence was a search); United States v. Vela, 486 F. Supp. 2d 587, 589–90 (W.D. Tex. 2005) (holding that using night-vision goggles to observe a vehicle was not a search); Baldi v. Amadon, 2004 WL 725618, at *2–3 (D.N.H. Apr. 5, 2004) (deciding that the use of a night scope to observe the exterior of home was not a search).

273. FRT is a sense-enhancing technology that assists and augments a human's natural ability to see, recognize, and identify faces. *See* Amos, Ludwiczuk & Satyanarayanan, *supra* note 270, at 1–3. However, FRT enhances sight significantly less than thermal imaging does—which essentially gave the agents in *Kyllo* superhuman "x-ray" vision. Moreover, even scent-detecting dogs, which can detect odors "at almost non-existent levels,"

The Court has already evaluated how law enforcement may obtain and use data.[274] In *Riley v. California*, the Court analyzed how the immense data contained on cell phones altered the search incident to arrest exception to the warrant requirement.[275] The variety and expansive nature of the information contained on a cell phone combined with the ability to access information beyond the device's storage make reviewing the data on the phone a window into many private aspects of a person's life.[276] Thus, the Court found searching a cell phone without a warrant violated the Fourth Amendment.[277]

In *Carpenter*, the Court implied that pre-digital age search capabilities created assumptions of privacy even when in public places, and the Court wanted to preserve those reasonable privacy presumptions.[278] *Carpenter* established a three-factor test for considering technological advancements as law enforcement search tools: "(1) 'the deeply revealing nature' of the

---

especially when compared to human abilities, have been the subject of *Kyllo* analysis. United States v. Whitaker, 820 F.3d 849, 853 n.1 (7th Cir. 2016).

274. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018); Riley v. California, 573 U.S. 373, 401–03 (2014). For a detailed analysis of how courts have viewed data searches during the electronic data era, see Thomas K. Clancy, *Fourth Amendment Satisfaction-The "Reasonableness" of Digital Searches*, 48 TEX. TECH. L. REV. 37, 38 (2015). Courts began to approach issues involving seizure of computers and data storage devices differently than they had previously approached seizures of documents. *See id.* at 41–49; *see also, e.g.*, People v. Gall, 30 P.3d 145, 162 (Colo. 2001) (en banc) (Martinez, J., dissenting) (noting the fundamental differences between computers and traditional "papers" because of the communication functions of computers and the breadth of personal information contained on such devices). "Fourth Amendment analysis regarding the search and seizure of computers must be approached cautiously and narrowly because of the important privacy concerns inherent in the nature of computers, and because the technology in this area is rapidly growing and changing." *Gall*, 30 P.3d at 165.

275. *Riley*, 573 U.S. at 381, 394.

276. *See id.* at 394–98. Although the Court in *Riley* limited law enforcement's free reign to search the depths of a suspect's cell phone, cell phones present privacy issues that exceed the scope of *Riley*. For example, browsing history—which third party companies' tracking cookies can mine—implicates similar privacy concerns as does information contained on a cell phone. *See* Daniel de Zayas, Comment, Carpenter v. United States *and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History*, 88 AM. U. L. REV. 2209, 2250–51 (2019).

277. *See Riley*, 573 U.S. at 393–98. When the Court established the search incident to arrest exception, the Court only intended to carve out a small exception that was minimally invasive. *See id.* The search incident to arrest exception, based on the Court's holdings in *Chimel v. California*, 395 U.S. 752 (1969), and *Arizona v. Gant*, 556 U.S. 332 (2009), outlines two specific justifications for search incident to arrest: ensuring officer safety and preventing destruction of evidence.

278. *See Carpenter*, 138 S. Ct. at 2217.

information; (2) 'its depth, breadth, and comprehensive reach'; and (3) 'the inescapable and automatic nature of its collection.'"[279] Applying each of these factors to FRT demonstrates why privacy advocates have little faith the Court will protect against FRT's deployment.

First, FRT is not "deeply revealing" in the same way as the Court defines historical cell site location information. The Court returned to its analysis in *Jones*, noting that it was already settled law that individuals have a reasonable expectation of privacy of their physical movements.[280] This is strike one against FRT: in contrast to tracking one's physical movements over time, FRT[281] identifies a person by their face, which is afforded no privacy protections under well-established legal precedent.[282]

Second, FRT does not implicate the same level of "depth, breadth, and comprehensive reach" as does cell site location information.[283] "*Depth* refers to the detail and precision of the information stored[;] *breadth* refers to . . . how frequently the data is collected, and for how long the data has been recorded[;] *comprehensive reach* refers to the number of people tracked in the database."[284] FRT could implicate the *depth* aspect if additional information drawn into the database and provided real-time to officers extends beyond what is commonly available to police agencies today.[285] Nevertheless, the *depth* aspect is unlikely at issue for information contained within state and federal criminal justice databases. The *breadth* aspect requires a durational standard absent from the application of FRT.[286] Thus, no considerations of the *breadth* aspect are appropriate in evaluating FRT searches. However, FRT's implementation implicates the *comprehensive reach* aspect. Looking to government databases of known

---

279. Ohm, *supra* note 251, at 370 (citing *Carpenter*, 138 S. Ct. at 2223).

280. Lipman, *supra* note 258, at 446 (noting that it was Justice Sotomayor's concurrence in *Jones* that laid the foundation for the Court's rationale in *Carpenter*).

