AMERICAN CIVIL LIBERTIES UNION

April 8, 2024

OCRE/Public Comments
ATTN: Facial Recognition Technology
U.S. Commission on Civil Rights
1331 Pennsylvania Ave. NW, Suite 1150
Washington, DC 20425
frt@usccr.gov

Submitted via e-mail

RE: Request for Comment on Civil Rights Implications of the Federal Use of Facial Recognition Technology

The American Civil Liberties Union (ACLU) submits this comment to inform the U.S. Commission on Civil Rights' investigation into use of facial recognition technology (FRT) by the U.S. Department of Justice (DOJ), U.S. Department of Homeland Security (DHS), and U.S. Department of Housing and Urban Development (HUD).

As explained in detail below, use of face recognition technology in law enforcement (Part I), immigration enforcement (Part II), and housing (Part III) raises a number of civil rights and civil liberties concerns, including contributing to unjustified arrests and other encounters with police, exacerbating racism in policing outcomes and access to benefits and services, and violating Americans' Fourth Amendment right to privacy.

I. Face Recognition Technology in Law Enforcement Investigations

As the ACLU has previously explained,[1] law enforcement use of face recognition technology poses a number of serious threats to civil liberties and civil rights, making it dangerous both when it fails and when it functions. Accordingly, the ACLU has repeatedly called for a federal moratorium on the use of facial recognition by law and immigration enforcement agencies.[2]

Current uses of FRT to attempt to identify images of unknown suspects have contributed to multiple wrongful arrests, and the impacts of those failures are not distributed equally—nearly every publicly known wrongful arrest due to police reliance on an incorrect FRT result has been

[1] ACLU, Response to Request for Information (RFI) on Public and Private Uses of Biometric Technologies (FR Doc. 2021-21975) 3–4 (Jan. 14, 2022), https://www.aclu.org/sites/default/files/field_document/2022.01.14_aclu_response_to_ostp_biometric_tech_rfi.pdf; ACLU, Response to Request for Comment on Law Enforcement Agencies' Use of Facial Recognition Technology, Other Technologies Using Biometric Information, and Predictive Algorithms (Executive Order 14074, Section 13(e)) (Jan. 19, 2024), https://www.aclu.org/documents/aclu-comment-facial-recognition-and-biometric-technologies-eo-14074-13e.

[2] Press Release, ACLU, ACLU Calls for Moratorium on Law and Immigration Enforcement Use of Facial Recognition (Oct. 24, 2018), https://www.aclu.org/press-releases/aclu-calls-moratorium-law-and-immigration-enforcement-use-facial-recognition.

of a Black person.[3] Contrary to the assurances of law enforcement agencies, human review of FRT results often exacerbates, rather than ameliorates, the deep unreliability of this technology. Among other reasons, that is due to cognitive biases toward trusting computer outputs and because human identifications based on FRT results are tainted by the propensity of the technology to return images of lookalikes who are not actually the suspect. Further, police and prosecutors have regularly withheld material information about their use of FRT from courts and defendants. Additional dangers loom as police departments experiment with, and federal agencies invest in, the capability to use automated face recognition technology on live or recorded video, which threatens to enable mass surveillance on a previously inconceivable scale.

In recognition of these dangers, more than 20 jurisdictions—including Boston; Minneapolis; Pittsburgh; Jackson, Mississippi; San Francisco; King County, Washington; and the State of Vermont—have enacted legislation halting most or all law enforcement or government use of face recognition technology. Others, such as the states of Maine and Montana, have enacted significant restrictions on law enforcement use of the technology. And law enforcement agencies in jurisdictions such as New Jersey and Los Angeles have prohibited use of Clearview AI, an FRT vendor that markets a particularly privacy-destroying system built on a database of tens of billions of non-consensually collected faceprints.

As the ACLU and dozens of other organizations have previously explained,[4] the twin dangers of highly consequential misidentifications and pervasive surveillance mean that government agencies should not be deploying face recognition technology at all. Federal law enforcement agencies should place a moratorium on their own use of face recognition technology, and should prevent state and local governments from using federal funds to purchase or access the technology.

1. Face recognition technology is unreliable and biased, and accuracy tests do not reflect its performance in real-world applications.

a) FRT consistently shows racial and gender biases that persist despite improvements in algorithm training data.

Even under optimal conditions, FRT systems are not designed to provide positive identification. Rather, at most the technology provides an "algorithmic best guess."[5] It will

[3] *See* Nat'l Acad. of Scis., *Facial Recognition: Current Capabilities, Future Prospects, and Governance* 83 (2024), https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-and-governance.

[4] Letter from ACLU et al. to Joseph R. Biden, President, United States of America (Feb. 16, 2021), https://www.aclu.org/sites/default/files/field_document/02.16.2021_coalition_letter_requesting_federal_moratorium_on_facial_recognition.pdf.

