Richmond Journal of Law & Technology Volume XXVII, Issue 2

A FACIAL CHALLENGE: FACIAL RECOGNITION TECHNOLOGY AND THE *CARPENTER* DOCTRINE

Ari B. Rubin*

Cite as: Ari B. Rubin, *A Facial Challenge: Facial Recognition Technology and the* Carpenter *Doctrine*, 27 RICH. J.L. & TECH., no. 2, 2021.

* Ari B. Rubin is clerk to Chief Judge Matthew J. Fader of the Maryland Court of Special Appeals. The author received his juris doctor from Georgetown University Law Center in 2020. Prior to law, he was a film and TV writer and producer, and he has written opinion pieces for publications like *Politico*, *The Huffington Post*, and *The New York Daily News*. The author would like to thank Professor James W. Zirkle for providing rich exposure to national intelligence issues.

I. INTRODUCTION

[1] In the 1943 Alfred Hitchcock film, *Shadow of a Doubt*, a handsome, young Uncle Charlie visits his sister's family, including a teenage niece, in the suburbs.[1] Soon after Uncle Charlie's arrival, the niece notices an unusual quirk: more than camera shy, Uncle Charlie refuses to be caught on film at all. Uncle Charlie steps out of frame whenever a photographer appears, and when a stranger tries to snap his photo on the sidewalk, Charlie grabs the camera and exposes the film. *Spoiler alert*: Uncle Charlie is a criminal on the run. Not long ago, with a little effort, it was possible to go one's entire life without leaving a photographic trace.

[2] Imagine Uncle Charlie's plight today. The government would have photographed him when he got his driver's license, his passport, and every time he crossed through customs. His gym would have photographed him when he joined; and so too his bank, graduate school, and supermarket co-op. There would be photos of him in his high school yearbook; in the digital archives of countless resorts, theme parks, and tourist attractions where he posed for portraits-for-purchase; and of course, in the photos he posted online, from social media clippings, to family albums, and the photos that other people took of him. Combine that with live video captured of him daily—city surveillance cameras, cameras in commercially owned buildings,[2] and cameras in his and his friends' homes on so-called smart devices[3]—and Uncle Charlie's image today, even if Uncle Charlie tried to remain anonymous in today's society, his image would be uncontainable.

---

[1] *See* SHADOW OF A DOUBT (Universal Pictures 1943); *see also Shadow of a Doubt*, TCM, https://www.tcm.com/tcmdb/title/341154/shadow-of-a-doubt#synopsis [https://perma.cc/BKX6-XN3L] (providing a brief synopsis of the film).

[2] *See, e.g.*, Hannah Devlin, *'We Are Hurtling Towards a Surveillance State': The Rise of Facial Recognition Technology*, GUARDIAN (Oct. 5, 2019), https://www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurtling-towards-surveillance-state [https://perma.cc/YYN7-MKB8].

[3] *See* Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 936–37, 937 n.25 (2016) (discussing "internet connected cameras" placed in common devices).

[3] The omnipresence of imagery today would be only half of the challenge for Uncle Charlie. Society has now taken the first steps towards making that wealth of data instantly and continuously searchable. Contemporary Facial Recognition Technology ("FRT") can tap the limitless digital photobook and do at least three things: (1) instantly identify an unknown person by comparing his image against a database; (2) associate other government, commercially held, and public data about him, assembling a digital biography; and (3) enable real- or near-real-time tracking whenever he steps into public.[4] The Sherlockian investigative process that once consumed a film's entire plot would now conclude before the curtain opened.

[4] It would be foolish to look at this technological shift with only dread. FRT will undoubtedly change lives, and in some ways, for the better—from producing economic gains and more useful consumer tools, to providing advancements in criminal justice and national security. This article addresses the harms that FRT will cause; specifically, in courts. The question posed, however, is whether governments, with FRT in their toolbelts, should be limited in its use, and if so, by what constraints. Importantly, the Supreme Court in 2018 provided the beginning of an answer in *Carpenter v. United States*.[5] Following the *Carpenter* holding, this article argues that courts must restrict use of FRT in criminal prosecutions by applying a minimal Fourth Amendment warrant requirement. Even with that limitation, law enforcement and national

[4] *See* Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/GTB8-XKVU] (describing technology startup Clearview, offering near real-time FRT capabilities using publicly available data); *see also* Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://nyti.ms/2Nkhh6K [https://perma.cc/E43Q-U68R] (providing examples of facial-recognition image sources for law enforcement).

[5] *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018) (addressing the use of comparable, real-time cellular tracking technology).

security professionals will find ample room for its deployment, but one better balanced with society's needs.

[5] Part I of this article focuses on FRT itself: how it works, and the costs and benefits that might result in the criminal-justice system. In weighing those interests, it finds that FRT produces concerns far greater than those concerning other invasive investigative tools and concludes that unmitigated use of FRT in criminal trials will violate defendants' constitutional and normative rights.

[6] Part II then looks at the constitutional and statutory limits other scholars have proposed as checks on FRT and finds them all wanting. Part III proposes an alternative solution. It looks to the *Carpenter* holding and shows how the Court's reasoning would likely encompass FRT under its umbrella of privacy-related Fourth Amendment concerns. Establishing a warrant requirement based on probable cause for certain FRT uses under the *Carpenter* doctrine would level the playing field for defendants and investigators, while still allowing key warrantless exceptions when they are most critical to community safety.

II. FRT IN CRIMINAL INVESTIGATIONS AND NATIONAL SECURITY

A. FRT's Abilities and Limitations

[7] In the simplest sense, FRT acts as an automated police lineup. An FRT user might include criminal investigators, private companies, or even fellow community members.[6] This Paper will focus on the criminal

[6] *See* Ryan Mac et al., *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, BUZZFEED (Feb. 27, 2020, 11:37 PM), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement [https://perma.cc/4MY2-MY9J] (discussing long list of users signed up for one commercial FRT provider's services, including the FBI, sports leagues, and local schools); *see also* Jeffrey Dastin, *Rite Aid Deployed Facial Recognition Systems in Hundreds of U.S. Stores*, REUTERS (July 28, 2020, 11:00 AM), https://www.reuters.com/investigates/special-report/usa-riteaid-software [https://perma.cc/DTK2-8QAJ] (discussing how the drugstore chain Rite Aid used FRT

investigator or national security analyst. A criminal investigator or FRT analyst begins the process with an input, called a "probe photo."[7] The probe photo might come from anywhere: a police booking shot, the person's social media presence, or a blurry freeze-frame from a video surveillance camera.[8] The technology then automatically compares a computer analysis of the photo against analyses of a database of other photos—FBI mug shots,[9] government photo libraries (such as drivers' records), or commercial photo libraries (sometimes lifted from public websites)[10]—and returns possible matches.[11] In the criminal-justice context, authorities can then use other investigative tools and corroborative evidence to narrow the list of possible suspects to confirm a single, most-probable match with corroborative evidence.[12]

to match "customers entering a store to those of people Rite Aid previously observed engaging in potential criminal activity").

[7] Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Court*, CHAMPION, at 14 (July 2019), https://www.nacdl.org/getattachment/548c697c-fd8e-4b8d-b4c3-2540336fad94/challenging-facial-recognition-software-in-criminal-court_july-2019.pdf [https://perma.cc/C7KZ-R7FE] (defining a probe photo).

[8] *See* Valentino-DeVries, *supra* note 4 (providing examples of probe-photo sources for law enforcement).

[9] *See Facebook Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GOA Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains*: *Hearing on GAO-19-579T Before the H. Comm. on Oversight & Reform*, 116th Cong. 2 n. 5 (2019) [hereinafter Goodwin Testimony] (statement by Gretta L. Goodwin, Director of Homeland Security and Justice).

[10] *See id.* at 3–4, n.7.

[11] *See Face Facts: Dispelling Common Myths Associated with Facial Recognition Technology*, SEC. INDUS. ASS'N 2, https://www.securityindustry.org/wp-content/uploads/2019/06/facial-recognition-20193.pdf [https://perma.cc/J4M3-MDXX].

[12] *See id.* at 5 ("A final determination of whether a match exists is made visually by trained law enforcement analysts. Further steps to verify an individual's identity are part of the police work following this visual determination.").

[8] The process is akin to eyewitness confirmations used by police officers for centuries,[13] now with the aid of computer-driven algorithms. This enables FRT's uncanny speed and volume.[14] The algorithm works by identifying distinctive elements of a person's face, such as the distance between eyes or the size of the chin, and converts it into mathematical data, often called a "face template."[15] The accuracy of these algorithms depends on how many individual points the software can discern on the photos, and then on the quality and number of database photos it examines and from which it can learn patterns.[16] Present-day accuracy is high.

[9] In a 2020 study of nearly 200 FRT systems worldwide, the National Institute of Standards and Technology ("NIST") found that the best FRT systems had false positive rates of only .01–.03%, while the worst performers had a false negative rate of no more than 1%.[17] Comparing this level of accuracy to that of eyewitness identification, a study of criminal

[13] *See* John Edgar Hoover, *The Role of Identification in Law Enforcement: An Historical Adventure*, 46 ST. JOHN'S L. REV. 613–16 (1972) (describing investigative techniques, such as fingerprinting and collecting witness testimony, used before the advent of contemporary forensics).

[14] *See Algorithms that Mimic the Brain's Processing Networks Preferred for Some Functions of Face Detection and Recognition Technology*, NAT'L INST. JUST. (Mar. 5, 2020), https://nij.ojp.gov/topics/articles/algorithms-mimic-brains-processing-networks-preferred-some-functions-face-detection [https://perma.cc/T6VR-G94Y] (comparing relative speed and efficiency of new algorithms with older techniques and technologies).

[15] *Facial Recognition, Street-Level Surveillance*, EFF (Oct. 24, 2017), https://www.eff.org/pages/face-recognition [https://perma.cc/E4JG-VUD5].

[16] *See* Andrew Jason Shepley, *Deep Learning for Face Recognition: A Critical Analysis*, ARXIVLABS §§ IV, VI (Jul. 12, 2019, 10:55 PM), https://arxiv.org/pdf/1907.12739.pdf [https://perma.cc/V5M7-XUFJ].

[17] Michael McLaughlin & Daniel Castro, *The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist nor Sexist*, INFO. TECH. & INNOVATION FOUND. (Jan. 27, 2020), https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms [https://perma.cc/S785-35QE].

convictions overturned following discovery of new DNA evidence showed that 73–80% of them had relied on at least one eyewitness. In each of those cases, a wrongful imprisonment was thus based, at least in part, on an erroneous identification (or false-positive).[18] Accuracy continues to improve as FRT firms develop new techniques.[19]

[10] Beyond accuracy, FRT offers two additional advantages that would have been unimaginable a generation ago: (1) a universe of searchable photos on the internet; and (2) speed.

[11] Federal and state authorities have a growing pool of mug shots and other official records utilized by searchable databases.[20] A 2019 analysis

[18] *See* Hal Arkowitz & Scott O. Lilienfeld, *Why Science Tells Us Not to Rely on Eyewitness Accounts*, SCI. AM. (Jan. 1, 2010), https://www.scientificamerican.com/article/do-the-eyes-have-it/ [https://perma.cc/K8LL-BZMH]; *Eyewitness Accuracy in Police Lineups*, AM. PSYCH. ASS'N (Apr. 2014), https://www.apa.org/action/resources/research-in-action/eyewitness# [https://perma.cc/7JXJ-WQQG]; *see also* Innocence Staff, *How Eyewitness Misidentification Can Send Innocent People to Prison*, INNOCENCE PROJECT (Apr. 15, 2020), https://www.innocenceproject.org/how-eyewitness-misidentification-can-send-innocent-people-to-prison/ [https://perma.cc/UWL2-MYHH] (finding that 69% of 367 DNA-based exonerations involved eyewitness misidentifications). *But see* Kaitlin Jackson & Samuel Gross, *Tainted Identifications*, NAT'L REGISTRY OF EXONERATIONS (Sept. 22, 2016), http://www.law.umich.edu/special/exoneration/Pages/taintedids.aspx [https://perma.cc/QXK5-WT5H] (noting how another organization tracked wrongful convictions and concluded of the 1,886 cases in its database from 1989 to 2016, 30% involved misidentifications).

[19] *See* Olivia Shen, *Getting the Balance Right with Facial Recognition*, *Commentary*, CTR. FOR STRATEGIC & INT'L STUD. (Jan. 8, 2020), https://www.csis.org/analysis/getting-balance-right-facial-recognition [https://perma.cc/Z9TJ-5BBE] ("The National Institute of Standards and Technology (NIST), which has tested facial recognition algorithms from a majority of the industry, estimates that algorithms have improved 20 times over between 2014 and 2018. Error rates have dropped by 95 percent….").

[20] *See The Use of Facial Recognition Technology by Government Entities and the Need for Oversight of Government Use of This Technology Upon Civilians: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 4 (2019) [hereinafter Greco Statement] (statement of Kimberly J. Del Greco, Criminal Justice Information Services Division, Federal Bureau of Investigation) ("The FACE Services Unit performs facial recognition

reported that the FBI photobank held 641 million images.[21] A 2016 study concluded that at least twenty-six and as many as thirty states allow authorities to access driver's license and state ID photos.[22]

[12] In addition to government-managed databases, private companies have compiled their own sets of photos, both to develop proprietary technologies and consolidate a database from which authorities may search for suspects.[23] For instance, in 2016 technology firm Microsoft published what was then the largest publicly available dataset in the world, containing over ten million images of nearly 100,000 individuals.[24] Of greater concern than its size was the sourcing: all of the photos were scraped from sites on

searches of FBI databases (e.g., FBI's NGI-IPS), other federal databases (e.g., Department of State's Visa Photo File, Department of Defense's Automated Biometric Identification System, Department of State's Passport Photo File), and State photo repositories (e.g., select State Departments of Motor Vehicles, criminal mugshots, corrections photos, etc.)").

[21] Goodwin Testimony, *supra* note 9, at 5–6, 6 n.8 (noting that "[t]he over 641 million refers to photos, not the total number of [individuals]").

[22] Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. PRIV. & TECH., at 2 (Oct. 2016) [hereinafter *Line-Up*].