281. It is worth noting that FRT can be employed as a means of tracking, by incorporating it into surveillance cameras, compiling data over time, to determine where a person has been. This is the potential next iteration of FRT after its deployment as a tool to immediately identify people in public. The idea of tracking people's movements by automated scanning technology is the subject of scholarly analysis. *See, e.g.*, Brooks, *supra* note 17, at 18 ("By plotting vehicle locations at specific times and tracking their movements, [automated license plate scanners (ALPRs)] can be used to paint incredibly detailed portraits of drivers' lives. These scans can be used to determine past behaviors, predict future ones, to solve crimes, or simply to track an individual's movements. As more ALPRs are used, the portraits they paint will likely continue to grow more detailed and invite potential misuse.").

282. *See supra* Section V.B.1.

283. *See* Ohm, *supra* note 251, at 361 (citing *Carpenter*, 138 S. Ct. at 2223).

284. Ohm, *supra* note 251, at 372–73.

285. For example, information posted to social media, provided to the government for civil purposes, or obtained via other non-law enforcement means.

286. Ohm, *supra* note 251, at 372–73.

faces alone reaches millions of Americans.[287] Adding non-governmental sources of data to the mix makes the reach of FRT almost incomprehensible.

Finally, the collection and compilation of facial photos in FRT databases are neither "inescapable" nor "automatic." This factor identifies that "individuals might sometimes relinquish their Fourth Amendment rights when they assume the risk of surveillance, for example by publishing information to the general public."[288] People willingly—aside from photos captured incident to arrest—provide their images regardless of the collection method.[289] Although FRT captures images automatically and in real-time from a scan, these images are not what comprise the facial databases.[290] Thus, these images are not the kind of "information" collected and stored for future review. Therefore, this final factor does not prevent law enforcement from assembling databases of facial images.

The sum of these factors offers little indication that the Court would find law enforcement's use of FRT unconstitutional, at least under the *Carpenter* test. Although, the *Carpenter* Court's approach hints that increased Fourth Amendment protections may arise out of technology-enhanced policing,[291] nothing in the Court's analysis provides grounds for a constitutional challenge to FRT's use by law enforcement. To privacy advocates, this would not be an ideal result.[292] Moreover, even if the Court does eventually find FRT's use constitutes a search, the delays in the judicial process will necessarily mean the privacy rights of millions of Americans will be infringed upon without legislative action.

---

287. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-579T, *supra* note 89, at 6 (statement of Gretta L. Goodwin, Director Homeland Security & Justice); Garvie, Bedoya & Frankle, *supra* note 66; *see also* FERGUSON, supra note 88, at 97.

288. Ohm, *supra* note 251, at 376.

289. Users publicly post their photos online, allowing third parties and government entities to collect this information. *See* Natalie Kim, Note, *Three's a Crowd: Towards Contextual Integrity in Third-Party Data Sharing*, 28 HARV. J.L. & TECH. 325, 327, 332–33 (2014). Citizens opt to provide their photos to the government to obtain licenses and passports.

290. If FRT cameras—or any other cameras for that matter—were constantly operating and compiling facial images for future review, the analysis under this factor would change. Retroactively reviewing scanned faces captured by these cameras would more likely be unconstitutional.

291. *See* Elizabeth E. Joh, *Artificial Intelligence and Policing: Hints in the* Carpenter *Decision*, 16 OHIO ST. J. CRIM. L. 281, 289 (2018).

292. *See supra* notes 149–51 and accompanying text; *see also* Hamann & Smith, *supra* note 24.

C. Slow Courts, Fast Technology

Establishing new law through the courts occurs at the pace of a snail in molasses, while technology develops at light-speed. New technologies combine[293] to create new challenges that the law has not yet contemplated. Development of case law involving advancing technology is the slowest mode of the law's potential adaptability. Nevertheless, Congress and state legislatures leave many legal issues in the hands of the courts.[294] To challenge the use of FRT by law enforcement, a plaintiff must first establish standing, requiring a concrete injury attributable to the technology.[295] Even once a party navigates the complexity of proving standing, the case must make it through litigation to allow the courts an opportunity to rule.

Furthermore, the likelihood that a legitimate lawsuit goes to trial is minute.[296] Although some case law does arise out of pre-trial motions, the

---

293. Smartphones provide perhaps the best example: the iPhone X combines high definition display, touch-screen, digital camera, microprocessor, FRT, voice-recognition, and battery technologies, to name a few. *iPhone X – Technical Specifications*, APPLE (Aug. 9, 2019), https://support.apple.com/kb/sp770?locale=en_US [https://perma.cc/WLK2-BUU8]. Although this Comment examines the use of FRT by law enforcement, the commercial implications of its use are readily apparent. The combination of FRT with databases facilitates targeted messaging to consumers and collection of individuals' shopping behaviors when they visit brick and mortar locations equipped with FRT cameras. *See* Elias Wright, Note, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 611, 632–33 (2019). Facebook already offers advertisers the option of targeting "core audiences," considering consumers' location, demographics, interests, behaviors, and connections. *Ad Targeting: Help Your Ads Find the People Who Will Love Your Business*, FACEBOOK, https://www.facebook.com/business/ads/ad-targeting [https://perma.cc/B6WK-D92R].