[5] Eyal Press, *Does A.I. Lead Police to Ignore Contradictory Evidence?*, The New Yorker (Nov. 13, 2023), https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence/; *see also* Nat'l Acad. of Scis., *Facial Recognition: Current Capabilities, Future Prospects, and Governance* 48–49 (2024), https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-and-governance.

frequently produce possible matches that are incorrect.[6] The accuracy of the technology is affected by several factors, including the performance and training of the algorithm, the makeup of the matching database, and the features of the probe image (including angle, lighting, occlusion, and pixelation).[7] Most disturbingly, the technology continues to have markedly higher false match rates for people of color and women than for white people and men.[8]

Reputable testing shows that face recognition algorithms misidentify Black people, people of color, and women at higher rates. Widely reported National Institute for Standards & Technology (NIST) testing in 2019 found FRT algorithms were up to 100 times more likely to misidentify Asian and African American people than white men, and that women and younger individuals were also subject to disparately high misidentification rates.[9] While some reports indicate that demographic differentials in false match rates have lessened for some algorithms, testing by NIST and academic researchers indicates that the problem persists.[10]

Early coverage of racial and gender disparities in FRT false-match rates focused on the lack of equal representation by race and gender in photo datasets used to train the algorithms.[11] It has become clear that ensuring more diverse representation in training datasets will not eliminate the problem of demographic disparities in false-match rates. While other factors may also be at play, this is partly because the color-contrast settings in digital cameras disproportionately result

[6] Because FRT systems conducting one-to-many searches are generally configured to produce multiple possible matches, even when the algorithm identifies a true match, it will also necessarily generate numerous false matches.

[7] Nat'l Acad. of Scis., *Facial Recognition: Current Capabilities, Future Prospects, and Governance* 47 (2024), https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-and-governance

[8] *Id.* at 24, 56–57.

[9] Patrick Grother et al., U.S. Dep't of Com., Nat'l Inst. for Standards & Tech., *Face Recognition Vendor Test Part 3: Demographic Effects* 2–3, 8 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; *See also* Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, Wash. Post (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

[10] Patrick Grother, U.S. Dep't of Com., Nat'l Inst. for Standards & Tech., *Facial Recognition Vendor Test (FRVT) Part 8: Summarizing Demographic Differentials* 15 (July 2022), https://pages.nist.gov/frvt/reports/demographics/nistir_8429.pdf; *see also* Aman Bhatta et al., *The Gender Gap in Face Recognition Accuracy Is a Hairy Problem*, Procs of the IEEE/CVF Winter Conference on Applications of Computer Vision (2023) https://openaccess.thecvf.com/content/WACV2023W/DVPBA/papers/Bhatta_The_Gender_Gap_in_Face_Recognition_Accuracy_Is_a_Hairy_WACVW_2023_paper.pdf; K.S. Krishnapriya et al., *Issues Related to Face Recognition Accuracy Varying Based on Race and Skin Tone*, 1 IEEE Transactions on Tech. & Soc'y 8 (2020), https://ieeexplore.ieee.org/document/9001031; K.S. Krishnapriya et al., *Characterizing the Variability in Face Recognition Accuracy Relative to Race*, 2019 IEEE/CVF Conf. on Computer Vision and Pattern Recognition Workshops (April 2019), https://arxiv.org/abs/1904.07325.

[11] Patrick Grother et al., U.S. Dep't of Com., Nat'l Inst. for Standards & Tech., *Face Recognition Vendor Test Part 3: Demographic Effects* 71 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

in underexposed images of darker-skinned people,[12] which reduces FRT accuracy when attempting to process and match those images.[13]

The use of FRT compounds pre-existing racial disparities in policing in other ways. Research shows that law enforcement use of face recognition technology "contributes to greater racial disparity in arrests," with an increase in Black arrest rates and decrease in white arrest rates.[14] This may be partly a result of cognitive biases of officers who decide when to run FRT searches and how heavily to rely on FRT results, and on racial disparities in the makeup of photo databases used to attempt to generate matches, including arrest photo (i.e., "mugshot") databases that reflect longstanding overpolicing of people of color. In jurisdictions that are required to track demographic information related to FRT searches, data shows disproportionate use on people of color. In New Orleans, for example, "nearly every use of the technology from last October to this August was on a Black person."[15] In Detroit, all 129 FRT searches in 2020 were conducted on images of Black people.[16] In 2021, 95.6% of FRT searches by Detroit police were conducted on images of Black people.[17]

In light of these dynamics, it is unsurprising that nearly every known case of a wrongful arrest in the U.S. due to police reliance on an incorrect FRT result has involved arrest of a Black person. Concern about FRT exacerbating existing racism in policing has motivated many of the bans on police use of the technology at the state and local level.[18] Federal agencies should implement equivalent bans.

---

[12] *See* Sarah Lewis, *The Racial Bias Built into Photography*, N.Y. Times (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html.

[13] *See* Haiyu Wu et al., *Face Recognition Accuracy Across Demographics: Shining a Light into the Problem*, arXiv No. 2206.01881 (Apr. 16, 2023), https://arxiv.org/abs/2206.01881; Nat'l Acad. of Scis., *Facial Recognition: Current Capabilities, Future Prospects, and Governance* 24, 84–87 & Box 4–2 (2024), https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-and-governance.

[14] Thaddeus L. Johnson et al., *Facial Recognition Systems in Policing and Racial Disparities in Arrests*, 39 Gov't Info. Q. No. 4 (2022).

[15] Alfred Ng, *'Wholly Ineffective and Pretty Obviously Racist': Inside New Orleans' Struggle with Facial-Recognition Policing*, Politico (Oct 31, 2023), https://www.politico.com/news/2023/10/31/new-orleans-police-facial-recognition-00121427.

[16] Detroit Police Dep't, *Annual Report on Facial Recognition, 2020* (Jan. 27, 2021), https://detroitmi.gov/sites/detroitmi.localhost/files/2021-02/Facial%20Recognition%202020%20Annual%20Report.pdf.

[17] Detroit Police Dep't, *Annual Report on Facial Recognition, 2021* (May 13, 2022) (on file with authors).