[23] *See* Madhumita Murgia, *Who's Using Your Face? The Ugly Truth About Facial Recognition*, FIN. TIMES (Sept. 18, 2019), https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e [https://perma.cc/4SDV-759C] (describing how private databases "are used to train and benchmark algorithms that serve a variety of biometric-related purposes – recognising [sic] faces at passport control, crowd surveillance, automated driving, robotics, even emotion analysis for advertising").

[24] *See* 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/S2CQ-T5DL]; *see also* Madhumita Murgia, *Microsoft Quietly Deletes Largest Public Face Recognition Data Set*, FIN. TIMES (June 6, 2019), https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2 [https://perma.cc/ZVA2-TRNM] (referencing that Microsoft's database, known as MS Celeb, published the data in 2016).

the internet without any person's consent.[25] More controversially, FRT firm Clearview AI has scraped three billion images from online sites like Facebook and YouTube to build a private database.[26] Interest groups have estimated that nearly 50% of all U.S. adults are currently in a law enforcement accessible records.[27]

[13] The second distinct advantage is speed. One popular FRT commercial provider reports that it can provide better than 99% accuracy within seconds.[28] As opposed to eyewitness lineups and manual photograph comparisons, processes that could historically take hours or days, FRT provides a faster and more efficient means of identifying probable suspects.[29] FRT enables an instant match, but it is still not an instant process: the investigator must choose and upload a probe photo into the FRT software for analysis before a match occurs.[30] Notably, when a probe photo

[25] *See* Murgia, *supra* note 23 (adding that journalists later revealed that military researchers and foreign firms used the database to train their own FRT systems and that Microsoft pulled the database from public accessibility in 2019).

[26] Rebecca Heilweil, *The World's Scariest Facial Recognition Company, Explained*, VOX (May 8, 2020, 11:51 AM), https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement [https://perma.cc/GW6L-3DSJ]; *see also* Mutnick v. Clearview AI, Inc., Nos. 20 C 512, 2020 U.S. Dist. LEXIS 109864, at *2 (N.D. Ill. May 19, 2020) (reporting plaintiff's allegation of Clearview AI's collection of "over 3 billion facial images" to build "a searchable database").

[27] *See Line-Up*, *supra* note 22.

[28] *See* Dan Grimm, *The Fastest Facial Algorithm Just Got Faster*, SAFR (July 19, 2019), https://safr.com/general/the-fastest-facial-algorithm-just-got-faster/ [https://perma.cc/DZD4-R4ZE] (reporting that SAFR scored 99.87 percent on "the University of Massachusetts Labeled Faces in the Wild test").

[29] *See, e.g.*, N.Y. STATE MUN. POLICE TRAINING COUNCIL, IDENTIFICATION PROCEDURES: PHOTO ARRAYS AND LINE-UPS MODEL POLICY 2–13 (2015), https://pceinc.org/wp-content/uploads/2015/06/Eyewitness-Identification-Model-Photo-Array-and-Lineup-ID-Procedures.pdf [https://perma.cc/R594-WWW4] (describing labor-intensive, multi-step processes recommended for line ups and photo arrays).

[30] *See Line-Up*, *supra* note 22, at 10–12 (describing the procedure for obtaining and analyzing a probe photo with FRT).

is taken from a video, the investigator typically must identify and capture single frames.[31] The resulting delay is not a shortcoming in the technology; rather, it is a policy of individual agencies or technology providers.[32] Authoritarian regimes like China are known to use constant, real-time FRT tracking of its citizens in certain regions.[33] Even authorities in British and American cities, like Detroit, are testing such tools.[34]

[14] Despite the benefits of using FRT compared to traditional investigative processes, FRT has its shortcomings. Accuracy, while demonstrably higher than eyewitness confirmation, is imperfect. Accuracy percentages drop if probe photos are poor quality.[35] While new FRT

---

[31] *See, e.g.*, Martin Kaste, *Real-Time Facial Recognition is Available, But Will U.S. Police Buy It?*, NPR (May 10, 2018, 2:10 PM), https://www.npr.org/2018/05/10/609422158/real-time-facial-recognition-is-available-but-will-u-s-police-buy-it [https://perma.cc/3ZGQ-BSR6] (quoting a Los Angeles police officer who indicated that "the investigator needs to take a still from [the] video" and compare it digitally "to the county's collection of booking photos").

[32] *See id.* (quoting the Los Angeles County Sheriff's Department facial recognition manager, who stated "[w]e don't want to do anything that the public doesn't want us to do….I value personal privacy.").

[33] *See* Zak Doffman, *China Is Using Facial Recognition to Track Ethnic Minorities, Even in Beijing*, FORBES (May 3, 2019, 5:33 PM), https://www.forbes.com/sites/zakdoffman/2019/05/03/china-new-data-breach-exposes-facial-recognition-and-ethnicity-tracking-in-beijing/#297516834a75 [https://perma.cc/99PE-V3J7] (describing FRT use in China).

[34] *See, e.g.*, Adam Satariano, *Real-Time Surveillance Will Test the British Tolerance for Cameras*, N.Y. TIMES (updated Sept. 17, 2019), https://www.nytimes.com/2019/09/15/technology/britain-surveillance-privacy.html [https://perma.cc/6WT5-E2M3] (describing FRT use in Britain); Gregory Barber & Tom Simonite, *Some US Cities Are Moving into Real-Time Facial Surveillance*, WIRED (May 17, 2019, 7:00 AM), https://www.wired.com/story/some-us-cities-moving-real-time-facial-surveillance/ [https://perma.cc/RXJ8-DDH9] (denoting FRT use in Detroit and Chicago).

[35] *See* William Crumpler, *How Accurate are Facial Recognition Systems—and Why Does It Matter?*, CSIS: TECHNOLOGY POLICY BLOG (Apr. 14, 2020), https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-–-and-why-

software is increasingly capable of dealing with issues like non-frontal images, poor lighting, distance, and blur, these factors can still lead to unreliable results that require additional human corroboration.[36] FRT designers and users have pursued solutions to overcome this issue, including policies requiring better probe photos, rather than relying on technological fixes alone.[37]

[15] A second, highly controversial problem is lower accuracy rates for racial minorities and women. A recent NIST study showed that across all of the FRT services it tested, minorities were subject to false positives rates of ten to beyond 100 times greater than non-minorities, and false negatives rates of up to 3 times greater.[38] An M.I.T. study revealed that some tools had up to nearly a 35% error rate for images of darker-skinned women, in part because the designers used databases overwhelmingly white, male imagery to train their AI systems.[39]

[16] Accuracy errors are more concerning when paired with statistics showing greater likelihood of minorities' exposure to FRT use in the first place, in part because of more prevalent surveillance in poorer and more

does-it-matter [https://perma.cc/5HW2-THWZ] (describing how image quality affects accuracy).

[36] *See* PATRICK GROTHER ET AL., NAT'L INST. SCI. & TECH., ONGOING FACE RECOGNITION VENDOR TEST (FRVT) PART 2: IDENTIFICATION 5, 34 (2018).

[37] *See id.* at 5.

[38] *See The Facial Recognition Technology (Part II): Ensuring Transparency in Government Use: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 6 (2020) (statement of Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology).

[39] *See* Steve Lohr, *Facial Recognition 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/49TF-ZCYF].

diverse metropolitan areas.[40] The Detroit police department's own statistics for the first-half of 2020 found that of the seventy times its officers had used FRT in their investigations, on all but two occasions, the suspects were Black.[41] Even though the differences between white male and minority accuracy is lessening as the technology improves accuracy is higher than eyewitness identification, the disproportionate results means a greater likelihood of false criminal exposure for vulnerable communities.[42]

B. Balancing the Equities

[17] Considering its capabilities, FRT could be a force for good, and users are already experiencing its utility. Smartphones with FRT biometric unlocking features became popular with the release of the iPhone X in 2017.[43] Social media sites like Facebook commonly use on FRT to enable

[40] *See* Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L. J. 527, 553 (2017) ("[S]urveillance technologies are frequently targeted at disfavored or marginalized populations . . . .").

[41] *See* DETROIT POLICE DEP'T, WEEKLY REPORT ON FACIAL RECOGNITION (2020), https://detroitmi.gov/sites/detroitmi.localhost/files/202006/DPD%20Report%20on%20Facial%20Recognition%20Usage%20%20061520%20-%20062120.pdf [https://perma.cc/YP75-GGFD] (week of June 22, 2020) (showing that the suspect's race in the two remaining occurrences was classified "unknown").

[42] *See* Shen, *supra* note 19; Kami Chavis Simmons, *Future of the Fourth Amendment: the Problem with Privacy, Poverty, and Policing*, 14 U. MD. L. J. RACE, RELIGION, GENDER & CLASS 240, 240 (2014) ("The manner in which urban, inner-city communities are over-policed and the aggressive law enforcement strategies employed in these areas, along with the current constitutional regime that has allowed these practices to flourish, are primarily responsible for the privacy inequities."). *See generally* Bianca A. White, *The Invisible Victims of the School-to-Prison Pipeline: Understanding Black Girls, School Push-Out, and the Impact of the Every Student Succeeds Act*, 24 WM. & MARY J. WOMEN & L. 641, 646–48 (2018) (describing over-policing in minority-dominant schools, which arguably perpetuates the cycle of deprivation and criminal enforcement for vulnerable communities).

[43] *See* JV Chamary, *How Face ID Works on iPhone X*, FORBES (Sept. 16, 2017, 5:00 AM), https://www.forbes.com/sites/jvchamary/2017/09/16/how-face-id-works-apple-iphone-x/#1882f3cd624d [https://perma.cc/2A3U-JK34].

automatic photo tagging.[44] Advertisers now use FRT to target ads to specific customers as they pass digital billboards.[45]

[18] Greater benefits will emerge in health (identifying potential medical concerns with face scans),[46] search and rescue (finding missing persons in crowds),[47] and sex-trafficking prosecutions (identifying victims online).[48] Additionally, FRT can provide considerable community safety benefits, starting with improved law enforcement.[49] It is worth noting here that this involves the simultaneous process of determining who an unknown

[44] Emily Birnbaum, *Facebook Ends Facial Recognition Photo Tagging Suggestions*, THE HILL (Sept. 3, 2019, 3:23 PM), https://thehill.com/policy/technology/459771-facebook-ends-facial-recognition-photo-tagging-suggestions [https://perma.cc/7J6X-AV9Z].

[45] *See* Eden Gillespie, *Are You Being Scanned? How Facial Recognition Technology Follows You, Even as You Shop*, THE GUARDIAN (Feb. 23, 2019, 9:11 PM), https://www.theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop [https://perma.cc/36RP-HGLK].

[46] *See* Laura Cox, *5 Applications of Facial Recognition Technology*, DISRUPTION HUB (Jul. 13, 2017), https://disruptionhub.com/5-applications-facial-recognition-technology [https://perma.cc/DJ95-59UD].

[47] *See Facial Recognition Technology: (Part I) Its Impact on our Civil Rights and Liberties, Hearing Before the H.R. Comm. on Oversight & Reform*, 116th Cong. 7 (2019) [hereinafter Ferguson Statement] (statement of Andrew Guthrie Ferguson, Professor of Law, David A. Clarke School of Law, University of the D.C.).

[48] *See, e.g.*, Tom Simonite, *How Facial Recognition is Fighting Child Sex Trafficking*, WIRED (June 19, 2019, 7:00 AM), https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking [https://perma.cc/UR73-648U].

[49] *See, e.g.*, William J. Bratton, *Face Recognition is Not the Enemy*, N.Y. DAILY NEWS (Jan. 26, 2020, 5:00 AM), https://www.nydailynews.com/opinion/ny-oped-face-recognition-is-not-the-enemy-20200126-pjz4z367bvgfhaws465je5o52m-story.html [https://perma.cc/B9XU-ZE28] (arguing the merits of FRT use in policing); Khari Johnson, *AI Weekly: Facial Recognition Policy Makers Debate Temporary Moratorium vs. Permanent Ban*, VENTUREBEAT (May 17, 2019, 2:01 PM), https://venturebeat.com/2019/05/17/ai-weekly-facial-recognition-policy-makers-debate-temporary-moratorium-vs-permanent-ban [https://perma.cc/Z26R-279A] (discussing the debate between FRT's critics and defenders).

perpetrator is based on a visual image, and just as importantly, determining who that perpetrator is not; in other words, screening out wrongly accused defendants.[50]

[19] In national security, the benefits from real-time monitoring could be game-changing. Already, the Department of Homeland Security (DHS) has begun FRT scanning persons entering U.S. borders.[51] The ability to stop bad actors from broaching U.S. soil can be lifesaving.[52] Likewise, authorities can make significant security gains by employing real-time FRT surveillance to scan everyone entering a high security event, like the Super Bowl, or less contained environments, like street festivals.[53] From one perspective, FRT offers broad improvements over traditional identification techniques in each of these contexts.

[20] Equal costs, most notably privacy concerns, weigh against FRT use. Real-time tracking entails the possibility that interested parties—whether government, corporate, or malicious individuals (imagine an FRT-armed

[50] *See* INT'L JUSTICE INFO. SYS. & INT'L ASSOC. OF CHIEFS OF POLICE, LAW ENFORCEMENT FACIAL RECOGNITION USE CASE CATALOG 14 (2019).

[51] *See* Jon Porter, *U.S. Facial Recognition Will Cover 97 Percent of Departing Airline Passengers Within Four Years*, THE VERGE (Apr. 18, 2019, 5:52 AM), https://www.theverge.com/2019/4/18/18484581/us-airport-facial-recognition-departing-flights-biometric-exit [https://perma.cc/547A-9WUQ].

[52] *See* CHARLES B. DEWITT, AN UNCERTAIN SHIELD: THE NATION'S BORDERS IN THE 1990S 26, 72–80 (1990) (describing "how current measures [c. 1990] fail to stop terrorists at the borders of the United States" and offering solutions).