294. There are a variety of explanations for this phenomenon: (1) the issue may not be of substantial importance to garner legislative attention; (2) the specific challenges that cause injury may not be readily apparent until after a harm, *see infra* note 295; and (3) even if legislation is appropriate, the political nature of legislative decision making sometimes render passage through multiple legislative bodies and a signature by an executive a practical impossibility.

295. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992). Standing requires that the plaintiff suffered a concrete and particularized injury that is "fairly . . . trace[able] to the challenged action of the defendant." *Id.* at 560–61 (quoting Simon v. E. Ky. Welfare Rts. Org., 426 U.S. 26, 41 (1976)) (internal quotation marks omitted). The issue of standing is a sticky one under Fourth Amendment analysis. *See generally* Robert H. Whorf, *The Effects of Eliminating the Concept of Fourth Amendment Standing—Thirty Years in Hindsight*, 26 THOMAS M. COOLEY L. REV. 555 (2009) (providing an in-depth examination of the Fourth Amendment standing problem). However, in *Rakas v. Illinois*, the Supreme Court effectively dispelled the notion of Fourth Amendment standing and focused on the substantive Fourth Amendment inquiry. 439 U.S. 128, 140 (1978).

296. *See* Jeffrey Q. Smith & Grant R. MacQueen, *Going, Going, but Not Quite Gone*, JUDICATURE, Winter 2017, at 26, 28, https://judicialstudies.duke.edu/wp-content/uploads/2018/01/JUDICATURE101.4-vanishing.pdf [https://perma.cc/GF5P-894B]. Approximately 1% of civil cases filed in federal court are resolved at trial. *Id.*

high rate of disposition through settlement deprives the judiciary of the opportunity to create law.[297] It can take years for the rare case that does go to trial to make it to that phase of litigation.[298] Because courts may not have the opportunity to rule on FRT for an extended period, the technology could become entrenched in law enforcement practices before courts consider its constitutional implications.

In the Fourth Amendment context, new technology exposes the weaknesses of the slow process of judicial law creation. It took the Court over a decade to address law enforcement's use of thermal imaging as it eventually did in *Kyllo*.[299] The search of a cell phone incident arrest, the

---

297. *See id.* at 35. The continued evolution necessary for the development of common law suffers because of the trend away from trials.

> Another weighty concern is how the disappearance of trials impacts the development of the law itself. There are several aspects to this issue. First, there is the danger that law developed only through motions "will be arid, divorced from the full factual content that has in the past given our law life and the capacity to grow."

Id. (quoting Stephen B. Burbank, *Vanishing Trials and Summary Judgment in Federal Civil Cases: Drifting Toward Bethlehem or Gomorrah?*, 1 J. EMPIRICAL LEGAL STUD. 591, 625–26 (2004)). The authors go on to note additional aspects of the issue:

> Second, the diminishing number of trials will no doubt produce less law relating to the types of issues that arise at trial. This, in turn, may lead to greater uncertainty about trial outcomes and substantive law. . . . Third, the lack of trials also means there are fewer actual verdicts to serve as markers or data points for valuing claims.

Id. (citations omitted) (citing Amanda M. Rose, *The "Reasonable Investor" of Federal Securities Law: Insights from Tort Law's "Reasonable Person" & Suggested Reforms*, 43 J. CORP. L. 77, 113–14 (2017)).

298. *See* U.S. CTS., TABLE 6.3 U.S. DISTRICT COURTS—MEDIAN TIME INTERVALS (IN MONTHS) FROM FILING TO DISPOSITION FOR CIVIL CASES AND CRIMINAL DEFENDANTS (2018), https://www.uscourts.gov/sites/default/files/data_tables/jff_6.3_0930.2018.pdf [https://perma.cc/5NQ5-LF9U]. The average time from filing to disposition in civil matters is over twenty-six months when the matter goes to trial. *Id.* This duration has been steadily growing, from eighteen months in 1995 to over twenty-six months in 2018, more than a 45% increase. *Id.* There is little reason to believe that this trend will abate. Thus, the development of common law is proportionately slow.

299. By the early 1990s, thermal imaging was in regular use by law enforcement. *See* Susan Moore, *Does Heat Emanate Beyond the Threshold?: Home Infrared Emissions, Remote Sensing, and the Fourth Amendment Threshold*, 70 CHI.-KENT L. REV. 803, 810–11 & n.37 (1994). Academics addressed the issue around the same time. *See, e.g.*, *id.*; Mindy G. Wilson, *The Prewarrant Use of Thermal Imagery: Has This Technological Advance in the War Against Drugs Come at the Expense of Fourth Amendment Protections Against Unreasonable Searches?*, 83 KY. L. REV. 891 (1995). The U.S. District Court for Hawaii confronted the issue of thermal imaging's use as a search of the home as early as 1991, which was subsequently reviewed by the Ninth Circuit in 1993. United States v. Penny-Feeney, 773 F. Supp. 220 (D. Haw. 1991), *aff'd*, 984 F.2d 1053 (9th Cir. 1993).