[18] *See, e.g.*, King County, Wash., Ordinance No. 19296, Statement of Facts ¶¶ 2–3 (2021) ("The council finds that the propensity for surveillance technology, specifically facial recognition technology, to endanger civil rights and liberties substantially outweighs the purported benefits, and that such technology will exacerbate racial injustice. . . . Bias, accuracy issues and stereotypes built into facial recognition technology pose a threat to the residents of King County."); Minneapolis, Minn., Code of Ordinances art II, § 41.10(c) ("Facial recognition technology has been shown to be less accurate in identifying people of color and women. Facial recognition technology has the potential to further harm already disadvantaged communities through incorrect identifications.").

b) Tests of FRT accuracy do not account for real-world conditions.

Proposals to mitigate harms of FRT use in law enforcement sometimes revolve around selecting FRT algorithms with relatively higher accuracy rates and relatively lower demographic disparities in false match rates. Although well-intentioned, these proposals rest on extremely shaky ground because current FRT accuracy tests do not reflect the conditions of real-world FRT use. Additionally, testing data is difficult to interpret, is susceptible to manipulation, and is difficult to compare across algorithms.[19]

As explained in a 2022 report from the Georgetown Center on Privacy and Technology, existing FRT accuracy tests do not control for the many variables characterizing real-world law enforcement uses of FRT.[20] A study designed to assess accuracy rates of FRT algorithms *as actually used in police investigations* would need to account for both algorithmic and human factors in the FRT search process, as well as the tremendous variability in the quality of probe images, which often feature low resolution, poor lighting, and other deficiencies. But existing studies do not do so.

FRT algorithms conducting one-to-many searches are not designed to return a single "match." Instead, an FRT algorithm will return a list of *possible* candidate matches, usually organized in order of the "similarity score" assigned by the algorithm to each candidate match.[21] Statistical measures of how often a true match to the probe image appears somewhere in that candidate list do not reflect the accuracy of the FRT search *process*, because a human analyst must still assess the list of candidate-match images—which may run to several hundred images[22]—and determine whether one of those images appears to be a true match. As demonstrated by the known cases of misidentifications leading to wrongful arrests,[23] that human review process is prone to error.[24]

---

[19] Marissa Gerchick & Matt Cagle, *When it Comes to Facial Recognition Technology, There Is No Such Thing as a Magic Number*, ACLU (Feb. 7, 2024), https://www.aclu.org/news/privacy-technology/when-it-comes-to-facial-recognition-there-is-no-such-thing-as-a-magic-number.

[20] Clare Garvie, *A Forensic Without the Science: Facial Recognition in U.S. Criminal Investigations* at 15–16, Geo. L. Ctr. on Privacy & Tech. (2022), https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/.

[21] Nat'l Acad. of Scis., *Facial Recognition: Current Capabilities, Future Prospects, and Governance* 46 (2024), https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-and-governance.

[22] *See,* Dep. Of Jennifer Coulson at 29, *Williams v. City of Detroit*, No. 21-cv-10827 (E.D. Mich.), ECF No. 60-2 (Michigan State Police analyst explaining that candidate list included 486 images generated by the FRT search).

[23] *See infra* Part I.2.

[24] Clare Garvie, *A Forensic Without the Science: Facial Recognition in U.S. Criminal Investigations* at 22–24, Geo. L. Ctr. On Privacy & Tech., (2022), https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/ ("A wealth of psychology research demonstrates that overall, humans are not innately good at identifying unfamiliar faces."); Nat'l Acad. of Scis., *Facial Recognition: Current Capabilities, Future Prospects, and Governance* 61–63, 83–84 (2024), https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-and-governance.

Human choices introduce additional risk of errors at other points in the FRT search process too. For example, law enforcement personnel may manipulate a low-quality probe image to try to make it more suitable for a FRT search, but that manipulation will often increase the risk of error. Analysts may attempt to brighten the photo, reduce pixelation, interpolate facial features that are obscured, or even combine photographs into a composite image.[25] When photo manipulation introduces data that was not part of the native image, it often increases the risk that the search will generate false matches. Police have even been documented using composite sketches as probe images, even though FRT systems are designed to process photographs of actual faces, not artist renderings of a witness's recollection of a face.[26] Even after this practice was widely discredited,[27] at least one FRT company, Cognitec, continues to encourage police to engage in it.[28]

Humans must also select a similarity threshold for the FRT algorithm. When an FRT system conducts a one-to-many search, it assigns a similarity score to each image in the matching database. FRT algorithms are typically programmed with a cut-off so that they return images as possible matches only if their similarity score exceeds a particular threshold. Choosing a similarity threshold involves tradeoffs: a lower threshold will lower the risk of missing a true match while raising the risk of overwhelming the examiner with false matches; a higher threshold will lower the number of false positives that are provided, but increase the chance of missing a true match. Moreover, a similarity threshold that a FRT operator believes to be optimal may work relatively well for one demographic group (*e.g.*, white people) while elevating the false-match rate for another demographic group (*e.g.*, Black people).[29] Further complicating matters, some agencies set no similarity threshold, or a threshold so low as to be meaningless. The Michigan State Police, for example, has configured its FRT algorithms to return 243 candidate images each time a search is run regardless of similarity score, meaning those results can include some or all candidate images with extremely low similarity scores.[30] These choices can have huge consequences for the risks of false identifications in real-world uses of the technology.

The image matching database used in a search also impacts outcomes. Searches will almost always return false matches. If a search is run against a database that does not include the person

[25] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Geo. L. Ctr. on Privacy & Tech. (May 16, 2019), https://www.flawedfacedata.com/.

[26] *Id.*

[27] *See id. See also, e.g.*, Mont. Code § 44-15-106 ("A law enforcement agency may not use facial recognition technology to identify an individual based on a sketch or other manually produced image.").