[53] *See* Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y. TIMES (Mar. 13, 2018), https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html [https://perma.cc/B3G3-SGK2]; Angelica Mari, *Brazilian Police Introduce Live Facial Recognition for Carnival*, ZD NET (Feb. 25, 2020, 7:37 PM), https://www.zdnet.com/article/brazilian-police-introduces-live-facial-recognition-for-carnival/ [https://perma.cc/EAN9-HHYR].

jealous husband)—can put names to nearly every person in public.[54] Unlike traditional police photo arrays that include only persons arrested and booked,[55] FRT databases include perfectly law-abiding populations that neither know about their inclusion nor have any ability to opt-out.[56] By linking publicly available information, such as social media, voting history, financial records, and even shopping records, those names could be immediately associated with detailed biographical descriptions, including home addresses.[57] Advertisers already build these sort of profiles for clients.[58] Corporations can use profiles for marketing purposes, parents can

[54] *See* Woodrow Hartzog & Evan Selinger, *Why You Can No Longer Get Lost in the Crowd*, N.Y. TIMES (Apr. 17, 2019), https://www.nytimes.com/2019/04/17/opinion/data-privacy.html [https://perma.cc/R75G-RS7Z].

[55] *See, e.g.*, NEW ORLEANS POLICE DEPARTMENT OPERATIONS MANUAL, Ch. 42.8.1 at 3 (2017), https://www.nola.gov/getattachment/NOPD/Policies/Chapter-42-8-1-Eyewitness-Identification-Photographic-Line-Ups-EFFECTIVE-3-12-17-(3).pdf [https://perma.cc/XQ2F-29RH].

[56] *See Facial Recognition Technology: Part 1 Its Impact on Our Civil Rights and Liberties: Hearing Before the Comm. on Oversight & Reform*, 116th Cong. 4 (2019) [hereinafter Garvie Statement] (statement of Clare Garvie, Senior Associate, Center on Privacy & Technology at Georgetown Law).

[57] David S. Ardia, *Privacy and Court Records: Online Access and the Loss of Practical Obscurity*, 2017 U. ILL. L. REV. 1385, 1395–96 (2017) (discussing, for instance, how in addition to sensitive material already available on websites like home addresses and voting histories, internet-accessible court files can be interlinked with other online resources to expose private information like financial and medical records).

[58] *See* Heather Kelly, *You've Got Snail Mail: Targeted Online Ads Are Now Literally Following You Home*, WASH. POST (Jan. 30, 2020, 7:00 AM), https://www.washingtonpost.com/technology/2020/01/30/junk-mail-targets-ads [https://perma.cc/H2LU-3HME]; Jennifer Valentino-Devries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/27EG-GCE4] (noting that some firms combine online information with even more invasive tracking technologies hidden on cellphone apps).

use them to learn about their children's friends, and local authorities can use them to disrupt unwanted activities.[59]

[21] During mass protests, like the 2015 and 2020 Black Lives Matters marches, police used body cameras and surveillance networks to identify protestors, raising concerns of a First Amendment chilling effect.[60] FRT proliferation could make such applications commonplace. Beyond speech and associational rights, legal scholars have warned of a particularly adverse effect on undocumented persons and asylum applicants who, in

[59] Heesun Wee, *What You May Not Know About the Boom in Digital User Data*, CNBC.com (updated Sept. 13, 2013, 4:33 PM), https://www.cnbc.com/2012/03/27/what-you-may-not-know-about-the-boom-in-digital-user-data.html [https://perma.cc/9SDE-V2K5] (noting advertisers that compile user profiles from publicly available information); Mike Masnick, *Instead of Parents Spying on Their Kids Online, Why Not Teach Them How to Be Good Digital Citizens*, TechDirt (July 23, 2019, 9:32 AM), https://www.techdirt.com/articles/20190714/18181742586/instead-parents-spying-their-kids-online-why-not-teach-them-how-to-be-good-digital-citizens.shtml [https://perma.cc/DU6P-QW8M] (discussing parents tracking their children's whereabouts and activities online); Heather Kelly, *Police Embrace Social Media as Crime-Fighting Tool*, CNN (updated Aug. 30, 2012, 5:23 PM), https://www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html [https://perma.cc/J7CH-YXXU] (discussing police identifying suspects using data scraped from social media accounts).

[60] *See* Dean DeChiaro, *Democrats Seek Answers on High-Tech Surveillance of Protesters by U.S. Agencies*, ROLL CALL (June 9, 2020, 6:02 PM), https://www.rollcall.com/2020/06/09/democrats-seek-answers-on-high-tech-surveillance-of-protesters-by-u-s-agencies [https://perma.cc/V2E6-EZG9] (detailing congressional investigation into alleged use of surveillance in 2020 political protests and related First Amendment concerns); *cf.* George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, THE INTERCEPT (July 24, 2015, 2:50 PM), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson [https://perma.cc/GB34-J7GM] (discussing the 2015 report about the Department of Homeland Security using social media and cellphone location services to monitor and track Black Lives Matter protesters); Darwin Bond-Graham, *Counter-Terrorism Officials Helped Track Black Lives Matter Protestors*, E. BAY EXPRESS (Apr. 15, 2015), http://www.eastbayexpress.com/oakland/counter-terrorism-officials-helped-track-black-lives-matter-protesters/Content?oid=4247605 [https://perma.cc/YJZ3-9UJK] (discussing how Californian law enforcement and counter-terrorism forces cooperated in using social media to monitor Black Lives Matter protesters).

losing their anonymity, might fear otherwise available legal, medical, and essential services.[61]

[22] Criminal prosecutions introduce a second category of potential harms resulting from FRT, based on pervasive use of FRT by police. A 2016 study conservatively estimated that at least one quarter of the 18,000 law enforcement agencies across the country have access to FRT.[62] FRT use introduces equity concerns, specifically due capacity for disproportionate error rates when used to identify minorities and females.[63] FRT users are responsible for avoiding matching errors by relying on high quality photos, but in practice, many police agencies fail to do so.[64] Proper police FRT use goes beyond merely making a match, but additional investigating to confirm the best match.[65] As already discussed, FRT does not return a single confirmation, but a user-determined number of likely targets, ranging from two to dozens.[66] If authorities fail to follow-up on FRT matches—which

[61] *See* Ferguson Statement, *supra* note 47, at 4.

[62] Garvie Statement, *supra* note 56, at 19.

[63] *See supra* text accompanying notes 38–42.

[64] *See* Garvie Statement, *supra* note 56, at 13–15 ("The New York Police Department (NYPD) has used 'celebrity comparisons' to find suspects whose photographs are too poor quality to return face recognition results…[t]he NYPD also uses Photoshop and other photo editing tools to edit or add in new features into suspect photographs…[a]t least six police departments across the country permit or encourage the use of face recognition on forensic sketches….").

[65] *See* Greco Statement, *supra* note 20, at 3–4 (explaining of the FBI's FRT lab, "[t]his service does not provide positive identification, but rather, an investigative lead and analysis results that are returned to the FBI agent in the form of a 'most likely candidate.' The FBI agent must perform additional investigation to determine if the results provided by the FACE Services Unit is the same person as the probe photo.").

[66] *See supra* text accompanying note 11.

may be inevitable due to crushing caseloads in many local agencies[67]—the exactitude that FRT offers will always suffer in practice, and worse, promote an overreliance on photo confirmation in the first place.[68] In one notorious case, the pairing of a bad source photo and sloppy police procedures (asking a witness to confirm the suspect's identity with reference only to the faulty source photo), Detroit Police wrongfully booked a man whom even the arresting officers admitted looked nothing like the culprit.[69]

[23] Additionally, FRT use in the criminal context will almost always produce admissible fruits evidence.[70] Prosecutors and investigators, in lieu of using an FRT identification directly in trial, instead use FRT to find a suspect who the prosecutors then identify in court with other circumstantial evidence, transforming the suspect's identification into admissible fruits of the FRT match.[71] This is true even though authorities might never have

[67] *See generally* K. Babe Howell, *Prosecutorial Discretion and the Duty to Seek Justice in an Overburdened Criminal Justice System*, 27 GEO. J. LEGAL ETHICS 285, 290–96 (2014) (describing enormous burden on police and justice systems).

[68] *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CENTER ON PRIV. AND TECH. (May 16, 2019), https://www.flawedfacedata.com [https://perma.cc/LA9Z-KVGN] [hereinafter *Garbage*].

[69] *See* Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/NSW7-AV3U]; Timothy B. Lee, *Detroit Police Chief Cops to 96-Percent Facial Recognition Error Rate*, ARS TECHNICA (June 30, 2020, 12:12 PM), https://arstechnica.com/tech-policy/2020/06/detroit-police-chief-admits-facial-recognition-is-wrong-96-of-the-time [https://perma.cc/P5ED-3ZRG].

[70] *See* Segura v. United States, 468 U.S. 796, 815 (1984) ("The Court has never held that evidence is 'fruit of the poisonous tree' simply because 'it would not have come to light but for the illegal actions of the police'…[s]uppression is not justified unless 'the challenged evidence is in some sense the product of illegal governmental activity.'").

[71] *See* Jackson, *supra* note 7, at 17.

looked at the defendant if not for using FRT.[72] Not only are defendants unable to attack the identification when only seemingly admissible evidence appears at trial, in many instances, defendants are unaware that the officer used FRT in the first place.[73]

[24] How should this cost-benefit balance be reconciled? The poet, Homer, told the iconic story of Scylla and Charybdis, the sea monster and whirlpool that were so near to each other that no sailor could pass.[74] The heroic Odysseus found his way through by sailing nearer Scylla, the one that would exact the least harms.[75] The inevitable and beneficial uses of FRT in law, commerce, and other fields demand similar precision and settling for the fewest costs, rather than turning away from the maelstrom entirely.

[25] The first step in the analysis is to divide and label FRT's potential uses in the security and justice fields. Consider the three most common applications:

1. Using FRT to identify a suspect incident to arrest, once he or she is in custody.

---

[72] *See* United States v. Crews, 445 U.S. 463, 474 (1980) (stating even the initial "illegality of" detention "cannot deprive the Government of the opportunity to prove [the defendant's] guilt through the introduction of evidence wholly untainted by the police misconduct.").

[73] *See Garbage*, *supra* note 68; *see also* Sarah St. Vincent, *What if Police Use 'Rekognition' Without Telling Defendants?*, JUST SEC. (June 5, 2018), https://www.justsecurity.org/57275/police-rekognition-telling-defendants [https://perma.cc/2VF6-MYWT] (documenting public defenders in jurisdictions across the country who have reported prosecutors' failure to disclose prior facial recognition searches, including the identities of other possible matches, and noting the potential violation of *Brady* requirements as a result).

[74] *See generally* HOMER, THE ODYSSEY, Book XII (Samuel Butler trans., 1900) (recounting the story of Scylla and Charybdis).

[75] *Id.* at lines 101–10.

2. Using FRT to determine an unknown person's identity, based on a photo of him or her at a crime scene.
3. Using FRT in real-time mass surveillance to find suspects in public.[76]

[26] These three categories move from least to most concern over issues of privacy invasion (including catching non-suspect bystanders in the search) and risk of finding the wrong suspect. At the same time, they move in decreasing degree of probable cause. In other words, identifying a person upon booking, after first using non-FRT to determine him a suspect, provokes fewer privacy and Fourth Amendment concerns than police relying on FRT to choose whom to arrest, or using it across a city to deter bad actors from committing crimes.

[27] The best way then to maximize community safety while minimizing violations of citizens' constitutional and normative rights will be to focus on those instances when the potential harm that FRT might incur upon the targeted person is greatest. That occurs when a person faces a criminal trial because of an FRT identification and little other basis. The search, arrest, and evidence against him are all potential civil rights violations if authorities used FRT improperly. Whereas society might benefit from advertisers using FRT to provide more useful products and the intelligence community finding known terrorists, society only suffers when criminal defendants are not afforded their full rights under the law.

III. WHAT MIGHT BE DONE

[28] This section addresses the following question: what might be done to assure that suspects retain adequate, balanced protections when government agencies use FRT for investigations or criminal trials. It analyzes four possible, but ultimately ineffective mechanisms to block some or all FRT evidence. The four possibilities are: (1) under *Daubert*

[76] *See Line-Up*, *supra* note 22, at 12 (adding a fourth category: using FRT to identify a person whom an officer encountered on patrol but has not yet arrested, which falls within the second application).

standards;[77] (2) as a violation of the Confrontation Clause;[78] (3) as self-incrimination under the Fifth Amendment;[79] or (4) by legislation barring its use.[80]

[29] To fully understand the legal context in which this analysis takes place, it helps first to view FRT as an evolutionary step in increasingly capable identification techniques. We should not compare FRT only to eyewitness identification, its closest analog, but to other biometric tools that investigators use, such as fingerprints, handwriting comparisons, blood types, and DNA analysis.[81] Likewise, other forms of surveillance and tracking are relevant: traditional wiretaps, video surveillance, GPS tracking, and cellphone tower data.[82] Each of these tools pits suspects' rights against the interests of justice, each to a different degree of invasiveness and accuracy (based on the technique's abilities and how the investigator employed it).

[30] For example, one of the oldest forensic tools—fingerprints—has a long record of proven science behind it,[83] and its use in the criminal justice

[77] *See generally* Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579 (1993) (analyzing the evidentiary standard for expert scientific testimony).

[78] *See* U.S. CONST. amend. VI.

[79] *See* U.S. CONST. amend. V.

[80] Khari Johnson, *Congress Moves Toward Facial Recognition Regulation*, VENTURE BEAT (Jan. 15, 2020), https://venturebeat.com/2020/01/15/congress-moves-toward-facial-recognition-regulation [https://perma.cc/YHK8-68GC].

[81] *See* Kalyani CH, *Various Biometric Authentication Techniques: A Review*, 8 J. BIOMETRICS & BIOSTATISTICS, 1, 2 (2017).

[82] *See* DEP'T JUST., NAT'L INST. JUST., INVESTIGATIVE USES OF TECHNOLOGY: DEVICES, TOOLS, AND TECHNIQUES 11–14 (2007), https://www.ncjrs.gov/pdffiles1/nij/213030.pdf [https://perma.cc/9ULJ-8DM3].