subject of *Riley*, took even longer—almost twenty-five years—for the Court to rule upon.[300] Cell site location information was used by police agencies as evidence of a suspect's location in criminal trials for as long as that information was known to be available before being addressed by the Court in *Carpenter*.[301] During the intervening years, countless citizens were the subject of searches that the Court later decided were unconstitutional.[302] Although some of these searches captured information later used to convict those guilty of criminal acts, the police unconstitutionally infringed upon the privacy rights of innumerable innocent people, as well.[303]

FRT poses an even greater risk to Americans' privacy. The examples mentioned above all involve a level of targeting specific people. Thermal imaging targeted *particular* suspects' homes;[304] searching cell phones incident to arrest involved *individuals* already under arrest; and, law enforcement requested cell site location information to service providers for *specific* people.[305] Operators of FRT cannot target suspects in the

---

"In the court's view, the thermal imager was an extra-sensory, non-intrusive device." Annabelle L. Lisic, *Thermal Imaging and the Fourth Amendment*, MD. B.J., Jan.–Feb. 2001, at 16, 20. In contrast, the Court in *Kyllo* held that "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." Kyllo v. United States, 533 U.S. 27, 40 (2001).

300. *See* Allison A. Murphy, *Criminal Law*—Smith v. Indiana*: Pushing the Envelope of Unreasonable Searches and Seizures*, 23 AM. J. TRIAL ADVOC. 447, 449 (1999) (citing United States v. Meriwether, 917 F.2d 955 (6th Cir. 1990) (holding that the Fourth Amendment protections do not apply to a phone number seized from a pager)).

301. *See* Shannon Jaeckel, *Cell Phone Location Tracking: Reforming the Standard to Reflect Modern Privacy Expectations*, 77 LA. L. REV. 143, 146 (2016). *See generally* Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L.J. 381 (2003) (analyzing police use of CSLI to track suspects' movements in the late 1990s and early 2000s).

302. *See* Mana Azarmi, *Location Data: The More They Know,* CTR. FOR DEMOCRACY & TECH. (Nov. 27, 2017), https://cdt.org/insights/location-data-the-more-they-know/ [https://perma.cc/A8ZB-VUMG].

303. *See id.*

304. *See* Lisic, *supra* note 299, at 20 (noting that the use of a thermal imager often followed lengthy investigations into a suspect's illicit drug activities).

305. However, the *Carpenter* court limited its holding, excluding "tower dumps," which allow companies to obtain the information of every person whose phone communicated with a cell tower over a specified period of time. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018). Justice Gorsuch expressed his dissatisfaction with the majority's exclusion of tower dumps, writing:

> Why isn't a tower dump the *paradigmatic* example of "too permeating police surveillance" and a dangerous tool of "arbitrary" authority—the touchstones of the majority's modified *Katz* analysis? On what possible basis could such mass data collection survive the Court's test while collecting a single person's data does not? Here again we are left to guess.

Id. at 2267 (Gorsuch, J., dissenting).

same way. An FRT camera scans every person who comes within its line of sight; the identification process invades each person's privacy almost instantaneously. Where searches later determined to be unconstitutional under *Kyllo*, *Riley*, and *Carpenter* likely resulted in the invasion of thousands of people's privacy, almost every person who ventures outside could have their privacy exposed in a jurisdiction with FRT-equipped police. If left to the courts alone, this result is unavoidable. As illustrated by the analysis above, the Court is ill-equipped to deal with the question of cutting-edge technology implemented by law enforcement.[306] The tool the Court lacks to be able to do this effectively is legislation that addresses FRT head-on.[307]

VI. A PROPOSED CONGRESSIONAL STATUTORY SOLUTION

Congress is in the best position to address the use of FRT and its invasion into the private lives of Americans. Any state-enacted legislation is likely incapable of addressing the issues of FRT because it is not an isolated state issue. Instead, this is a national problem that only the federal government can properly address. However, the national character of the issue is not the only justification for congressional action. The legislative

306. *See* Kerr, *supra* note 161, at 809 ("When technology is new or in flux, and its use may have privacy implications far removed from property law, Fourth Amendment rules alone will tend not to provide adequate privacy protections. Statutory protections are needed to protect privacy and regulate government uses of developing technologies."). More generally, some academics note that courts are not capable of regulating police at all. *See, e.g.*, BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 73 (2017) ("It is time to face the facts. The courts are not up to the task of regulating policing. At best, all courts can do is declare, after the fact, whether what the police did was consistent with the Constitution. They can't (and really shouldn't) write detailed policing policies designed to keep things from going wrong in the first place. . . . Indeed, the courts are even less democratically accountable than the police themselves."). Accordingly, Congress must act to protect privacy rights from over-policing. *See infra* Part V.