[28] Cognitec, *Law Enforcement*, https://www.cognitec.com/law-enforcement.html (last visited Mar. 27, 2024) ("Faces in photographs or recorded videos, as well as facial sketches/composites, can be compared to image databases of known criminals and provide investigators with the most similar faces.").

[29] K.S. Krishnapriya et al., *Characterizing the Variability in Face Recognition Accuracy Relative to Race* 3, IEEE/CVF Conf. on Computer Vision and Pattern Recognition Workshops (2019), https://arxiv.org/abs/1904.07325 ("A specified FMR [false match rate] is usually realized by different threshold values relative to the African-American and the Caucasian impostor distributions.").

[30] *See* Dep. of Jennifer Coulson at 19, *Williams v. City of Detroit*, No. 21-cv-10827 (E.D. Mich. July 7, 2023), ECF No. 60-2; Nat'l Acad. of Scis., *Facial Recognition: Current Capabilities, Future Prospects, and Governance* 46, 83–84 (2024), https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-and-governance.

who is a true match to the probe photo, every result returned by the search will necessarily be a false match.[31] And even in searches where a true match is returned somewhere in the results, it will almost always be accompanied by numerous—sometimes hundreds—of false matches. Yet those false matches will often look similar to the suspect precisely because the algorithms are designed to identify similar-looking images, elevating the risk of law enforcement personnel incorrectly selecting one of them as a purported match to the suspect photo. And the risk of false-match lookalikes grows with larger matching databases, because there is a greater likelihood of similar-looking people occurring in a larger population.[32] NIST identified this dynamic in a FRT test using a matching database of 12 million images; databases used in police FRT searches are often much larger.[33] Further, when police use matching databases that reflect historical biases, such as arrest photo databases that overrepresent people of color, disparities in the makeup of the database may elevate false-match rates for people of color in search results.[34]

The risks posed by human choices and practices when it comes to FRT are wide-ranging. When faced with these risks, legislators and regulators may focus on technical solutions—such as setting similarity thresholds or scores on specific statistical metrics that a system must clear in testing to be deployed—as a way to prevent harms. But while auditing and testing of FRT, including testing conducted by agencies such as NIST, is informative, the breadth and results of such testing are easily oversimplified by vendors and policymakers. Indeed, vendors routinely hold up their performance on tests in their marketing to government agencies even though those tests are conducted in laboratory, not real-world, conditions.[35] And in some states, lawmakers have sought to legislate "performance scores" that set across-the-board accuracy or error-rate requirements for facial recognition algorithms used by police.[36]

---

[31] *See* Patrick Grother et al., *Face Recognition Vendor Test Part 3: Demographic Effects* 5, Nat'l Inst. of Standards & Tech. (Dec. 2019), https://pages.nist.gov/frvt/reports/demographics/nistir_8280.pdf.

[32] *See* Patrick Grother et al., U.S. Dep't of Com., Nat'l Inst. for Standards & Tech., *Face Recognition Vendor Test (FRVT) Part 2: Identification* 8 (Sept. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8271.pdf.

[33] *See, e.g.*, Dep. of Krystal Howard at 42, *Williams v. City of Detroit*, No. 21-cv-10827 (E.D. Mich. July 7, 2023), ECF No. 60-3 (Michigan State Police matching database contained 55 million images in 2023); Chris Burt, *Clearview AI Tops 40 Billion Reference Images in Facial Recognition Database*, BiometricUpdate.com (Nov. 24, 2023), https://www.biometricupdate.com/202311/clearview-ai-tops-40-billion-reference-images-in-facial-recognition-database (Clearview AI claims matching database of more than 40 billion images).

[34] *See* Thaddeus L. Johnson et al., *Facial Recognition Systems in Policing and Racial Disparities in Arrests*, 39 Gov't Info. Q. no. 4, at 2 (2022).

[35] For example, Clearview AI has touted that its face recognition algorithm has been "rated highly by the National Institute of Standards and Technology (NIST)." *See* Zurah Shaker, *Debunking the Three Biggest Myths About Clearview AI*, Clearview AI (2023), https://www.clearview.ai/post/debunking-the-three-biggest-myths-about-clearview-ai (last visited Jan 18, 2024). *See also* Marissa Gerchick & Matt Cagle, *When it Comes to Facial Recognition Technology, There Is No Such Thing as a Magic Number*, ACLU (Feb. 7, 2024), https://www.aclu.org/news/privacy-technology/when-it-comes-to-facial-recognition-there-is-no-such-thing-as-a-magic-number.

[36] *See, e.g.*, A.B. 642, 2023 Leg., Reg. Sess. (Cal. 2023), https://legiscan.com/CA/text/AB642/id/2796168 (proposal requiring police-used algorithms to have an "accuracy score of 98 percent true positives").

A fixation on simplistic FRT test scores and accuracy requirements not only ignores the above-discussed role of humans in the creation and use of FRT systems, it also risks obscuring findings that point to the harm of face recognition while overstating the probative value of such tests. For one example, this focus on specific metrics obscures that a FRT algorithm that clears some sort of "performance" score in one respect in testing — say, producing an overall true match rate above 98% or 99% on a given dataset at some similarity threshold — may also produce a false match rate for Black men three times the false match rate for white men in testing that is broken down by race.[37] A focus on these kinds of performance metrics also risks overstating what was actually tested—algorithms are routinely tested on datasets that differ in important ways from the photos of mugshots, licenses, or surveillance photos held by and used by police agencies. In addition, testing of FRT systems like the NIST evaluations may consider the performance of FRT systems across a variety of system settings, including the use of various similarity score thresholds for returning candidate match results.[38] The accuracy or error rates of a FRT system depend critically on this threshold, and if the threshold is often chosen or customized by the entity deploying the FRT system, testing results based on the use of other thresholds will not faithfully represent the system's performance in practice.