[83] *See* Paul C. Giannelli, Daubert *Challenges to Fingerprints*, 42 CRIM. L. BULL. 624, 640–41 (2006).

system is commonplace.[84] If investigators have appropriate cause and warrants to acquire prints, lawyers face little difficulty in admitting the results in court.[85] Some techniques raise reliability concerns while the science is still unproven, and some can be far more invasive. DNA was initially suspect for both reasons.[86] Defense attorneys challenged DNA analyses, raising concerns over how investigators gathered samples, and how prosecutors authenticated the evidence at trial.[87] Similarly, new surveillance techniques like GPS tracking (which evolved from less advanced homing beacons requiring more police effort) drew challenges as constituting privacy invasions and overbroad searches.[88]

[31] Courts weighing FRT evidence admission should consider all of this history in setting new standards. They will likely find is that FRT raises more concerns than its forbearers. FRT's ability to instantly link matches to a person's online presence and other biographical data provides more

[84] *See* Andre A. Moenssens, *Admissibility of Fingerprint Evidence and Constitutional Objections to Fingerprinting Raised in Criminal and Civil Cases*, 40 CHI.-KENT L. REV. 85, 123–24 (1963) (discussing fingerprint forensics as readily admissible in court in the early-1960s).

[85] *See* U.S. DEP'T JUSTICE, CRIMINAL RESOURCE MANUAL, § 251 FINGERPRINTING–SEARCH & SEIZURE (2020) (describing permissibility of fingerprinting under Fourth Amendment).

[86] *See generally* Janet C. Hoeffel, *The Dark Side of DNA Profiling: Unreliable Scientific Evidence Meets the Criminal Defendant*, 42 STAN. L. REV. 465 (1990) (taking a dim view on DNA evidence as lacking standards and portending Orwellian police tracking in the early 1990s).

[87] *See* Margann Bennett, *Admissibility Issues of Forensic DNA Evidence*, 44 U. KAN. L. REV. 141, 152–57 (1995).

[88] *See* Bethany L. Dickman, *Untying Knotts: The Application of Mosaic Theory to GPS Surveillance in* United States v. Maryland, 60 AM. U. L. REV. 731, 738–41 (2011) (describing the use of traditional tracking device surveillance and comparing it to GPS tracking).

information than even blood-based techniques like DNA.[89] This is true even though certain DNA techniques can avail investigators of private medical and genealogical history.[90] The information FRT can return, in contrast, extends as far as the data was ever published online.[91]

[32] Moreover, FRT includes in real-time tracking capabilities, which DNA testing lacks.[92] FRT stands apart from other tracking techniques, like cellphone monitoring, because the latter does not return actual identity. While a defendant might argue that someone else had his cellphone at the time of an accident or crime, a defendant challenging FRT cannot claim that someone else had his face. FRT also differs from earlier techniques because of the size of FRT's search database and the inclusion of persons who have

[89] *See* Teneille R. Brown, *Double Helix, Double Standards: Private Matters and Public People*, 11 HEALTH CARE L. & POL'Y 295, 313–14 (2008) (stating that because DNA provides such intimate details on an individual's genetic makeup, and that genetic information is generally expected to be private, FRT's ability to provide more information than DNA is concerning).

[90] *See* Emily M. Strak, *Genetic Standing: The Constitutionality of Familial DNA Searching on Genealogical Research Databases*, 1 CTS. & JUST. L.J. 44, 47–49 (2019) (distinguishing single-tandem repeat ("STR") DNA typing, used for forensic identification matching and which provides little genetic information, from single nucleotide polymorphisms ("SNP") typing, which does contain important medical data); *see also* Maryland v. King, 569 U.S. 435, 464 (2013) (stating that law enforcement's usage of individuals' DNA for identification purposes is not unconstitutional).

[91] *See* Dave Gershgorn, T*his Simple Facial Recognition Search Engine Can Track You down Across the Internet*, MEDIUM (June 9, 2020), https://onezero.medium.com/this-simple-facial-recognition-search-engine-can-track-you-down-across-the-internet-518c7129e454 [https://perma.cc/8UK5-WNQ2] (describing FRT services' abilities to search widely across the internet by using a person's facial recognition match).

[92] *See* Devlin, *supra* note 2 (describing current and prospective ability of FRT alone and/or in combination with technologies to enable real-time tracking); *see also* Catalin Cimpanu, *Chinese Company Leaves Muslim-Tracking Facial Recognition Database Exposed Online*, ZDNET (Feb. 14, 2019), https://www.zdnet.com/article/chinese-company-leaves-muslim-tracking-facial-recognition-database-exposed-online [https://perma.cc/2L3R-RJDG] (describing China's use of live-tracking with FRT to monitor members of Uighur ethnic group).

never run afoul of the law.[93] These unique characteristics mean that even though evidentiary challenges have failed against prior police tools, they might succeed here.

A. Daubert Challenge

[33] Attorneys may challenge FRT admissibility in court for a variety of reasons. The first might be by attacking its reliability as scientific testimony. In1923, lawyers in U.S. courts challenged expert testimony by turning to the *Frye* standard, which held that such evidence was admissible only when the principles and methodologies used were "sufficiently established to have gained general acceptance" by the scientific community.[94] However, the *Frye* standard proved overburdensome as new sciences emerged that were entirely reliable but failed to gain recognition in courts because of their slow uptake by practitioners.[95]

[34] The Supreme Court embraced a new and still current approach with *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, in which the Court identified a list of factors that trial judges could apply to assess both relevance and reliability.[96] The Court asked: (1) whether the technique or theory has been tested; (2) whether it has been subjected to peer review; (3)

---

[93] *See, e.g.*, Kate O'Flaherty, *Clearview AI's Database Has Amassed 3 Billion Photos. This Is How if You Want Yours Deleted, You Have to Opt Out*, FORBES (Jan. 26, 2020), https://www.forbes.com/sites/kateoflahertyuk/2020/01/26/clearview-ais-database-has-amassed-3-billion-photos-this-is-how-if-you-want-yours-deleted-you-have-to-opt-out/#6cd5919c60aa [https://perma.cc/WS3W-Z53E] (describing how Clearview database is scraped from publicly available social media and that objecting individuals must affirmatively opt out).

[94] Frye v. United States, 293 F. 1013, 1014 (D.C. Cir. 1923).

[95] *See* Richard A. Wise et al., *A Tripartite Solution to Eyewitness Error*, 97J. CRIM. L & CRIMINOLOGY 807, 820 (2007) (stating that the rigid Frye standard which rendered emerging sciences unreliable was eventually replaced by the federal courts and some state courts).

[96] *See* Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 587, 595 (1993).

if its error rate was known; (4) if standards for its operation existed and were maintained; and (5) whether it was generally accepted in the scientific community.[97] *Daubert* placed the burden of proof on the proponent of the evidence.[98] In 2000, drafters and the Court amended the Federal Rules of Evidence to incorporate *Daubert* factors as Rule 702.[99]

[35] Opponents of FRT evidence will face two insurmountable obstacles in a reliability challenge: the use of fruits evidence and FRT's accuracy.

[36] First, prosecutors are not likely to admit FRT matches themselves as evidence. Because the investigator must find the proper match within the multiple matches returned by corroboration, a competent prosecutor will avoid a reliability challenge by simply establishing identity in court based on that extrinsic proof.[100] Ideally, the match will lead to other witnesses who can testify as to the defendant's identity. If admission is possible without referring to the FRT technique—meaning the FRT match is in no way exculpatory—the defense attorney might not even know that FRT was used: Under the dictates of *Brady*, the prosecutor might well be entitled to never inform the defendant of FRT's role.[101]

[97] *See id.* at 592–94.

[98] *See* Judge Harvey Brown, *Procedural Issues Under Daubert*, 36 HOUS. L. REV. 1133, 1134–38 (1999).

[99] *See* FED. R. EVID. 702 (amended 2014); *see also* John Nawara, *Machine Learning: Face Recognition Technology Evidence in Criminal Trials*, 49 U. LOUISVILLE L. REV. 601, 606–07 (2011).

[100] *See* Jackson, *supra* note 7, at 20.

[101] *See* Lynch v. State, 260 So. 3d 1166, 1170 (Fla. Dist. Ct. App. 2018) (citing Brady v. Maryland, 373 U.S. 83 (1963)) (denying a defendant's challenge on *Brady* grounds to prosecutors' failure to disclose having used FRT); *see also* Aaron Mak, *Facing Facts*, Slate: Future Tense (Jan. 25, 2019), https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html [https://perma.cc/Z93L-HQQQ].

[37] The second, and greater obstacle, is that FRT *will* likely succeed on reliability grounds. Admittedly, the technology is still novel.[102] *–Daubert's* suggested factors might be tough—but only initially. NIST performs regular analyses of FRT's capabilities, as do many independent groups, and each shows improving accuracy trends, with false positives and negatives far below comparable techniques.[103] In other words, the first four of *Daubert's* original assessments are likely already met. Admittedly, general acceptance in the scientific community, under either *Daubert* or *Frye* might be less of a given.[104] However, unless significant accuracy concerns emerge, the barrier will fall with time, if it has not already. A defense attorney could also challenge *Daubert's* other prong: relevancy. Especially if the prosecutor chose to present the FRT analysis along with corroborating evidence, the FRT might no longer "assist the trier of fact."[105] But it is a rare judge who will find the pure certitude of FRT unhelpful (non-relevant) to an identification.[106] Additionally, FRT has one final quality favoring its

[102] *See generally Game-Changing Tech or Dystopian Nightmare? How 16 Industries Could Be Transformed by Facial Recognition*, CB INSIGHTS (Apr. 10, 2019), https://www.cbinsights.com/research/facial-recognition-disrupting-industries [https://perma.cc/Y392-D43L] (describing future trends in FRT).

[103] *See* Chad Boutin, *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NAT'L INST. OF STANDARDS & TECH. (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software [https://perma.cc/Q93R-2AKJ]*; see also* Sophie Bushwick, *How NIST Tested Facial Recognition Algorithms for Racial Bias*, SCI. AM. (Dec. 27, 2019), https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/ [https://perma.cc/C7L9-YJQU] (discussing NIST's ongoing Face Recognition Vendor Test program).

[104] *See* Xanthé Mallett & Martin P. Evison, *Forensic Facial Comparison: Issues of Admissibility in the Development of Novel Analytical Technique*, 58 J. FORENSIC SCI. 859, 863 (July 2013) (concluding that the scientific community, as of 2013, was not at consensus about how to assess facial comparison accuracy).

[105] Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 591 (1993).

[106] *See* John Nawara, *Machine Learning: Face Recognition Technology Evidence in Criminal Trials*, 49 U. LOUISVILLE L. REV. 601, 609–10 (2011).

survival against a *Daubert* challenge: whomever FRT identifies will look like the sought-after suspect, even if the match is incorrect.[107] A technique based on two individuals looking alike is going to return a look-alike, and a judge would likely find it difficult to deny what she can see with her own eyes.

B. Confrontation Clause

[38] FRT can also be challenged as a violation of the Sixth Amendment's Confrontation Clause, although such a challenge would not likely succeed. Confrontation Clause challenges have succeeded with other comparable technologies, particularly DNA,[108] but applying the challenge to FRT is less apt than it appears.

[39] The Confrontation Clause grants criminal defendants the right to face their accusers.[109] When prosecutors seek to use hearsay evidence in a criminal trial, the defendant can challenge admissibility when they've had no opportunity to cross-examine the declarant.[110] Historically, such challenges succeeded unless the proponent could show that the hearsay statement had adequate "indicia of reliability."[111] The Supreme Court abrogated this rule in *Crawford v. Washington*,[112] in which it held that the

[107] Jackson, *supra* note 7, at 20 ("[E]yewitnesses are likely to confirm the selections made by FR[T] because suspects selected by FR[T] will *always* look like the true perpetrator.").

[108] *See, e.g.*, People v. John, 27 N.Y.3d 294, 297 (2016); State v. Norton, 443 Md. 517, 553 (2015).

[109] U.S. CONST. amend. VI.

[110] Crawford v. Washington, 541 U.S. 36, 68 (2004) ("Where testimonial evidence is at issue, however, the Sixth Amendment demands what the common law required: unavailability and a prior opportunity for cross-examination.").

[111] *See* Ohio v. Roberts, 448 U.S. 56, 66 (1980).

[112] *See* Crawford v. Washington, 541 U.S. 36, 68–69 (2004).

only means to admit hearsay evidence absent an opportunity to cross-examine the declarant, was if that statement was not intended to be testimonial in nature.[113]

[40] In *Williams v. Illinois*, the Court applied this standard to evidence produced in a laboratory: a DNA analysis of a police rape kit sample.[114] A commercial laboratory returned a DNA profile in a report that the police then used to find the defendant via a police DNA database.[115] The Court held that the report itself, which a lab technician referenced in the trial but that the prosecution never submitted into evidence, did not violate the Clause.[116] A plurality offered two justifications. First, the Court held that the report was not actually hearsay because it was not introduced to prove the defendant's innocence or guilt; instead, the witness mentioned it to establish how the police ultimately identified the suspect.[117] Second, the report was non-testimonial because the lab technician's primary purpose in creating it was to identify an at-large rapist, not to contribute to a trial.[118] The Court later held that only when a lab report is "created solely for an 'evidentiary made in aid of a police investigation," does it "ranks as testimonial."[119]

---

[113] *See id.* at 53–54; *see also* Whorton v. Bockting, 549 U.S. 406, 420 (2007) (ruling that the Clause does not apply to nontestimonial out-of-court statements); Ohio v. Clark, 576 U.S. 237 (2015) (stating that "the question is whether, in light of all the circumstances, viewed objectively, the 'primary purpose' of the conversation was to 'creat[e] an out-of-court substitute for trial testimony," meaning only if the declarant primarily intended to provide testimony that could be used against the defendant would the statement be at odds with the Confrontation Clause.).

[114] *See* Williams v. Illinois, 567 U.S. 50, 56–57 (2012).

[115] *See id.* at 59.

[116] *See id.* at 86.

[117] *See id.* at 76–77.

[118] *Id.* at 84–85.

[119] Bullcoming v. New Mexico, 564 U.S. 647, 664 (2011) (citations omitted).

[41] Based on these factors, FRT evidence will ultimately—if it does not already—pose no Confrontation Clause concern. First, as in *Williams*, prosecutors are unlikely to present an FRT match as direct evidence.[120] Also, in instances where an investigator sends a probe photo to an outside vendor rather than using the FRT software herself, the person performing the FRT match will not be choosing the guilty person, but instead, seeking to return a list of candidates. It will then be the police who investigate further and identify the ultimate suspect.[121] It is equally possible, if the FRT provider is not a police laboratory but an outside firm, that the analyst would have "no way of knowing whether it [would] turn out to be incriminating or exonerating—or both,"[122] or even for what purpose he was analyzing the image.