307. More than just FRT, this issue extends into other areas of expanding policing capabilities due to technological advancement. Other biometric identifying devices deserve similar critique. The accumulation of data is also unprecedented in the history of policing —how much should society allow police to know about Americans without taking investigative measures authorized at some level? This Comment does not address this line of inquiry or related questions; however, these issues are also worthy of in-depth analysis to determine whether the courts can resolve them within the current legislative landscape.

branch must impose checks on the executive branch to maintain a balance of powers between the three branches of government.[308]

Congress should act because it alone has the power to write statutes governing the agencies responsible for amassing databases of photos necessary for the full development of FRT—currently the FBI.[309] Although the FBI falls under the Department of Justice (DOJ),[310] which is an executive department,[311] statutory provisions guide some practices and procedures of the DOJ as a whole[312] and the FBI specifically.[313] For example, 28 U.S.C. § 534 requires the FBI to collect criminal and identification information and distribute it to appropriate agencies.[314] It is this provision that authorized the FBI to amass its biometric databases;[315] however, congressional regulation stops short of further limiting the FBI.[316]

The only limitations on what images the FBI adds to its facial recognition database are its internal policies.[317] However, federal agencies have also tapped into databases of facial photos that the FBI's policies exclude from its databases.[318] This demonstrates that the FBI's policies are insufficient to prevent privacy invasions. Further, if the FBI deviates from its internal policy, there are no legal ramifications. Thus, Congress should not only make the FBI's policies unbreakable but should also limit other federal agencies from creating their own FRT guidelines.

The statute must specifically address FRT[319] because, when it comes to advancing technology, applying a wide brush stroke is not effective. The intricacies of this technology's application differ from that of other

---

308. *See* Todd David Peterson, *Procedural Checks: How the Constitution (and Congress) Control the Power of the Three Branches*, 13 DUKE J. CONST. L & PUB. POL'Y 211, 251–63 (2017).

309. *See supra* Section II.B.1.

310. 28 U.S.C. § 531 ("The Federal Bureau of Investigation is in the Department of Justice.").

311. *Id.* § 501 ("The Department of Justice is an executive department of the United States at the seat of Government.").

312. *See, e.g.*, *id.* §§ 509–510, 516–519.

313. *See, e.g.*, *id.* §§ 534–535, 538.

314. *Id.* § 534; *see also infra* notes 324–27 and accompanying text.

315. Carrero, *supra* note 179, at 601 ("[T]he FBI cited 28 U.S.C. § 534 to permit the implementation and operation of the NGI System. This statute is broad enough to allow any piece of information that relates to identification records to be stored in a database . . . ." (citing DeLillo, *supra* note 178, at 266)).

316. *See id.* ("Essentially, the existing United States privacy laws do not offer much protection from government collection and misuse of biometric data.").

317. *See supra* notes 75–81 and accompanying text.

318. *See supra* notes 82–85 and accompanying text.

319. Although not the subject of this Comment, Congress could apply a similar approach to law enforcement's use of other biometric information for identification purposes.

technologies, and legislation should address FRT directly.[320] Legislators have spoken out about the disparities in FRT's capabilities in identifying women and people of color,[321] which should factor into the crafting of legislation. Until developers eliminate racial and gender biases from FRT systems, allowing law enforcement to use the technology risks disparate treatment of minority groups by law enforcement agencies. Assuming the technology improves—as is likely—and FRT becomes bias-free, Congress must draft FRT legislation that addresses issues specific to FRT. The specific issues involving FRT that Congress must consider in drafting legislation are (1) how law enforcement obtains the photos that comprise the facial database and the privacy implications inherent in the photos' acquisition; (2) the purpose of FRT's use; and (3) the interests in identifying deceased and missing persons.[322]

Congress must enact a statute to directly address the use of FRT by law enforcement. Legislators must balance the public policy benefits of allowing the use of FRT against the privacy rights of the general population.[323] The statutory scheme can achieve this balancing with two express measures. First, the amended law must limit the photographs included in any law enforcement FRT databases to those obtained via criminal investigations and subsequent to arrest or incarceration. Second, the statute must authorize a non-law enforcement agency, such as the Department of Health and Human Services, to maintain a separate database of faces for non-criminal FRT tasks, such as identifying missing or deceased persons.

---

320. Lawmakers could also incorporate this into a more complex statutory scheme applying to either law enforcement search tools or biometric information obtained by the government more generally. This Comment merely aims to establish that lawmakers should not lump FRT into broader categorical legislation that leaves too much open for interpretation —and potential exploitation—by law enforcement agencies and provides little guidance to the courts.

321. *See* Siegel, *supra* note 56. Representative Alexandria Ocasio-Cortez (D-N.Y.) addressed the issues of FRT in public statements made in 2019: "We have a technology that was created and designed by one demographic, that is only mostly effective on that one demographic, and they're trying to sell it and impose it on the entirety of the country." *Id.* Representative Rashida Tlaib (D-Mich.) has publicly stated "that facial recognition technology is broken." *Id.*

322. *See* 28 U.S.C. § 534(a)(2)–(3).

323. For example, the public interest in identifying missing and deceased persons outweighs individual privacy rights. *See supra* Part III. Additionally, information obtained via criminal investigations should garner no privacy protections.

A. Proposed Amendment to the Current Statutory Scheme

The most logical place to start is with 28 U.S.C. § 534, which governs the collection of biometric information. The statute currently reads, in relevant part:

> (A) The Attorney General shall—
>
> (1) acquire, collect, classify, and preserve identification, criminal identification, crime, and other records;
>
> (2) acquire, collect, classify, and preserve any information which would assist in the identification of any deceased individual who has not been identified after the discovery of such deceased individual;
>
> (3) acquire, collect, classify, and preserve any information which would assist in the location of any missing person . . . and provide confirmation as to any entry for such a person to the parent, legal guardian, or next of kin of that person . . . ; and
>
> (4) exchange such records and information with, and for the official use of, authorized officials of the Federal Government, including the United States Sentencing Commission, the States, including State sentencing commissions, Indian tribes, cities, and penal and other institutions.[324]

This Comment proposes the following changes—indicated in italics—to § 534:

> (A) The Attorney General shall—
>
> (1) acquire, collect, classify, and preserve *information obtained related to* criminal identification *and* crime; *and*
>
> (a) *any images added to the database or repository must be obtained via criminal investigations, incident to arrest, or by penal institutions;*
>
> (b) *images from any other source, including but not limited to state driver's license and identification records, applications for civil licenses, State Department records, legal immigration procedures, or from any non-governmental entity may only be collected under the parameters specified by subsection (a)(1)(A);*

---

324. 28 U.S.C. § 534.