Because of these and other differences, a face recognition algorithm's performance in testing cannot be easily or quickly generalized to make broad claims about whether a FRT algorithm is safe. Taking all of this into account, policymakers should recognize the critical importance of independent and holistic testing of FRT systems, and should also be cautious about looking to accuracy, error rate, or other threshold requirements as a panacea to the problems posed by law enforcement's use of face recognition. Any metric used to assess a FRT system will necessarily involve tradeoffs with real-world impacts.

Any test designed to assess accuracy of the FRT search process must at least account for the tremendous real-world variability in: probe image quality (including countless permutations and combinations of illumination, pose, angle, occlusion, facial expression, and image definition); probe image manipulation; the size and makeup of image matching databases; similarity threshold settings in FRT algorithms; the quality and nature of training of human analysts who must select an image from a gallery of candidates generated by the algorithm;[39] and the cognitive biases of

[37] For one demonstrative example, an FRT algorithm developed by the vendor NEC and submitted to NIST's vendor testing program produced an overall true match rate above 98% in testing at certain thresholds and using certain datasets. *See* Nat'l Inst. for Standards & Tech., *Face Recognition Vendor Test Report Card for NEC-2* 1, https://pages.nist.gov/frvt/reportcards/1N/nec_2.pdf (finding a false negative identification rate (FNIR) of less than .02—or 2%—for testing using multiple datasets. The true positive identification rate (TPIR) is one minus the FPIR). However, in other NIST testing, the same algorithm also produced false match rates for Black men more than three times the false match rate for white men at various thresholds. *See* Patrick Grother et al., U.S. Dep't of Com., Nat'l Inst. for Standards & Tech., *Face Recognition Vendor Test Part 3: Demographic Effects* Annex 16 at 34 fig.32, (Dec. 2019), https://pages.nist.gov/frvt/reports/demographics/annexes/annex_16.pdf.

[38] *See, e.g.*, Patrick Grother et al., U.S. Dep't of Com., Nat'l Inst. for Standards & Tech., *Face Recognition Vendor Test Part 3: Demographic Effects* 20–22 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf (discussing the thresholds used in the NIST vendor testing).

[39] *See* U.S. Gov't Account. Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties* 19 (Sept. 2023), https://www.gao.gov/assets/gao-23-

those human examiners.[40] Although some FRT accuracy tests assess some variability in probe image quality[41] or similarity thresholds, none account for the full range of variables that affect outcomes of real-world police FRT searches. Decisions about whether and how to use face recognition technology should not rest on illusory promises of accuracy, reliability, and fairness under current testing regimes.

2. Law enforcement reliance on FRT leads to wrongful arrests.

Proponents of law enforcement use of face recognition technology frequently defend against evidence of its dangers by emphasizing that police are warned that it is intended to generate investigative leads only and must be followed by additional investigation in order to demonstrate probable cause to arrest. However, records from law enforcement investigations across the country demonstrate that this admonition is woefully inadequate and fails to protect people against serious deprivations of liberty, as demonstrated by the FRT-based wrongful arrests publicly known to date. In at least five of the seven known cases, police were warned that FRT results do not constitute a positive identification or probable cause, but arrested an innocent person nonetheless.

Law enforcement organizations and FRT vendors have long offered boilerplate warnings that an FRT search result does not constitute a positive identification of a suspect, and additional investigation is needed to develop probable cause to arrest. Such warnings have been issued, for example, by the International Association of Chiefs of Police,[42] in the documentation from

105607.pdf ("From October 2019 through March 2022, seven agencies used facial recognition services to support criminal investigations. During this time period, one agency—HSI—required staff to take facial recognition training prior to using services, while the other six agencies did not have requirements in place."); Nicholas Bacci et al., *Validation of Forensic Facial Comparison by Morphological Analysis in Photographic and CCTV Samples*, 135 Int'l J. of Legal Med. 1965, 1965 (2021) (study showing that even trained examiners conducting morphological analysis on CCTV footage under ideal conditions had high false-positive and false-negative rates).

[40] *See generally* Itiel E. Dror et al., *The Impact of Human-Technology Cooperation and Distributed Cognition in Forensic Science: Biasing Effects of AFIS Contextual Information on Human Experts*, 57 J. Forensic Sci. 343 (2012); Daniel J. Solove & Hideyuki Matsumi, *AI, Algorithms, and Awful Humans*, 96 Fordham L. Rev. __, manuscript at 15 (forthcoming 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4603992 ("Empirical studies show that people readily defer to automated systems, overlook errors in algorithms, and deviate from algorithmic output in ways that render a less accurate result.").

[41] *See, e.g.*, Patrick Grother et al., U.S. Dep't of Com., Nat'l Inst. for Standards & Tech., *Face Recognition Vendor Test Part 3: Demographic Effects* (Dec. 2019), https://pages.nist.gov/frvt/reports/demographics/nistir_8280.pdf; Aman Bhatta et al., *Impact of Blur and Resolution on Demographic Disparities in 1-to-Many Facial Identification* (2023), https://arxiv.org/abs/2309.04447.