[42] Second, looking to the near future, it is even more likely that such evidence will not be considered hearsay at all. As is well understood regarding computer-assisted evidence, like a radar gun return or some lab reports, "[o]nly a person may be a declarant and make a statement. Accordingly, 'nothing "said" by a machine . . . is [hearsay].'"[123] For machine-made data to constitute hearsay, a human must play some intervening and interpretive role.[124] A standard example of non-hearsay

[120] *See Williams*, 567 U.S. at 62 (describing how a DNA expert testified as to her conclusions from comparing the defendant's DNA analysis with the analysis of a specimen found at the crime scene, which a non-testifying technician had performed; "[t]he [specimen's] report itself was neither admitted into evidence nor shown to the factfinder").

[121] *See* GROTHER ET AL., *supra* note 36, at 4 (explaining the FRT systems searches "submitted photographs against the reference database and produce[s] candidate matches" based on a user-determined level of similarity).

[122] *Williams*, 567 U.S. at 85.

[123] United States v. Washington, 498 F.3d 225, 231 (4th Cir. 2007) (quoting 4 Christopher B. Mueller & Laird C. Kirkpatrick, Federal Evidence § 380 (2d ed. 1994)).

[124] *See, e.g.*, United States v. Washington, 498 F.3d 225, 231 (citing § 8:13 *Machine and Animal Statements*, 4 MUELLER & KIRKPATRICK, FEDERAL EVIDENCE (4th ed.).

evidence is a computer-generated report of a database search.[125] In its current application, FRT might involve some human intervention.[126] This is expressly true when a user manipulates a probe photo before submitting it for analysis; for instance, changing the lighting or the coloration in order to make it more readable. But importantly, such manipulation is considered improper,[127] and as FRT advances and turns increasingly automated, opportunities for manipulation will diminish greatly.[128] It is thus only those systems that allow for human manipulation that present even the possibility of a Confrontation Clause challenge, and accordingly, police are less likely to use such systems moving forward.[129]

C. Fifth Amendment Privilege

[43] The Fifth Amendment protection against self-incrimination—that no one "shall be compelled in any criminal case to be a witness against himself"—appears at first to restrict the very heart of what FRT implies: the

[125] *See* Susan E.E.B. Sherman, *"I Object… It's Hearsay": Hearsay and Evidence in the Computer Emergency Response Team (CERT)*, SANS (Oct. 20, 2004), https://www.sans.org/reading-room/whitepapers/legal/hearsay-evidence-computer-emergency-response-team-cert-1541 [https://perma.cc/A6W4-W3V7] ("Computer-generated records contain the output of computer instructions without manual intervention. This fails the hearsay definition…because in computer-generated records, a 'person' is not making an assertion…. On the other hand, computer-stored information can be based on human generated contents…. If the person that entered the information does not testify…the computer-stored information is considered hearsay.").

[126] *See* Greco Statement, *supra* note 20.

[127] *See* Garvie Statement, *supra* note 56, at 14.

[128] *See, e.g.*, *Facial Recognition*, AWARE, https://www.aware.com/facial-recognition/ [https://perma.cc/Q46H-ACPA] (discussing the prevalence of fully automated FRT).

[129] *Cf.* Joseph Clarke Celentino, *Face-to-Face with Facial Recognition Evidence: Admissibility Under the Post-Crawford Confrontation Clause*, 114 MICH. L. REV. 1317, 1344 (2016) (agreeing with the same principle but arguing that more opportunity for human intervention will remain).

technology can use a person's face to give up an entire biography.[130] However, a Fifth Amendment argument will fail completely.

[44] To invoke the privilege against self-incrimination, an individual must show: (1) compulsion; (2) incrimination; and (3) a testimonial or communicative act.[131] The logic of an FRT challenge would be that a person whose face is documented and analyzed has provided communicative information that may be used against him in trial without his consent. The fatal flaw in this approach is that "the privilege is a bar against compelling 'communications' or 'testimony,' but . . . compulsion which makes a suspect or accused the source of '*real or physical evidence*' does not violate it."[132] Therefore, the movant must initially show that an image of his face is more than physical evidence; rather, it somehow communicates inner thoughts.

[45] The distinction between physical evidence and testimonial evidence can turn esoteric. Courts have held that many types of physical evidence which reveals a person's deeply intimate characteristics should still be considered non-communicative. In *Holt v. United States*, the Supreme Court stated that asking a suspect to put on and model a blouse did not violate the Fifth Amendment.[133] In *Schmerber v. California*, the Court reached the same conclusion about police extracting blood from a person to assess his blood alcohol level.[134] The Court in *Schmerber* narrowly defined the self-incrimination protection as requiring "testimony [ ]or evidence relating to some communicative act or writing by the petitioner."[135] Aside from an

[130] U.S. CONST. amend. V.

[131] *See* United States v. Doe (*In re Grand Jury Subpoena Duces Tecum*), 670 F.3d 1335, 1341 (11th Cir. 2012).

[132] Schmerber v. California, 384 U.S. 757, 764 (1966) (italics added).

[133] *See* Holt v. United States, 218 U.S. 245, 252–53 (1910).

[134] *See Schmerber*, 384 U.S. at 761.

[135] *Id.* at 765.

actual diary,[136] only a rare type of physical evidence appears to constitute a communicative act: evidence whose mere existence conveys a secret.[137] An example of this latter category is a business record that, if the declarant admitted existed by turning it over, would in effect admit to his involvement in the criminal act (regardless of what the record contained).[138] Thus, a wide range of expressive and somewhat revealing actions fail to constitute self-incrimination,[139] but physical evidence that reveals a person's otherwise unobtainable, inner-knowledge might still be self-incrimination.

[46] Arguing that the outward appearance of one's face is a person's private knowledge would be far-fetched. After all, for the match to occur, the person must have exposed his face and whereabouts to the government or public at some point, thus his identity is shared knowledge. Moreover, even if the movant were to argue that the facial match links to so much other personal information that the combined data becomes communicative as a

[136] *See* Couch v. United States, 409 U.S. 322, 350 (1973) (Marshall, J., dissenting) ("Diaries and personal letters that record only their author's personal thoughts lie at the heart of our sense of privacy.").

[137] *See* Toler v. United States, 2003 WL 21255039, at *7 (S.D. Ohio Apr. 29, 2003) (internal citation omitted) ("The Fifth Amendment may be implicated where the act of production of personal records confirms the existence or location of such materials and assurances of authenticity not otherwise available to the government.")*; see also* United States v. Doe, 465 U.S. 605, 609, 617 (1984) (holding that "turning over of the subpoenaed documents to the grand jury would admit their existence and authenticity," and therefore "respondent was entitled to assert his Fifth Amendment privilege").

[138] *See* United States v. Hubbell, 530 U.S. 27, 36–37 (2000) (finding that the act of producing the documents might have a compelled testimonial aspect because production would assert that the accused controlled the documents).

[139] *See, e.g.*, Doe v. United States, 487 U.S. 201, 219 (1988) (signing a consent form to release records was not compelled testimony); United States v. Wade, 388 U.S. 218, 222–23 (1967) (compelled speech merely to produce a voice sample did not violate the privilege); Gilbert v. California, 388 U.S. 263, 266–67 (1967) (handwriting sample did not violate the privilege).

whole,[140] the argument would still likely fail because investigators could have found most of that personal information through other means. Thus, the results were a foregone conclusion.[141]

[47] One could imagine a more advanced computer system using artificial intelligence to scan millions of records, assembling FRT-revealed information into conclusions that no investigator could otherwise reach, and that only the defendant would know.[142] But even in this hypothetical, the Fifth Amendment argument would fail on the compulsion prong.

[48] To exercise the privilege, a defendant must show compulsion.143 In *Bram v. United States*, an arrested sailor agreed to speak with a detective about a murder to which he ultimately confessed.144 The sailor subsequently claimed the police had forced his confession.[145] The Court held that merely being placed under arrest is not enough to render a

[140] *See Hubbell*, 530 U.S. at 41–42 (finding that even though the petitioner's statements themselves were not incriminating, the breadth of the requested documents was "tantamount to answering a series of interrogatories" that could lead to incriminating evidence).

[141] *See id.* at 44–45.

[142] *See, e.g.*, Karen Hao, *AI Is Sending People to Jail—and Getting It Wrong*, MIT TECH. REV. (Jan. 21, 2019), https://www.technologyreview.com/2019/01/21/137783/algorithms-criminal-justice-ai [https://perma.cc/X759-UWQF] (describing computer-aided tools purportedly capable of predicting convicts' recidivism rates).

[143] *See* United States v. Washington, 431 U.S. 181, 187 (1977) ("[U]nless the record reveals some compulsion, respondent's incriminating testimony cannot conflict with any constitutional guarantees of the privilege.").

[144] *See* Bram v. United States, 168 U.S. 532, 534–40 (1897).

[145] *See id.* at 539 ("[T]he defendant understood that he was a prisoner, and he obeyed every order and direction that the [detective] gave.").

confession involuntary.[146] *Miranda* aside,[147] for the privilege against self-incrimination to apply in non-custodial situations, authorities must exert through physical or psychological means a certainty in the declarant that he has no choice but to comply.[148]

[49] Therefore, no compulsion is present when police use FRT. The match often occurs with no active involvement by the defendant.[149] Again, the defendant may not even be aware when the FRT match occurs. In other words, to claim compulsion, the movant would have to show that he had no choice but to reveal the information. While generations ago, a person might live their entire life without ever posing for a photographer or putting personal data into a public forum, such exposure is involuntary in today's world. But even based on the Court's most generous Fifth Amendment interpretation, it is hard to imagine a judge today holding that mere situational involuntariness such as this—expectations of living in contemporary society—is the same as forced self-incrimination.[150]

---

[146] *See id.* at 561.

[147] *See* Miranda v. Arizona, 384 U.S. 436, 477 (1966).

[148] *See Washington*, 431 U.S. at 187 (1977) (quoting Michigan v. Tucker, 417 U.S. 433, 440 (1974)) ("[F]ar from being prohibited by the Constitution, admissions of guilt by wrongdoers, if not coerced, are inherently desirable. In addition to guaranteeing the right to remain silent unless immunity is granted, the Fifth Amendment proscribes only self-incrimination obtained by a 'genuine compulsion of testimony.' Absent some officially coerced self-accusation, the Fifth Amendment privilege is not violated by even the most damning admissions.").

[149] *But see Line-Up*, *supra* note 22, at 11 (Identifying an acceptable distinction when a person agrees to have their photo taken for the purpose of facial recognition).

[150] *See generally* Recent Decisions, *Searches and Seizures—Electronic Device—Misplaced Confidence*, 4 U. RICH. L. REV. 134 (1969) (citing *Miranda*, 384 U.S. at 467) ("Despite recent Supreme Court decisions extending effective implementation of the [F]ifth [A]mendment beyond criminal proceedings, the essential element of physical or psychological coercion must still be present to invoke [F]ifth [A]mendment protection. There still must be a setting in which the speaker's 'freedom of action is curtailed,' and, to date, electronic eavesdropping cases have not presented this factual setting.").

D. Legislative Fixes

[50] If rule-based or constitutional challenges prove insufficient, one might imagine legislatures stepping in with new laws. Indeed, some local and national leaders have already taken steps. In 2019, the San Francisco Board of Supervisors enacted a sharp restriction requiring all city departments, including the police, to seek the city's approval before employing tools like FRT and to publicly report all use of older surveillance technologies like license plate readers.[151] Washington State followed in early-2020 with a less demanding law—which Microsoft supported—requiring municipalities to give public notice before FRT is deployed and police departments to use FRT only with a warrant.[152]

[51] When the 2020 Black Lives Matter marches rose to challenge over-policing, many other municipalities joined the early adopters, barring police, schools, or other institutions from using FRT or merely requiring that they publish statistics about how often they do employ the technology.[153] Federal legislation has also emerged with varying approaches to FRT regulation. For instance, one bill that Democratic

[151] *See* Khari Johnson, *San Francisco Supervisors Vote to Ban Facial Recognition Software*, VENTURE BEAT (May 14, 2019), https://venturebeat.com/2019/05/14/san-francisco-first-in-nation-to-ban-facial-recognition-software [https://perma.cc/72RC-D2PR].

[152] *See* Ryan Tracy, *Washington State OKs Facial Recognition Law Seen as National Model*, WALL ST J. (Mar. 31, 2020), https://www.wsj.com/articles/washington-state-oks-facial-recognition-law-seen-as-national-model-11585686897 [https://perma.cc/Q6NS-A4C8].

[153] *See* Caroline Haskins & Ryan Mac, *Boston Just Banned Its Government From Using Facial Recognition Technology*, BUZZFEED NEWS (updated June 24, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/boston-vote-ban-facial-recognition [https://perma.cc/E4ZP-6QBT] (discussing bans by Boston and five other Massachusetts cities); Kyle Wiggers, *New York Bans Use of Facial Recognition in Schools Statewide*, VENTURE BEAT (July 22, 2020), https://venturebeat.com/2020/07/22/new-york-bans-use-of-facial-recognition-in-schools-statewide [https://perma.cc/2VGT-RF4L] (discussing New York State banning FRT use in schools).

senators have sponsored would bar federal officials from acquiring or using FRT or other biometric technologies and require states and local law enforcement agencies to pass similar bans to be eligible for federal funds.[154] But that bill died with the end of the 116th Congress and there is no indication that such legislation will soon pass.[155]

[52] Statutes can go a long way to assure consistent rules and prevent the worst abuses, but these statutes are not a panacea. Their shortcomings relate to limits on legislative power broadly,[156] and the challenges multiply when dealing with a tool that requires frequent use with individual actors making fact-specific assessments.[157]

---

[154] *See* Charlotte Jee, *A New US Bill Would Ban the Police Use of Facial Recognition*, MIT TECH. REV., (June 26, 2020), https://www.technologyreview.com/2020/06/26/1004500/a-new-us-bill-would-ban-the-police-use-of-facial-recognition [https://perma.cc/HQU6-QCZN]*; see also* Khari Johnson, *Congress Moves Toward Facial Recognition Regulation*, VENTURE BEAT (Jan. 15, 2020), https://venturebeat.com/2020/01/15/congress-moves-toward-facial-recognition-regulation [https://perma.cc/YHK8-68GC] ("Legislation in the past year has been proposed to limit use of facial recognition in public housing, establish a national AI strategy, or require businesses to receive opt-in approval from an individual to allow their image to be used to train a facial recognition model.").