> (2) exchange such records and information with, and for the official use of, authorized officials of the Federal Government, including the United States Sentencing Commission, the States, including State sentencing commissions, Indian tribes, cities, and penal and other institutions.[325]

The second aspect of the proposed legislative solution proposes a new provision within Title 42 of the U.S. Code:

> (A) *The Secretary of Health and Human Services shall—*
> (1) acquire, collect, classify, and preserve any information which would assist in the identification of any deceased individual who has not been identified after the discovery of such deceased individual;
> (2) acquire, collect, classify, and preserve any information which would assist in the location of any missing person . . . and provide confirmation as to any entry for such a person to the parent, legal guardian, or next of kin of that person . . . ; *and*
> (3) exchange such records and information with, and for the official use of, authorized officials of the Federal Government, including the United States Sentencing Commission, the States, including State sentencing commissions, Indian tribes, cities, and penal and other institutions *only when—*
> (a) *pursuant to an authorized warrant; or*
> (b) *in response to a written request that expressly relates to the rationale for collecting the information under subsections (a)(1)–(2).*[326]

The above revised statutory scheme separates the management and administration of the criminal database from that of the non-criminal database. The first amendments remove the non-criminal database from the Attorney General's authority. Further, these changes expressly limit how the Attorney General may assemble the criminal database of images to law enforcement and correctional inputs alone. The second, newly-

325. *See id.* (amended portions in italics).
326. *See id.* (amended portions in italics).

proposed addition to Title 42 puts the burden of maintaining a more general database in the hands of the Secretary of Health and Human Services.[327] For this database, no limitations are necessary. The rationale for these proposed changes follows.

B. Government Maintained FRT Databases

1. Limits on Compiling Databases of Faces

Congress should pass legislation that limits the source of photographs in databases maintained by law enforcement—both federally and for collaborations extending across state lines. With no protection likely to come from the bench and Congress's express authorization to compile and share biometric information of American citizens for a wide array of reasons, in the current legal landscape, law enforcement can run wild with FRT.

Moreover, the use of driver's license databases with FRT creates a multitude of issues. ICE's recent access to state DMV records to identify immigrants for deportation is particularly concerning. As noted above, FRT is not entirely accurate, especially when it comes to identifying members of minority groups.[328] Notably, the leading countries of origin for removals are all in Latin America with primarily Latino populations,[329] and over 18% of the American population identifies as Hispanic or Latino.[330] The combination of the risk of misidentification with the targeting of a minority population is ripe for disparate treatment of that minority group.

Perhaps most frightening, the only limitations on the FBI's compilation of its FRT database are self-imposed.[331] Although the FBI claims it does not allow its investigative teams or other law enforcement agencies to access the FBI's civil database,[332] there is no external legal requirement for such a limitation. Thus, the new statutory scheme should impose that external limitation. The identification photographs in any law enforcement

---

327. While this solution proposes that the Department of Health and Human Services should be responsible for maintaining the non-criminal database, this is merely a suggestion of one governmental entity that could manage such a database. Another entity, assuming its authority does not fall below the Attorney General or another law enforcement official—such as the Census Bureau—would not run contrary to this proposal.

328. *See supra* notes 44–47 and accompanying text.

329. *See FY 2016 ICE Immigration Removals*, U.S. IMMIGR. & CUSTOMS ENFORCEMENT (Dec. 5, 2017), https://www.ice.gov/removal-statistics/2016 [https://perma.cc/S73E-DHQP]. The leading countries of origin for removals in 2016 were Mexico, Guatemala, Honduras, and El Salvador. *Id.*

330. *QuickFacts: United States*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/fact/table/US/PST045219 [https://perma.cc/3TK5-DM2Z] (18.5%).

331. *See supra* notes 79, 309–19 and accompanying text.

332. *See supra* notes 78–79 and accompanying text.

FRT database should only include photographs obtained via criminal investigations, subsequent to arrest, and obtained by correctional institutions.

2. Establishing an Unidentified Persons Database Managed by a Non-Law Enforcement Agency

The statute should also expressly authorize the creation of a separate database exclusively for identifying missing and deceased persons. However, to prevent misuse and confusion, an agency whose primary aim is not criminal law enforcement should compile and maintain this separate database. This solution keeps the two sets of data compartmentalized and allows the administrating agency to compile the latter database from images obtained via a wide array of sources. Because the public interest in identifying deceased and missing persons outweighs privacy rights, this database would face far less stringent limitations.