[42] IJIS Institute, *Law Enforcement Facial Recognition Use Case Catalog* 3 (March 2019), https://www.theiacp.org/sites/default/files/2019-10/IJIS_IACP%20WP_LEITTF_Facial%20Recognition%20UseCasesRpt_20190322.pdf (a FRT search result is "a strong clue, and nothing more, which must then be corroborated against other facts and investigative findings before a person can be determined to be the subject whose identity is being sought").

companies that develop and sell FRT,[43] in law enforcement agency policies,[44] including the DOJ Bureau of Justice Assistance's 2017 FRT policy development template[45] and DHS's recently issued FRT policy,[46] and on face recognition search result forms provided to investigating officers.[47] However, though ubiquitous, these warnings have failed to prevent wrongful arrests due to police reliance on incorrect FRT results. Federal policy must reflect that these boilerplate admonitions are not adequate to avoid wrongful arrests flowing from false matches from FRT searches.

Two main problems are evident in the known cases of FRT-derived wrongful arrests. First, police reflexively treat the FRT result as a positive identification, ignoring or not understanding warnings that face recognition technology is manifestly not designed to positively identify or match photos.[48] In a New Jersey case, for example, a detective obtained an arrest warrant based

---

[43] *See, e.g.*, Ex. B at 25, Plaintiff's Response to Defendant's Motion to Dismiss, *ACLU v. Clearview AI., Inc.*, 2020 CH 04353 (Ill. Cir. Ct. Nov. 02, 2020), https://www.aclu.org/cases/aclu-v-clearview-ai?document=Plaintiffs-Response-to-Defendants-Motion-to-Dismiss (the Clearview AI Official Disclaimer 2019 notes that "[s]earch results established through Clearview AI and its related systems and technologies are indicative and not definitive. . . . Law enforcement professionals MUST conduct further research in order to verify identities."); *Code of Ethics*, Rank One Computing, https://roc.ai/code-of-ethics/ (last visited Jan. 18, 2024) ("Face recognition should not be used as the sole support of probable cause for arrest, search or seizure of any U.S. citizen or any property. Independent evidence should be required to establish probable cause."); Cognitec, *Fighting Crime and Curtailing Human Bias with Face Recognition* (last visited Jan. 18, 2024), https://www.cognitec.com/news-reader/fighting-crime-and-curtailing-human-bias-with-face-recognition.html ("the software is used as a lead generation tool only, as the starting point of an investigation that uses additional methods to find or identify the person").

[44] *See, e.g.*, N.Y. State Div. of Crim. Justice Servs., Mun. Police Training Council, *Facial Recognition Model Policy* 3 (Dec. 2019), https://www.criminaljustice.ny.gov/crimnet/ojsa/standards/MPTC%20Model%20Policy-Facial%20Recognition%20December%202019.pdf ("Potential identifications made using face recognition software shall be considered investigative leads only and shall not be deemed positive identification."); Ind. Intelligence Fusion Ctr., *Face Recognition Policy* 14 (June 2019), https://www.in.gov/iifc/files/Indiana_Intelligence_Fusion_Center_Face_Recognition_Policy.pdf ("A candidate image is an investigative lead only and does not establish probable cause to obtain an arrest warrant without further investigation."); L.A. Cnty. Reg'l Identification Sys., *Facial Recognition Policy* 6 (Sept. 2021), https://lacris.org/LACRIS%20Facial%20Recognition%20Policy%20v_2019.pdf ("Users acknowledge the result of any FR search provided by LACRIS shall be deemed an investigative lead only and RESULTS ARE NOT TO BE CONSIDERED AS PROVIDING A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.") (emphasis in original).

[45] U.S. Dep't of Justice, Bureau of Justice Assistance, *Face Recognition Policy Development Template* 22 (Dec. 2017), https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf.

[46] Dep't of Homeland Sec., Directive No. 026-11, *Use of Face Recognition and Face Capture Technologies* 6 (Sept. 11, 2023), https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_026-11-use-face-recognition-face-capture-technologies.pdf.

[47] *See, e.g.*, City of Detroit's Response to Plaintiff's Motion to Compel Discovery, Ex. 7, *Williams v. City of Detroit*, No. 21-cv-10827 (E.D. Mich. May 3, 2022), ECF No. 20-7.

[48] This may be in part due to automation bias, as well as poor training, perverse incentives to close cases, and other factors. *See, e.g.*, Shira Ovide, *A Case for Banning Facial Recognition*, N.Y. Times (June 9, 2020), https://www.nytimes.com/2020/06/09/technology/facial-recognition-software.html.

solely on an assertion that face recognition technology had generated "a high profile comparison" to the probe image and that "[t]he suspect was identified as Nijeer Parks."[49] This despite the detective having filled out a face recognition request form that warned prominently that any "possible match . . . should only be considered an investigative lead. Further investigation is needed to confirm a possible match through other investigative corroborated information and/or evidence. INVESTIGATIVE LEAD, NOT PROBABLE CAUSE TO MAKE AN ARREST."[50] Mr. Parks was subsequently arrested and jailed for 10 days for a crime he did not commit.[51]

In a Louisiana case, police relied solely on a face recognition search result generated by Clearview AI as purported probable cause, despite the law enforcement agency having signed a service agreement with Clearview acknowledging that FRT search results "are indicative and not definitive" and that officers "must conduct further research in order to verify identities or other data generated by the [Clearview] system. [Clearview] is neither designed nor intended to be used as a single-source system for establishing the identity of an individual."[52] That investigation led to the wrongful arrest of Randal Quran Reid, a Georgia resident who had never even been to Louisiana.[53]

In an Indiana investigation, police similarly obtained an arrest warrant based only upon an assertion that the detective "viewed the footage and utilized the Clearview AI software to positively identify the female suspect."[54] No additional basis for the purported identification was presented, nor did police explain that the FRT system was not in fact capable of providing a positive identification.