[155] *See* Janosch Delcker & Cristiano Lima, *Fight Against Facial Recognition Hits Wall Across the West*, POLITICO (Dec. 30, 2019), https://www.politico.com/news/2019/12/30/facial-recognition-privacy-089881 [https://perma.cc/EKH7-7FJ2].

[156] *See generally* ANDREW NOLAN ET AL., CONG. RSCH. SERV., R45323, FEDERALISM-BASED LIMITATIONS ON CONGRESSIONAL POWER: AN OVERVIEW 2 (2018), https://fas.org/sgp/crs/misc/R45323.pdf [https://perma.cc/Q7XQ-8JGS] (discussing internal and external constitutional limits on federal congressional power).

[157] *See* United States v. Brown, 381 U.S. 437, 446 (1965) (citing Fletcher v. Peck, 10 U.S. 87, 136 (1810) ("It is the peculiar province of the legislature to prescribe general rules for the government of society; the application of those rules to individuals in society would seem to be the duty of other departments.")*; see also id.* at 441–46 (interpreting Founder's intent with the Bill of Attainder clause, describing how legislatures are "not so well suited as politically independent judges and juries to the task of ruling upon . . . specific persons").

[53] Scattered legislation cannot limit private FRT deployment. Local efforts cannot control technology firms outside their jurisdiction, and legislatures can only intervene so far in corporate actions.[158] Once FRT tools become prevalent and available to private users, these tools can bleed into the criminal-justice system.[159] Consider for example the possibility that if officers could easily access publicly available FRT, perhaps simply by loading a suspect's picture into a Google-style search, it might be hard to deter or at least track such efforts. Such use might constitute misconduct in the face of a departmental prohibitions but consider the less nefarious example of a community member delivering his or her own FRT evidence from a home surveillance camera; the latter might be untouched by a ban on police use. This all goes to show that legislatures on their own could potentially struggle to contain pervasive technologies.

[54] Another concern is that relying on legislative fixes can create jurisdictional splits. Imagine two cities with contrasting FRT policies and a suspect who happens to travel between them. An officer in the more restrictive zone might turn to his neighboring department for help. Or more assuredly, inconsistent rules will lead to public confusion. Uncertainty can have a chilling effect on constitutionally justified behaviors; conflicting

[158] *See generally* NICOLE DUPUIS ET AL., NAT'L LEAGUE CITIES, CITY RIGHTS IN AN ERA OF PREEMPTION: A STATE-BY-STATE ANALYSIS 1, 3, 6 (2018), https://www.nlc.org/sites/default/files/ 2017-03/NLCSML%20Preemption%20Report%202017-pages.pdf [https://perma.cc/8CQC-2RTG] (criticizing growing trend of states preempting municipalities' policies, discussing the limits on state power and on cities' authority between jurisdictions); ROBERT MELTZ, CONG. RSCH. SERV., R42635, WHEN CONGRESSIONAL LEGISLATION INTERFERES WITH EXISTING CONTRACTS: LEGAL ISSUES 13 (2012), https://nationalaglawcenter.org/wp-content/uploads/assets/crs/R42635.pdf [https://perma.cc/E4K5-CMYP] (discussing limits on Congress' power to regulate businesses).

[159] *See, e.g.*, Kim Lyons, *ICE Just Signed a Contract with Facial Recognition Company Clearview AI*, THE VERGE (Aug. 14, 2020, 3:19 PM), https://www.theverge.com/2020/8/14/21368930/clearview-ai-ice-contract-privacy-immigration [https://perma.cc/CU9K-R35T].

FRT rules might indirectly deter activities like widespread civil rights marches.[160]

[55] The jurisdictional split would not be an issue if the federal government were to act. That said, national legislative or executive efforts face their own set of challenges. Regulatory or executive branch policies would be subject to the constant unknown of subsequent administrations reversing track. Even where Congress acts and does so decisively, (assuming it could find the appropriate federal authority to regulate local police in the first place), it is questionable how courts will interpret the rules. Courts must view whatever FRT legislation Congress passes considering existing constitutional protections in its own deep body of precedent. This potentially create a conflict between new statutes and court doctrine. One likely trend in the face of an outright, legislative moratorium would be new court-created exceptions to admit FRT evidence in certain instances. This is what occurred in search and seizure and *Miranda* disputes through exceptions to the exclusionary rule.[161] Even more of a challenge—because each use of FRT will occur under vastly different circumstances around the country—is that district courts will struggle to adapt broad and novel laws in their analyses of unusual cases, potentially interpreting them differently than Congress intended.[162]

---

[160] *See* Levinson-Waldman, *supra* note 40, at 597 (discussing Laird v. Tatum, 408 U.S. 1 (1972) ("a seminal 1972 Supreme Court case on the chilling effects of surveillance")).

[161] *See* Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 503–07 (2013) (discussing how exemptions in privacy laws regulating law enforcement conduct have emerged).

[162] *See* Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 MICH. L. REV. 1117, 1121 (2017) (arguing that "[s]tructural differences between the Fourth Amendment and investigative legislation make legislation a poor signal of constitutionally relevant judgments," because legislation misinterprets public sentiment, can be in conflict with constitutional rules, or can violate federalism principles); *see also* Yale Kamisar, *Can (Did) Congress Overrule Miranda?*, 85 CORNELL L. REV. 883, 884–85 (1999) (considering the possibility that Congress could act and the courts might simply ignore the rules, as was the case when in 1968, Congress passed 18 U.S.C. § 3501, which made the "*pre-Miranda* 'due process'—'totality of circumstances'—

[56] A final shortcoming is that legislators might simply get FRT regulation wrong. In an extreme scenario, the legislators might set sweeping prohibitions that prevent FRT deployment in otherwise beneficial situations, undermining community safety or subverting opportunities for valid commercial use (such as home surveillance).[163] When it comes to the narrow concern over courtroom evidence, these broad prohibitions might do more harm than good.

[57] Nevertheless, these challenges should not create the impression that legislatures have no role. Privacy advocates have noted many gaps that only Washington or municipalities can fill.[164] But if the courts have any constitutional basis to limit FRT, it will be in every party's interest to sharpen that approach first.

IV. THE FOURTH AMENDMENT SOLUTION

[58] Having found alternative means for regulating FRT evidence wanting, this final Part identifies a solution. Based on the Supreme Court's 2018 holding in *Carpenter v. United States*, regarding Cell Site Location Information ("CSLI"), FRT will likely be found subject to a Fourth Amendment warrant requirement.[165] First, Part III lays out the relevant

'voluntariness' rule the sole test for the admissibility of confessions in federal prosecutions, thereby purporting to overrule by legislation the Warren Court[].").

[163] Laura Daily, *As Homeowners Find New Uses for Security Cameras, Checking Law Should Be First Step*, WASH. POST (Aug. 27, 2019, 7:00 AM), https://www.washingtonpost.com/lifestyle/home/as-homeowners-find-new-uses-for-security-cameras-checking-law-should-be-first-step/2019/08/26/595152f2-c460-11e9-b72f-b31dfaa77212_story.html [https://perma.cc/G9CD-NVHW] (discussing the law and ethics of personal home surveillance).

[164] *See* Garvie Statement, *supra* note 56, at 23–27 (arguing for mandates on FRT training and reporting and suggesting that Congress should outright ban certain particularly invasive techniques, like FRT use with drones or police bodycams).

[165] *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

Fourth Amendment law. Second, it explains why and how the new *Carpenter* doctrine would encompass FRT.

A. Fourth Amendment Warrant Clause and the *Carpenter* Test

[59] The Fourth Amendment warrant clause protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[166] Courts analyze evidence derived from search or seizures by asking whether the Fourth Amendment protects the type of item at issue, and if so, whether the investigator's conduct was reasonable.[167] As contemporary search and seizure doctrine evolved, two competing views concerning protected use emerged: a property view and a privacy view.[168] The property view leans towards the historic Fourth Amendment approach, with its textual focus on "houses, papers, and effects."[169] Among original public meaning scholars, this remains the Amendment's sole purview.[170] However, in the mid-1960s, beginning with *Katz v. United States*, which dealt with a wiretap in a public phone booth,

[166] U.S. CONST. amend. IV.

[167] *See* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (internal citations omitted) (holding: "(a) that an enclosed telephone booth is an area where, like a home, and unlike a field, a person has a constitutionally protected reasonable expectation of privacy; (b) that electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment; and (c) that the invasion of a constitutionally protected area by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant").

[168] *See id.* at 352–54.

[169] *See Carpenter*, 138 S. Ct. at 2213 (citations omitted) (noting that the amendment had been traditionally "tied to common-law trespass" and judicial analysis focused on whether the government "obtains information by physically intruding on a constitutionally protected area").

[170] *See, e.g.*, United States v. Jones, 565 U.S. 400, 404 (2012) (finding a Fourth Amendment violation when police trespassed on a private vehicle to place a GPS tracker).

the Warren Court promoted a competing Fourth Amendment view primarily concerned with a person's reasonable expectation of privacy.[171]

[60] The evolving test for what constitutes a reasonable expectation of privacy has been highly sensitive to technological development. In the 1980s, the Court held that homing beacons planted by police on suspects' cars or other objects to track them (when up-close surveillance was impractical) did not violate defendants' reasonable privacy expectations because the police could have freely followed and observed the suspects on public roads without getting a warrant.[172] The Court analogized to historical means such as this again in 2001, when *Kyllo v. United States* held that authorities had violated the defendant's privacy expectation by using a thermal imaging device to detect a marijuana lab inside his home, even though authorities might have reached the same result by looking through an open window.[173] Distinguishing thermal imaging from historical mean, Scalia noted the negligible public awareness of such technology and that a person would not expect authorities to rely on it.[174] The *Kyllo* holding affirmed the basic rule that the longer a surveillance technology persisted, the more reasonable its warrantless use.[175]

---

[171] *See Katz*, 389 U.S. at 353 ("We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling.").

[172] *See, e.g.*, United States v. Karo, 468 U.S. 705, 721 (1984); United States v. Knotts, 460 U.S. 276, 285 (1983).

[173] *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).

[174] *See id.* (noting that the privacy expectation is higher where the technology is "not in general public use").

[175] *See* United States v. Moore-Bush, 963 F.3d 29, 42–43 (1st Cir. 2020) (internal quotation omitted) (quoting Kyllo, 533 U.S. at 34) (relying on *Kyllo* for the proposition that there is a higher Fourth Amendment safeguard for "uncommon and then new technology" as compared to "technology that is in general public use," to allow warrantless search by surveillance camera mounted on a public utility pole).

[61] While courts were labeling and limiting the public's reasonable privacy expectations, property-view jurists continued to mark the field for what constitutes personal possessions. First, the Supreme Court decided that a person loses both a privacy and property interest in the things that shares with the public, like her handwriting, voice, or "facial characteristics."[176] Second, a person has neither privacy in nor property of those things that she gives to a third-party, whether the recipient is an individual (absent a confidentiality privilege) or a commercial entity.[177] Under this rule, when a person shares even highly personal information with companies, such as phone records with telecommunication firms or financial activities with banks, the information is no longer his and thus not subject to Fourth Amendment protection.[178]

[62] The image of a person's face used in FRT would likely implicate both property and privacy exceptions. Whenever in public, short of wearing a mask, a person's face is on display, and she cannot later assert ownership of photos authorities capture, nor could she claim the intent to keep her appearance private.[179] Likewise, under third-party doctrine, a person could

[176] *See* United States v. Dionisio, 410 U.S. 1, 14 (1973) ("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.").

[177] *See* United States v. Miller, 425 U.S. 435, 443 (1976) (forming the origin of the rule where the Court held that the doctrine applied "even if the information is revealed on the assumption that it will be used only for a limited purpose…."); *see also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

[178] *See Smith*, 442 U.S. at 743–44 (finding no Fourth Amendment search when police used a pen register because Smith assumed the risk when he conveyed dialed numbers to the third-party phone company)*; see also* Miller, 425 U.S. at 442–43 (finding no Fourth Amendment search when police subpoenaed Miller's banks records, including months of canceled checks).

[179] *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, 413 (2014) ("When a person,

not claim a property or privacy right in a photo that she posted on social media or gave to a private company for public display.[180] Based on these traditional Fourth Amendment limitations, at the outset, it seems courts would exclude Fourth Amendment protection for FRT evidence. But the Supreme Court took a turn in the 2010s, melding the property and privacy doctrines into what could now be considered a new and still evolving exception—one that very likely will encompass FRT.

[63] In *United States v. Jones*, which like the 1980s cases *Karo* and *Knotts*, dealt with homing beacons, authorities tracked a defendant using a GPS device without a warrant.[181] The Court found this to be a Fourth Amendment violation.[182] The plurality ruled narrowly that the physical attachment of the tracker to the suspect's car while it was parked in his driveway was a trespass onto his land, hewing to the traditional Fourth Amendment property analysis.[183] But Justices both Sotomayor and Alito wrote notable concurrences proposing alternative theories, echoing what the dissent in the appellate holding described as a "mosaic" theory.[184] For the

'X' steps outside of their home and walks down a busy public street, it is easy to conclude that they have waived their right to claim a privacy interest in the fact that they are walking down the street in plain view of other pedestrians, police officers, and anyone else in the near vicinity.").

[180] *See* Laurie Buchan Serafino, *"I Know My Rights, so You Go'n Need a Warrant for That": The Fourth Amendment, Riley's Impact, and Warrantless Searches of Third-Party Clouds*, 19 BERKELEY J. CRIM. L. 154, 166 (2014).

[181] *See* United States v. Jones, 565 U.S. 400, 402–03 (2012); United States v. Karo, 468 U.S. 705, 721 (1984); United States v. Knotts, 460 U.S. 276, 285 (1983).

[182] *See Jone*s, 565 U.S. at 404–05.