Moreover, tasking an agency outside the Attorney General's authority with the responsibility of administrating furthers the goal of identifying missing and deceased persons. A statutory limitation on how the government uses citizens' images mitigates fears of government malfeasance. Although some privacy advocates may object to the government maintaining any such database, this approach balances the government's legitimate need for identifying the missing and deceased with over-surveillance and privacy concerns. Thus, the agency in charge of this database could tap into a wide array of publicly available images and even contract with private corporations that specialize in identification and assembly of databases.[333]

3. The Criminal Database

Information and photographs obtained via criminal investigation deserve their own database and administration. First, a person should know whether their photograph is, or could be, in the hands of law enforcement.[334] Further, a total bar on the use of FRT by law enforcement does not serve the best interests of society at-large. Police should integrate developing technologies, such as FRT, into their law enforcement techniques to protect the general

333. *See supra* notes 59–65 and accompanying text.

334. Law enforcement possesses mugshots and prison inmate photos; however, protections under this proposed legislation should afford images obtained when investigating a crime, such as images captured by surveillance cameras at a crime scene. By committing a crime, a person loses the protection of their image captured incident to their criminal activity.

population from criminal actors. This Comment argues that protection should not, however, come at the expense of diminished privacy to the entire population. Further, the law already limits the rights of convicted criminals—a notion society readily accepts.[335] Even though law enforcement photos would include more than just photos for convicted criminals—booking photos for arrestees who are not ultimately convicted of an offense, for example—the Court has already addressed that arrestees have a diminished expectation of privacy.[336] By creating a subset of rules for

---

335. *See* Ann Cammett, *Shadow Citizens: Felony Disenfranchisement and the Criminalization of Debt*, 117 PENN ST. L. REV. 349, 361 (2012).

> In the modern era, criminal disenfranchisement laws persist and largely withstand constitutional scrutiny. Courts closely analyze the constitutionality of state restrictions on the right to vote under fundamental rights jurisprudence. Since voting has been deemed a fundamental right, states must show that restrictions on voting are necessary pursuant to a compelling governmental interest, are narrowly tailored, and are the least restrictive means of achieving the state's objective. However, felon disenfranchisement laws have been exempted from the standard fundamental rights/equal protection analysis since the Supreme Court's decision in *Richardson v. Ramirez*.

Id. at 361–62 (footnotes omitted) (first citing Reynolds v. Sims, 377 U.S. 533, 561–62 (1964); then citing Richardson v. Ramirez, 418 U.S. 24 (1974)). However, "[t]he disenfranchisement of felons has long been challenged as anti-democratic and disproportionately harmful to communities of color." *Id.* at 349. Although there has been some liberalization of the restrictions on felon voting rights, felons still face obstacles to regaining the right to vote. *Id.*

In addition to losing the right to vote, convicted felons lose other rights under state law—varying state to state—including international travel, gun ownership, jury service, employment in certain areas, public social and housing services, and parental rights. *What Rights Do Convicted Felons Lose?*, LAW DICTIONARY, https://thelawdictionary.org/article/what-rights-do-convicted-felons-lose [https://perma.cc/K5FX-PEW5]. Like voting rights, the restrictions on other restrictions on the rights of felons have loosened to varying degrees. One result arising out of the Supreme Court's decision in *District of Columbia v. Heller*, 554 U.S. 570 (2008), is the loosening of restrictions on gun ownership by felons. *See generally* Deborah Bone, *The* Heller *Promise Versus the* Heller *Reality: Will Statutes Prohibiting the Possession of Firearms by Ex-felons Be Upheld After* Britt v. State*?*, 100 J. CRIM. L. & CRIMINOLOGY 1633 (2010). Two circuit courts upheld the Federal Firearms statute—which prohibits the possession of firearms by convicted felons—"on the grounds that the Second Amendment did not create an individual right to bear arms." *Id.* at 1634–35 (first citing Cases v. United States, 131 F.2d 916, 923 (1st Cir. 1942); then citing United States v. Tot, 131 F.2d 261, 266 (3d Cir. 1942), *rev'd*, 319 U.S. 463 (1943)). However, "[w]ith its decision in *Britt v. State*, [681 S.E.2d 320 (N.C. 2009),] the North Carolina Supreme Court became the first court in the country to hold that a statute criminalizing firearm possession by an ex-felon is unconstitutional as applied to the challenging plaintiff under a state constitution." Bone, *supra*, at 1633.

336. *See* Maryland v. King, 569 U.S. 435, 447–48 (2013). The Court ruled that

> In some circumstances, such as "[w]hen faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable." . . .

criminal photos, Congress could expressly authorize the FBI's administration of its NGI facial recognition system and codify the FBI's internal policies that protect the privacy rights of the innocent.

Furthermore, by keeping the criminal photo database compartmentalized from photos obtained via other means, other federal law enforcement agencies—including ICE—cannot run warrantless FRT searches through state DMV photo records. No one expressly agreed to allow law enforcement to include the image of their face in facial recognition searches when they obtained a driver's license. Also, society has a keen interest in people obtaining driver's licenses[337] and photo identification more generally.

The separation of databases also does not preclude law enforcement from obtaining driver's license information from state DMVs as long as law enforcement's request is coupled with a named target.[338] A total bar on law enforcement's ability to obtain driver's license information and photos could be crippling. Importantly, this Comment's proposed rule would even allow law enforcement to use FRT in conjunction with facial images obtained for driver's license issuance.[339] Law enforcement could acquire the image of a known person's face from the state DMV and then use that image within an FRT system. This Comment's proposed rule would only limit the reverse—using the DMV records to identify an unknown person.