Second, when police do conduct additional investigative steps, those steps often *exacerbate* the unreliability of FRT searches. This is a particular problem when police move directly from a facial recognition lead to a witness identification procedure. Face recognition technology is designed to generate a list of faces that are *similar* to the probe image, but may not in fact be a match to the face in the probe image. As one appellate court has explained, this "has obvious implications for the accuracy of the identification process because [a photo-lineup] array constructed around a mistaken potential match would leave the witness with no actual perpetrator to choose."[55] Even more, the FRT-generated image in a photo array is likely to appear more similar

[49] Exhibits to Defs' Motion for Summary Judgment, *Parks v. McCormac*, No. 21-cv-04021 (D.N.J. July 23, 2021), ECF No. 109-5, at 253.

[50] *Id.* at 290.

[51] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. Times (Dec. 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[52] Complaint Ex. 3, *Reid v. Bartholomew*, No. 23-cv-04035-JPB (N.D. Ga. Sept. 8, 2023), ECF No. 1-3.

[53] Kashmir Hill & Ryan Mac, *'Thousands of Dollars for Something I Didn't* Do', N.Y. Times (Mar. 31, 2023), https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html.

[54] Houston Harwood, *Company Says Facial Recognition Can't Be Used in Arrests, but It's Happening in Evansville*, Courier & Press (Oct. 19, 2023) https://www.courierpress.com/story/news/local/2023/10/19/evansville-police-using-clearview-ai-facial-recognition-to-make-arrests/70963350007/.

[55] *State v. Arteaga*, 296 A.3d 542, 557 (N.J. App. Div. 2023).

to the suspect than the filler photos, increasing the chance that a witness will choose that image out of the lineup even though it is not a true match.[56]

This problem contributed to all three known FRT-derived wrongful arrests by the Detroit Police Department.[57] In each, police obtained an arrest warrant based solely on the combination of a false match from FRT, and a false identification from a witness viewing a six-pack photo lineup that was constructed around the FRT lead and five filler photos. In two of those cases, the photo arrays were presented to eyewitnesses who had gotten good looks at the alleged perpetrators (in the third case the photo array was presented to a non-eyewitness who had merely viewed the same low-quality store surveillance footage that police already had in their possession). In all three cases, the witnesses chose the FRT-derived false-match, instead of deciding that the suspect did not in fact appear in the lineup. A lawsuit filed earlier this year in Texas alleges that a similar series of failures led to the wrongful arrest of Harvey Eugene Murphy Jr. by Houston police.[58]

Law enforcement personnel themselves make similar errors when reviewing FRT results. In a Maryland case, for example, an FRT search in an investigation into an assault on a bus driver generated an incorrect lead to a photo of Alonzo Sawyer. Maryland Transit Authority Police arrested Mr. Sawyer after "verifying" the results of the FRT search with Mr. Sawyer's former parole officer from an unrelated conviction. The parole officer opined that the image of the assault suspect looked like Mr. Sawyer, which police used to secure an arrest warrant.[59] The parole officer later recanted his mistaken identification, but too late to prevent Mr. Sawyer from being arrested and spending nine days in jail.

After the Detroit Police Department's third FRT-derived wrongful arrest became public last year, Detroit's Chief of Police acknowledged the problem of erroneous FRT results tainting subsequent witness identifications, explaining that by moving straight from FRT result to lineup "it is possible to taint the photo lineup by presenting a person who looks most like the suspect" but

---

[56] *See* Eyal Press, *Does A.I. Lead Police to Ignore Contradictory Evidence?*, New Yorker (Nov. 20, 2023), https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence/; Brief of Gary L. Wells, Ph.D as Amicus Curiae, *State v. Arteaga*, 296 A.3d 542 (N.J. App. Div. 2023); Laura Moy, *Facing Injustice: How Face Recognition Technology May Increase the Incidence of Misidentifications and Wrongful Convictions*, 30 Wm. & Mary Bill Rts. J. 337 (2021).

[57] *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 (describing the wrongful arrest of Robert Williams); Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. Times (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html (describing the wrongful arrest of eight-month pregnant Porcha Woodruff); Elisha Anderson, *Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit*, Detroit Free Press (July 10, 2020), https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/ (describing the wrongful arrest of Michael Oliver).

[58] Johana Bhuiyan, *Facial Recognition Used after Sunglass Hut Robbery Led to Man's Wrongful Jailing, Says Suit*, The Guardian (Jan. 22, 2024), https://www.theguardian.com/technology/2024/jan/22/sunglass-hut-facial-recognition-wrongful-arrest-lawsuit.

[59] Eyal Press, *Does A.I. Lead Police to Ignore Contradictory Evidence?*, New Yorker (Nov. 20, 2023), https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence/.

is not in fact the suspect.[60] He announced an intent to implement policy changes to prevent similar failures in future investigations.[61]

Indeed, in each of Detroit's FRT-derived wrongful arrest cases basic investigation would have easily ruled out the people produced by the FRT search as leads. In the case of Michael Oliver, for example, additional investigation would have revealed that Mr. Oliver had numerous visible tattoos where the suspect had none. In the case of Porcha Woodruff, police arrested her while eight months pregnant for a carjacking and armed robbery that took place less than a month prior, but surveillance footage and witness interviews would have easily established that the suspect was not visibly pregnant at the time of the alleged criminal conduct. And in the case of Robert Williams, basic investigation would have shown that Mr. Williams was driving home from work miles outside of Detroit at the time of the midtown-Detroit shoplifting for which he was charged. Yet officers' tendency to trust the algorithms' results overrode the need to conduct reliable investigation. Warnings that the FRT results do not constitute probable cause were not sufficient to motivate police to conduct adequate investigations.