[183] *See id.*

[184] *See id.* at 415 (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring); *see also* United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) ("[T]his novel aggregation approach to the reasonable expectation of privacy would prohibit not only GPS-augmented surveillance, but any other police surveillance of sufficient length to support consolidation of data into the sort of pattern or *mosaic*." (emphasis added)).

first time, the two justices identified a privacy interest in information that may be unprotected as individual pieces but become more invasive when police aggregate the information as a full picture.[185]

[64] After several similar holdings,[186] the Court in 2018 codified this notion of assembled information with its holding in *Carpenter*. In this case, FBI agents obtained business records without a warrant from a suspect's wireless phone provider including Cell Site Location Information (CSLI)—essentially, geographic triangulation data—from over a four-month period.[187] The CSLI, when compiled, created a near perfect, historical map of the suspect's movements.[188] That information "provide[d] an intimate window into [the suspect's] life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[189] Reviewing whether such information should be subject to a warrant, the Court found that the question

[185] *See* United States v. Jones, 565 U.S. at 415 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political professional religious and sexual associations."); *id.* at 430 (Alito, J., concurring) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

[186] *See* Riley v. California, 573 U.S. 373, 393–97 (2014) (holding that police officers must obtain a warrant to search a cell-phone due to the "immense storage" of sensitive information on a person's cell phone).

[187] *See* Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018) ("Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information.").

[188] *See id.* at 2217 ("Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts.").

[189] *See Jones*, 565 U.S. at 415 (Sotamayor, J. concurring).

implicated both the privacy issues in *Knotts* and *Jones*, and the third-party property issues in *Miller* and *Maryland*.[190] The Court held that the FBI's actions violated the defendant's "reasonable expectation of privacy in the whole of his physical movements."[191] Justice Roberts wrote for the majority that "the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection," made it unique from other information that a person voluntarily surrenders.[192]

[65] The Court described five factors underlying its concern with CSLI: "intimacy, comprehensiveness, expense, retrospectivity, and voluntariness."[193] These same factors appeared to varying degrees in other recent mosaic cases.[194] Providing an effective summary of the *Carpenter* holding and tying it to the Court's mosaic series, criminal-justice law professor Andrew G. Ferguson described five principles of what one could call a *Carpenter* doctrine:

1. **Anti-tracking principle**: a concern over comprehensive, long-term tracking capabilities of new surveillance technologies.
2. **Anti-aggregation principle**: a privacy harm from otherwise public information that new technologies can automatically combine into a mosaic, rendering it much more revealing.

[190] *See Carpenter*, 138 U.S. at 2215.

[191] *Id.* at 2219.

[192] *Id.* at 2223.

[193] *Id.* at 2234 (Kennedy, J., dissenting) (describing majority's holding).

[194] *See, e.g.*, Riley v. California, 573 U.S. 373, 396 (2014) ("Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute); United States v. Jones, 565 U.S. 400, 415–16 (2012) ("The government can store such records and efficiently mine them for information years into the future. . . . And because GPS monitoring is cheap . . . it evades the ordinary checks that constrain abusive law enforcement practices."); United States v. Graham, 796 F.3d 332, 348 (4th Cir. 2015).

3. **Anti-permanence principle**: information that third parties store for a long time and that the government can instantly retrieve at any point.
4. **Anti-arbitrariness principle**: a potential for arbitrary government power in the use of a new technology, without constitutional or statutory check.
5. **Anti-pervasive surveillance principle**: the desire to avoid a permeating state of government surveillance.[195]

[66] This neatly summarized *Carpenter* doctrine in effect shows how the Court has established a Fourth Amendment right in otherwise publicly available information if the tools authorities used would enable them to lie in wait for incriminating behavior. As Justice Roberts describes in one of the mosaic cases described it, such surveillance would be as pervasive as the "'general warrants' . . . of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[196]

[67] Though the *Carpenter* doctrine has not emerged into common use by courts,[197] other scholars have already suggested criminal investigative

[195] Ferguson Statement, *supra* note 47, at 12–14.

[196] *Riley v. California*, 573 U.S. 373, 403 (2014).

[197] *See, e.g.*, *Moore-Bush*, 963 F.3d 29, 42–43 (finding that "[e]ven absent the explicit limiting language in *Carpenter*, *Carpenter's* reasoning does not undermine" the holding that surveillance cameras mounted on public utility poles do not violate the Fourth Amendment); United States v. Wanjiku, 919 F.3d 472, 484 (7th Cir. 2019) (accepting the "general argument that the Supreme Court has recently granted heightened protection to cell phone data," but holding that neither *Carpenter* nor *Riley* "addresses searches at the border where the government's interests are at their zenith, and neither case addresses data stored on other electronic devices such as portable hard drives and laptops"); Commonwealth v. McCarthy, 484 Mass. 493, 513 (2020) (Gants, C.J., concurring) ("If a law enforcement agency possessed comparable historical locational data that could produce a mosaic of an individual's movements equivalent to that produced by CSLI, [such as with] surveillance cameras using facial recognition software, we would require law enforcement to obtain a search warrant based on probable cause").

arenas in which it might apply (such as police searches of commercial DNA databases belonging to popular family tree websites).[198]

B. FRT is Subject to a Fourth Amendment Warrant Requirement

[68] FRT will likely be subject to a warrant requirement under the *Carpenter* doctrine, because the technology implicates all five of the Court's *Carpenter* principles. To apply the *Carpenter* doctrine, remember that FRT evidence is likely to emerge in three separate applications: (1) incident to arrest; (2) to determine an unknown person's identity based on a probe photo; and (3) in real-time mass surveillance to find suspects.[199] One will find that each of these acts raises *Carpenter* concerns to different degrees.

[69] First, the anti-tracking principle. This is the interest a person has in authorities not unjustifiably following her. Justice Sotomayor wrote in *Jones* that "[a]wareness that the Government may be watching chills associational and expressive freedoms."[200] Anti-tracking principle also captures the concern Justice Scalia raised in *Kyllo* of public unfamiliarity with the police's technology.[201] It is contrary to the Fourth Amendment if police can track a citizen without a warrant in ways that she did not know

[198] *See, e.g.*, Antony Barone Kolenc, *"23 and Plea": Limiting Police Use of Genealogy Sites After* Carpenter v. United States, 122 W. VA. L. REV. 53, 55 (2019) (arguing that *Carpenter* creates a warrant requirement in searching the records of companies like Ancestry, 23andMe, and GEDmatch).

[199] Ferguson Statement, *supra* note 47, at 6.

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

[201] Kyllo v. United States, 533 U.S. 27, 40 (2001) (discussing increased Fourth Amendment concerns specifically when "the Government uses a device that is not in general public use").

were physically possible.[202] Of the three FRT applications, anti-tracking concerns are least present when the suspect is already in custody.

[70] No tracking occurs when in custody; the FRT simply puts a name to a face. But in the second application, finding an unknown person's name with a photo, the database match will likely return location information as well, at least the suspect's location when the match photo was taken.[203] If the FRT also returns more recent imagery and multiple returns, police could gain a sense of the suspect's movements. At the extreme end, real-time surveillance would entail not just finding a suspect in one location, but the ability to follow that suspect anywhere she moves. Thus, at least two of these applications strongly implicate the anti-tracking principle.

[71] Second, the anti-aggregation principle. This principle, embodied in mosaic theory, holds that harm to a defendant's rights is greatest when automated tools enable police to easily combine what are otherwise innocent records into a criminalizing *ukase*.[204] FRT possess this quality at its core.[205] It works by combining innocent photos and associated records that prove incriminating in combination with new facts.[206] FRT databases

[202] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (citing Jones, 565 U.S. at 430) (society had an expectation "that law enforcement agents and others would not-and indeed, in the main, simply could not-secretly monitor and catalogue every single movement of an individual's car for a very long period").

[203] Ferguson Statement, *supra* note 47, at 17–18 (discussing concerns with real-time tracking including the ability to identify a suspect's location).

[204] Ferguson Statement, *supra* note 47, at 17–18 (expressing concern over police obtaining an "all-encompassing record of the holder's whereabouts").

[205] John D. Woodward, *And Now, the Good Side of Facial Profiling*, RANDBLOG (Feb. 4, 2001), https://www.rand.org/blog/2001/02/and-now-the-good-side-of-facial-profiling.html (discussing how FRT would enable authorities "to compile a comprehensive profile of an individual's movements and activities).

[206] *See* Alfred Ng, *Facial Recognition Could Take over, One 'Convenience' at a Time*, CNET (Jan. 13, 2020), https://www.cnet.com/news/at-ces-facial-recognition-creeps-into-everything/ [https://perma.cc/YR6R-6Y97].

might reveal not just a suspect's whereabouts but a whole biography that could tie her circumstantially to a crime.[207] If a database photo came from an employment ID or a gun license application, authorities could know where the suspect worked or whether, perhaps, she was armed. Authorities could also look for other known criminals also captured in the suspect's match photos. Together, the searches could produce a virtual rap sheet.[208] Looking at the three FRT applications, they all rely on aggregation. Even with the first case (when dealing a suspect in custody), FRT requires narrowing down a pool of matches, and as a result the corroboration effort will likely involve looking at several photos of the suspect, each feeding more personal information. Real-time surveillance would violate aggregation even more, because it adds new data with each sighting. The only natural limits on how much data any of the occasions provide is the suspect's own digitized history.

[72] Third, the anti-permanence principle. This principle implicates the Court's concerns with retrospectivity.[209] It is the ability to look not only at a recent occasion but to view it through a history of actions—some innocent, some not.[210] As Justice Roberts captured it, "[w]ith access to CSLI, the Government can now travel back in time."[211] Compounding the Court's

[207] *See* Jennifer Valitino-Devries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/Q3D6-PHR6].

[208] *See* Brief of the Center for Democracy & Technology as Amicus Curiae in Support of Appellees at 24–25, United States v. Moore-Bush, 963 F.3d 29 (1st Cir. 2020).

[209] *See* Ferguson Statement, *supra* note 47, at 13–14.

[210] *See* Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 935 (2016) ("Yet when it comes to criminal investigation, time travel seems increasingly possible….[W]e increasingly create a diary…via our smartphones and online technologies.").

[211] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018); *see also* Stephen E. Henderson, *Fourth Amendment Time Machines (And What They Might Say About Police Body Cameras)*, 18 U. PA. J. COSNT. L. 933, 939 (2016) ("This 'time-machine' like

concern was that the police need not even know in advance what period they wanted to search; it could become a fishing expedition.[212] Again, all three FRT applications implicate anti-permanence. It does not matter under what circumstance the police are conducting the search; the concern lies in the historical breadth of the databases. If a suspect's database photo came from Facebook and police search the rest of that user's profile, it might reveal not only the suspect's identity but all the other information that the suspect provides: perhaps images of his illegal drinking back in high school or anecdotes about what he did on his wedding night. Any former high school senior knows, once he posts a photo online, it tends to survive forever.[213]

[73] Fourth, the anti-arbitrariness principle. Here, the Court explained that the greater ease and lower cost for police to access personal data as "compared to traditional investigative tools" weighed in favor of stronger privacy rights, not weaker.[214] Nearly every case in the *Carpenter*-doctrine line built its arguments atop the constitutional framers' concern with arbitrary search and seizures.[215] The Warrant Clause was intended "to

capability to access permanently stored data acknowledged a fear about the creation of overbroad and unlimited data systems which allow for retrospective searching.").

[212] *See Carpenter*, 138 S. Ct. at 2218.

[213] *See* Zoe Schiffer, *How to Erase Your Personal Information from the Internet (It's not Impossible!)*, VOX (Sept. 11, 2019, 3:46 PM), https://www.vox.com/the-highlight/2019/9/11/20859597/internet-privacy-erase-history-google-facebook [https://perma.cc/QFE4-LF6M] (describing difficulty of removing personal data).

[214] *See Carpenter*, 138 S. Ct. at 2217–2218 (Alito, J., concurring) (citing Jones, 546 U.S. at 429) ("Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so 'for any extended period of time was difficult and costly and therefore rarely undertaken.'").

[215] *See, e.g.*, Riley v. California, 573 U.S. 373, 403 (2014) (internal citation omitted) ("Opposition to such searches was in fact one of the driving forces behind the Revolution itself.…[It] was 'the first scene of the first act of opposition to the arbitrary claims of Great Britain.'"); Maryland v. King, 569 U.S. 435, 467 (2013) (Scalia, J., dissenting) (internal citation omitted) ("Patrick Henry warned that the new Federal Constitution would expose the citizenry to searches and seizures 'in the most arbitrary

secure 'the privacies of life' against 'arbitrary power'"; "to place obstacles in the way."[216] In *Carpenter*, arbitrariness concerns emerged most strongly with the third-party doctrine.[217] The Court said that because new technology placed more information in the hands of third parties than ever before, unfettered application of that exception would allow "private letters, digital contents of a cell phone—any personal information reduced to document form, in fact—[to] be collected by subpoena for no reason other than 'official curiosity.'"[218]

[74] As applied to FRT, the potential for arbitrary searches is even greater. Authorities can utilize FRT even without a subpoena. Many of the match photo databases that FRT relies upon are publicly available or accessible on the open market,[219] unlike CSLI, for which cellphone providers control the proprietary data.[220] To conduct an FRT search, the investigator need only choose a probe photo and open his laptop.[221] Like anti-aggregation and anti-permanence, all three FRT applications implicate this concern regarding FRT's extraordinary ease. Though real-time surveillance does so perhaps to the least degree because such systems are

manner'….Madison's draft of what became the Fourth Amendment answered these charges.").

[216] *See Carpenter*, 138 S. Ct. at 2214 (citing Boyd v. United States, 116 U.S. 616, 630 (1886); then citing United States v. Di Re, 332 U.S. 581, 595 (1948)).

[217] *See id.* at 2216.

[218] *Id.* at 2222 (internal citation omitted).

[219] *See* Lyons, *supra* note 159.

[220] *See* Rachel Levinson-Waldman, *Cellphones, Law Enforcement, and the Right to Privacy*, BRENNAN CTR. JUSTICE at 2, 4 (2018), https://www.brennancenter.org/sites/default/files/201908/Report_Cell_Surveillance_Privacy.pdf [https://perma.cc/GE9C-NW8U] (describing how, under *Carpenter*, authorities must rely on court processes to obtain CSLI).