. . .

> The instant case can be addressed with this background. The Maryland DNA Collection Act provides that, in order to obtain a DNA sample, all arrestees charged with serious crimes must furnish the sample on a buccal swab applied, as noted, to the inside of the cheeks. The arrestee is already in valid police custody for a serious offense supported by probable cause. The DNA collection is not subject to the judgment of officers whose perspective might be "colored by their primary involvement in 'the often competitive enterprise of ferreting out crime.'"

Id. (citations omitted) (first quoting Illinois v. McArthur, 531 U.S. 326, 330 (2001); then quoting Terry v. Ohio, 392 U.S. 1, 12 (1968)). Similarly, the photos obtained by the police following valid arrests should carry no special protections.

337. *See supra* note 103 and accompanying text.

338. DMV records serve an important function to law enforcement, and state laws authorize law enforcement access to particular information. *See, e.g.*, *How Your Information Is Shared*, CAL. DEP'T MOTOR VEHICLES, https://www.dmv.ca.gov/portal/driver-education-and-safety/educational-materials/fast-facts/how-your-information-is-shared-ffdmv-17/ [https://perma.cc/9Y3A-7GQC] (explaining that information obtained by the DMV, such as residence address, photographs, and vehicle information, is available to law enforcement authorized by statute in California).

339. It would also allow law enforcement to use DMV information and images as they currently do—mostly to have a clear image of a suspect's face. *See, e.g.*, *id.*

Thus, a person is not sacrificing the privacy of their faceprint when obtaining identification.

C. Balancing Privacy with Law Enforcement Interests

The proposed legislation strikes a balance between privacy concerns and law enforcement's legitimate interests in deploying FRT. Failing to check law enforcement's use of FRT allows law enforcement agencies to invade citizens' privacy in ways never before possible. Congress must consider these privacy invasion concerns when evaluating law enforcement's use of technology. Law enforcement should remain on the cutting edge of technology; criminals exploit technology to circumvent police tactics, and lawmakers must allow law enforcement agencies to keep up. On the other hand, private citizens should not suffer the consequences of having their privacy breached. As technology continues to evolve and law enforcement's capabilities extend in unprecedented ways, Congress must take a careful look at how these new advancements impact the rights of Americans. Sacrificing fundamental rights under the guise of protecting citizens from criminal actors should be a compromise that lawmakers are unwilling to make.

VII. CONCLUSION

FRT is an ever-improving technology that has vast implications for the everyday lives of Americans. This Comment focused on the use of FRT in the law enforcement context, advocating for limiting how law enforcement obtains images compiled into facial databases. However, there remains a wide array of privacy issues concerning the application of FRT in other ways. This Comment tackled the low hanging fruit of the arguments against FRT's widespread implementation—the constitutional problems under the Fourth Amendment.

As noted, the judiciary is ill-equipped to address the problem of FRT's use as a search tool by law enforcement. Under existing Fourth Amendment jurisprudence, courts are likely to uphold law enforcement's use of FRT as constitutional. However, FRT still challenges American privacy in ways we should be unwilling to concede without greater consideration. The courts do not possess the requisite arsenal to address issues of FRT and other cutting-edge technologies because they fall outside traditional understandings of the rights afforded under the Constitution.

Finally, the current statutory framework that governs FRT's use is sparse. Congress has left the matter of technology-enhanced policing in the hands of the police; this open authorization would allow FRT's unimpeded application by law enforcement agencies. This "fox guarding the henhouse"

approach is ripe for abuse. Thus, lawmakers must impose limits on FRT: Congress should address the challenge of FRT directly and restrict the databases of "known faces" to photos obtained via criminal investigative and enforcement measures. Moreover, Congress should codify the FBI's internal policies that are the only limitation on how the agency uses FRT. By making this policy binding law, Congress would limit the potential for abuses that are an inherent feature of self-policing guidelines.

How developing technology will impact everyday policing remains in the realm of conjecture. Nonetheless, lawmakers must consider several interests when permitting or restricting law enforcement's use of new technologies. First, lawmakers must allow technology-enhanced policing on some level. Second, they must consider the impact such technologies have on accepted rights of American citizens. In the context of FRT, allowing law enforcement to more easily identify suspects has vast crime prevention benefits. However, FRT's use by law enforcement could also infringe upon the privacy rights of all Americans. The legislative solution proposed herein balances these concerns. Most critically, the time for action confronting the use of FRT by law enforcement—and similar issues of technology enhanced policing—is now.

Congress should consider how technology changes police practices before they become ingrained as normal police procedures. Congress must evaluate how improved technology used by police impacts the privacy rights of all Americans. The wait and see approach—the default for judicial review of an issue—is simply unacceptable in the context of police practices that invade privacy. If Congress fails to act on FRT, police will scan and identify millions of Americans with the technology, granting government agents unprecedented access to the privacies of those citizens' lives. Continued inaction brings us ever closer to an Orwellian surveillance state. The young person walking down that suburban sidewalk should be able to hold their head high and smile at the passing police cruiser without fear of harassment by an overly invasive face scan.[340]

340. Unless there is a warrant authorizing police to find and detain them. In that case, FRT is coming for them.