[221] *See* Mac, *supra* note 6.

still less prevalent and more costly to set up (a distinction that will likely ebb with time).[222]

[75] Finally, the anti-pervasive surveillance principle. Justice Sotomayor explained in *Jones* that constant real-time GPS tracking undermined "the Fourth Amendment's goal to . . . prevent a too permeating police surveillance."[223] Anti-pervasiveness concerns are heightened, the Court noted, when engaging in the activity that makes surveillance possible is practically involuntary for the defendant.[224] The intimacy of the information exposed by the constant tracking further flouts the Warrant Clause's purpose.[225] For FRT, the three applications produce varied results. For application incident to arrest, FRT might enable retrospective surveillance, but that monitoring does not continue. Thus, the principle is at its least concerning. The opposite is true for real-time FRT surveillance, which is even more pervasive than CSLI or GPS because a suspect's face is always with her; the privacy sacrifice is flatly involuntary.[226] On top of this concern, real-time surveillance will likely record countless bystanders, any

[222] *See* NANCY G. LA VIGNE ET AL., URBAN INST., EVALUATING THE USE OF PUBLIC SURVEILLANCE CAMERAS FOR CRIME CONTROL AND PREVENTION 19–20 (2011) (describing costs and difficulties cities face in setting up widespread surveillance systems).

[223] United States v. Jones, 565 U.S. 400, 416–17 (2012) (Sotomayor, J. concurring) (omitting internal quotations) (citing United States v. Di Re, 332 U.S. 581, 595 (1947)); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

[224] *See Carpenter*, 138 S. Ct. at 2214 (quoting Riley v. California, 573 U.S. 373, 385(2014)) ("[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society.").

[225] *See id.* at 2217 ("As with GPS information, the time-stamped data provides an intimate window into a person's life."); *see also* Riley, 573 U.S. at 395 ("[M]ore than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.").

[226] *Cf. Carpenter*, 138 S. Ct. at 2218 ("While individuals regularly leave their [GPS-tracked] vehicles, they compulsively carry cell phones with them all the time.").

one of whom might spontaneously engage in what authorities deem criminal behavior. With no probable cause, authorities could practically automate the investigative process for crimes that they would never have even known about before FRT.

[76] Based on this analysis, the outcome for FRT seems inevitable. For the third FRT application, real-time tracking, whenever authorities utilize FRT absent a warrant, a person's Fourth Amendment rights are violated. Real-time tracking implicates all five of the *Carpenter* doctrine's concerns. When authorities use FRT for identification incident to arrest or based on an unknown person's photos, they potentially violate the suspects' rights if that search goes at all beyond identification to reveal linked information like his social media presence, or if the source of the database photo is itself inculpating (by tying the person to relevant facts of the crime).[227] Accordingly, as the Court held in *Carpenter*, the government must at a minimum "obtain a warrant supported by probable cause before acquiring such records."[228] This—the probable cause standard—is the Fourth Amendment floor.

[77] Some scholars argue that the probable cause burden is too low, considering FRT's invasive impact. Professor Ferguson, who identified the five *Carpenter*-doctrine principles, has staked out the position that authorities should face a "probable cause-plus" standard, with the "plus" referring to additional minimization efforts.[229] Other advocates push for

[227] *Compare* United States v. Hubbell, 530 U.S. 29 (2000) (Marshall, J., dissenting) (finding a Fifth Amendment violation because the mere existence of a defendant's records proved his guilt), *with* Couch v. United States, 409 U.S. 322, 350 (1972) ("Diaries and personal letters that record only their author's personal thoughts lie at the heart of our sense of privacy.").

[228] *See Carpenter*, 138 S. Ct. at 2221.

[229] *See* Ferguson Statement, *supra* note 47, at 22 ("Federal legislation should authorize use of face recognition for investigative targeting on a probable cause-plus standard, requiring an assertion of probable cause in a sworn affidavit, plus declarations that care was taken to minimize unintended collection of other face images, and that proper steps have been taken to document and memorialize the collection.").

sharper limits, such as a complete moratorium.[230] Some legislative proposals already before Congress—for instance, a bill from Senators Mike Lee and Chris Coons—adopt the probable cause-plus rule.[231] Considering the balance of equities[232] and the limited effectiveness of legislative fixes,[233] the existence of a Constitutional floor is arguably the more important finding. The precise standard that lawmakers employ beyond this should rightly be sensitive to evolving societal mores.

[78] Critics of overly burdensome warrant requirements will argue that even a probable cause standard is too high. They would say that the *Carpenter* doctrine is too ill-defined and FRT is too early in its spread for courts to impose a strict constitutional limit. Additionally, these critics would argue that doing so will unfairly favor criminal defendants at the public's expense[234] and impede technological development.[235] In response to such concerns, it is essential to recognize the two historic exceptions to the warrant requirement that will likely survive under the *Carpenter*

[230] *See* Garvie Statement, *supra* note 56, at 23.

[231] *See* Facial Recognition Technology Warrant Act of 2019, S. 2878, 116th Cong. § 3(d) (as introduced in Senate, Nov. 14, 2019) ("Minimization Requirement.—Any use of facial recognition technology pursuant to a covered court order shall be conducted in such a way as to minimize the acquisition, retention, and dissemination of information about the individuals other than those for whom there was probable cause to seek the covered court order obtained under subsection (a)(2)(A).").

[232] *See supra*, Section 1.0.

[233] *See supra*, Section II.0.

[234] *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (criticizing the mosaic theory on the ground that there is no clear line delineating when the mosaic becomes sufficiently complete to constitute a search under the Fourth Amendment).

[235] *See* Meredith Whittaker & Daniel Castro, *Should Government Halt the Use of Facial-Recognition Technology?*, WALL ST. J. (Feb. 23, 2020, 10:01 PM), https://www.wsj.com/articles/should-government-halt-the-use-of-facial-recognition-technology-11582513260 [https://perma.cc/XCC6-4NUH].

doctrine and still enable FRT use in scenarios with which critics would be most concerned.

[79] First, the public safety exception is likely to survive under the *Carpenter* doctrine. Courts have recognized a public safety exception under the Fourth Amendment in the so-called special needs category.[236] A court may grant a special needs exception for evidence obtained without a warrant by performing a fact-specific balancing test.[237] The test weighs the importance of the government's interest, the practicality and value of securing a warrant that requires individual suspicion, and the gravity of the privacy invasion that resulted.[238] The government's purpose in the disputed incident must have been something other than "crime detection."[239] Courts have permitted the exception in instances of highway sobriety checkpoints[240] and searches of travelers' bags on subways,[241] among other examples.

[80] The *Carpenter* holding itself provides the clearest guide as to whether courts will permit FRT based on public safety, stating the

[236] *See* Camara v. Municipal, 387 U.S. 523, 538 (1967) (holding that warrants to search for housing code violations in entire areas could be issued on the basis of area-wide standards that do not require a showing of individualized suspicion in a founding case on the special needs exception).

[237] *See* Mann v. San Diego, 907 F.3d 1154, 1164–65 (9th Cir. 2018) (citation omitted) (applying the exception when "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable").

[238] *See* National Treasury Employees Union v. Von Raab, 489 U.S. 656, 665–66 (1989)*; see also* D. H. Kaye, *The Constitutionality of DNA Sampling on Arrest*, 10 CORNELL J. L. & PUB. POL'Y 455, 489–91 (2001).

[239] *See* Chandler v. Miller, 520 U.S. 305, 314 (1997).

[240] *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 447 (1990) (permitting suspicion-less sobriety checkpoint).

[241] *See* MacWade v. Kelly, 460 F.3d 260, 263 (2d Cir. 2006) (upholding searches in New York City subway system for purpose of preventing terrorist attacks).

following: "Our decision today does not call into doubt warrantless access to CSLI in such circumstances. While police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation, *the rule we set forth does not limit their ability to respond to an ongoing emergency*."[242] The question is under what conditions courts might approve such an exception. As the above analysis shows, there is already less Fourth Amendment protection for searches incident to arrest.[243]

[81] Courts will likely make an outright public safety exception for FRT in routine bookings to assure the person is put in adequate detention facilities based on his criminal history or to aid in recapturing him if he escapes.[244] In other words, FRT incident to arrest would rarely require a warrant. At the other end of the spectrum would be real-time FRT surveillance in non-emergencies. For instance, monitoring for dangerous behavior at a protest, which privacy rights activists already equate to the abuses wrought using "general warrant[s]" in the colonial-era.[245] One need

[242] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (emphasis added) (speaking approvingly of public safety exceptions for "warrantless searches related to bomb threats, active shootings, and child abductions").

[243] Cupp v. Murphy, 412 U.S. 291, 295 (1973) ("Chimel [v. California] stands in a long line of cases recognizing an exception to the warrant requirement when a search is incident to a valid arrest. The basis for this exception is that when an arrest is made, it is reasonable for a police officer to expect the arrestee to use any weapons he may have and to attempt to destroy any incriminating evidence then in his possession." (citing 395 U.S. 752 (1969)) (internal citations omitted)).

[244] *See* United States v. Kelly, 55 F.2d 67, 70 (2d Cir. 1932) (discussing a related Fourth Amendment exception known as "true identity," which allows warrantless acquisition of biometric data from a suspect upon arrest and booking, works in exactly this way). Courts will likely require that police use FRT matching incident to arrest for identity purposes alone; the technique must not return any additional biographical data beyond a standard criminal record.

[245] *See* Stanford v. Texas, 379 U.S. 476, 486 (1965) ("[T]he Fourth and Fourteenth Amendments guarantee…that no official of the State shall ransack his home and seize his books and papers under the unbridled authority of a general warrant."); *see also* Joseph, *supra* note 60.

not make so sharp a critique to conclude that the government could only justify a safety exception in such cases by showing that they had an important and specific interest in monitoring for criminal activity, could do so neutrally, and that they lacked alternative reasonable means.[246] As a practical matter, if the FRT warrant requirement were already clearly established law, authorities would likely try to obtain emergency court approval at the outset in a scenario like this, rather than dubiously relying on the public safety exception.

[82] Finally, an attenuation exception is likely to persist under *Carpenter*.[247] Under this court-made rule, the government in some instances may introduce not the warrantless evidence itself, but fruits evidence that police derive from it, if sufficiently attenuated. FRT related fruits evidence typically arises when law enforcement corroborates an FRT match through additional investigation, for instance, by going to a suspect's home, interviewing a person there, and having a witness who confirms a suspect's ties to a crime.[248] Courts may admit that witness' testimony based on weighing: (1) the gap in "temporal proximity" between FRT use and finding the witness; (2) "presence of intervening circumstances"; and (3) attention to "the purpose and flagrancy of the official misconduct."[249] In weighing

[246] *Cf.* Levinson-Waldman, *supra* note 40, at 592–96 (arguing that real-time surveillance would not be permissible without a warrant in terrorism emergencies).

[247] *See* Brent D. Stratton, *The Attenuation Exception to the Exclusionary Rule: A Study in Attenuated Principle and Dissipated Logic*, 75 J. CRIM. L. & CRIMINOLOGY 139, 140–41 (1984) ("The attenuation exception…permits the use of evidence discovered through the government's misconduct if the connection between the misconduct and the discovery of the evidence is sufficiently weak.").

[248] *See* Segura v. United States, 468 U.S. 796, 815 (1984); Jackson, *supra* note 68, at 17. *See also* United States v. Humphries, 636 F.2d 1172, 1178 (9th Cir. 1980) ("[W]hen identification [is] based solely on [the witness's] contact with [the defendant] prior to the unlawful arrest[,] [i]t is not in any way a 'fruit' of that unlawful arrest.").

[249] Utah v. Strieff, 136 S. Ct. 2056, 2062 (2016).

the final factor, courts often look to the impact its ruling will have on dissuading police misconduct.[250]

[83] This exception is less accommodating to warrantless FRT use than the public safety exception. If the first two prongs are met, a court would still struggle to find any acceptable reason for the officer having avoided a warrant.[251] Far from relying on an attenuation exception as a matter of course, officers would have to cite unusual circumstances that brought the FRT match into their hands.[252] In instances where, perhaps, third parties offered FRT evidence to the police, or if an investigator found an old, warrantless match but sought additional evidence based on independent investigation without ever showing newly-questioned witnesses the FRT photo, a court might consider an opening. Again, as a practical matter, authorities are unlikely to seek out this exception. This is often because with a clear warrant requirement it would be rare that investigators could argue having acted in good faith. But it will remain an alternative for outlier cases.

[84] These exceptions show that public safety advocates' worst fears are unlikely to occur. Courts will treat FRT like any other evidence subject to a Fourth Amendment probable cause standard. This application of the *Carpenter* doctrine establishes a balanced warrant requirement, scaled fairly in intensity to the three different applications in which FRT might emerge.

---

[250] *See* Wong Sun v. United States, 371 U.S. 471, 488 (1963).

[251] *See, e.g.*, Utah v. Strieff, 136 S. Ct. 2056, 2063 (2016) (finding that the third factor, examining the purpose and flagrancy of an arresting officer's conduct, tipped the scales conclusively against suppression because the officer's warrantless search was "at most negligent" and a consequence of "good-faith mistakes." The majority refused to interpret the officer's investigatory stop as purposeful misconduct, which would weigh this factor in favor of suppression).

[252] *See, e.g.*, *Wong Sun* at 491 (internal citation omitted) (concluding that although a defendant had been wrongfully interrogated without a warrant initially, because he was released and "had returned voluntarily several days later" to confess, "the connection between the arrest and the statement had become so attenuated as to dissipate the taint").

V. CONCLUSION

[85] FRT can inspire Orwellian visions of constant surveillance, all-knowing states, and powerful corporations. It has the potential, in national security investigations, to upend decades of spy craft to America's detriment. Use by domestic authorities threatens constitutional rights. For these reasons, legislators and rights advocates have expressed concern; they are why the Fourth Amendment warrant requirement exists. But so too must courts recognize FRT's benefits, especially those that pertain to fairer and more accurate trials. Far from opening a new era of uncertain law enforcement capabilities, courts will likely import the *Carpenter* doctrine and employ traditional probable cause safeguards.

[86] This Paper identified FRT's revolutionary capabilities, weighed the costs and benefits, and concluded that criminal defendants needed some protection against its use. It then looked at four possible constitutional and statutory mechanisms to limit FRT evidence's role in court and found that none of them would succeed. Finally, it turned to the Court's recent Fourth Amendment jurisprudence and identified why, under the *Carpenter* doctrine, courts must require that police obtain a warrant based on probable cause before collecting FRT evidence. This is the right outcome considering the equities. Authorities and judges will decide how smoothly the new rules take hold.