Experts on eyewitness identifications agree that police should develop "evidence-based grounds to suspect that an individual is guilty of the specific crime being investigated before including that individual in an identification procedure."[62] Because FRT searches lack reliability, FRT results can never constitute such "evidence-based grounds" for conducting a photo lineup. Similarly, neither an FRT result alone, nor an FRT result plus an identification procedure, can constitute probable cause, and relying on them as such creates an intolerable risk of false identification and wrongful arrest. Even a short time in jail can have devastating effects, including loss of employment, separation from family and inability to care for children, negative notations on credit reports that are never updated to indicate the arrest was wrongful, and others. Because police have repeatedly proved unable or unwilling to follow FRT searches with adequate independent investigation, police access to the technology should be strictly curtailed.

3. Law enforcement use of FRT is marred by lack of transparency.

Problems with the use of FRT in investigations are compounded by lack of transparency, including inadequate disclosures to courts and criminal defendants.

a) Law enforcement omits material information about FRT from warrant applications.

Excessive secrecy begins pre-arrest, with inadequate disclosures to magistrates by police applying for arrest warrants. Law enforcement officers have a constitutional obligation to provide accurate information in arrest warrant applications so that magistrates can independently determine

[60] City of Detroit Government, *WATCH LIVE: Chief White Will Provide Updated Comments on a Lawsuit Filed Last Week*, Facebook (Aug. 9, 2023), https://www.facebook.com/CityofDetroit/videos/287218473992047.

[61] *Id.*

[62] Gary G. Wells et al., *Policy and Procedure Recommendations for the Collection and Preservation of Eyewitness Identification Evidence*, 44 L. & Hum. Behav. 3, 8 (2020), https://doi.org/10.1037/lhb0000359.

whether there is probable cause.[63] But police routinely overstate the certainty of FRT matches and withhold details about FRT searches that would let judges understand why those searches lack reliability and are not a proper basis for probable cause.

In some cases, police completely conceal the fact of their reliance on FRT. In the Louisiana investigation leading to the wrongful arrest of Randal Quran Reid, for example, the detective misleadingly wrote only that he was "advised by a credible source" that the man in the surveillance footage was Mr. Reid.[64] A judge signed off on the arrest warrant, unaware of the role FRT had played in the investigation. The warrant was eventually recalled after Mr. Reid's attorney presented prosecutors with photos and videos of him that made clear that he was not, in fact, the person in the surveillance footage of the crime under investigation. But at that point, Mr. Reid had already spent nearly a week in jail, and his parents had spent thousands of dollars on legal counsel.[65]

Even when police disclose their use of FRT, they frequently withhold critical information about the search. In the case of Nijeer Parks, for example, Woodbridge, New Jersey, police did disclose the use of FRT in a warrant application, but left out details crucial to evaluating the reliability of the FRT search, including that the probe image was a heavily shadowed and pixelated scan of a fake driver's license,[66] and that the officer who conducted the FRT search told the lead detective that he had "altered the photo on the license a little to get the pixels clear."[67] The warrant application also misrepresented the FRT result as a "high profile comparison" rather than what it really was: a low-reliability investigative lead.[68] Similarly, in the case of Robert Williams in Detroit, police failed to explain to the magistrate that the probe image was low-resolution and not suitable for producing a reliable match, nor that the FRT results returned a possible match to Mr. Williams's old, expired driver's license photo, but not to his current license photo (which was also in the database that was searched but was not identified as among the 243 most likely matches to the suspect).[69] This should have been an indication that the algorithm's results lacked reliability.

Because magistrate judges are unlikely to have independent expertise about FRT, it is critical that officers fully inform them of information that explains the fundamental lack of reliability of FRT results. Otherwise, judges are likely to over-rely on FRT search results and make

---

[63] *See Franks v. Delaware,* 438 U.S. 154, 165 (1978).

[64] Affidavit for Arrest Warrant, *State v. Reid*, No. F-21850-22 (24th Jud. Dist Ct. Parish of Jefferson Jul. 18, 2022), https://int.nyt.com/data/documenttools/affidavit-warrant-recall-f-21850-22-randal-reid-redacted/1f81c9d0a4abda7a/full.pdf.

[65] Kashmir Hill & Ryan Mac, *'Thousands of Dollars for Something I Didn't* Do', N.Y. Times (Mar. 31, 2023), https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html.

[66] Exhibits to Defs' Motion for Summary Judgment, *Parks v. McCormac*, No. 21-cv-04021 (D.N.J.), ECF No. 109-5, at 281–82.

[67] *Id.* at 380.

[68] *Id.* at 253. In a second arrest warrant application submitted by a different officer, police omitted any mention of use of FRT. *See id.* at 267–68.

[69] First Amended Complaint ¶¶ 11, 69–71, 79, 110, *Williams v. City of Detroit*, No. 21-cv-10827 (E.D. Mich.), ECF No. 54.

unjustified probable cause findings. Yet, DHS's policy on use of FRT does not address the necessity of fulsome and accurate disclosures in warrant applications.[70]

b) Prosecutors withhold information about FRT from criminal defendants.

Inadequate disclosures continue post-arrest, where prosecutors routinely resist turning over adequate information about FRT use as part of their pre-trial disclosure obligations under *Brady* and related doctrines.

In a criminal prosecution, the government has a responsibility to disclose material information that tends to exculpate the defendant and/or undermine the credibility of prosecution witnesses.[71] Information is material if it tends to undermine confidence in the result of the criminal case.[72] This disclosure obligation attaches whether or not the defense has requested it.[73]

Face recognition technology is unreliable in many ways that human witnesses are, and defendants should be able to confront its unreliability. Identifications by a human witness selecting from a lineup clearly implicate *Brady*;[74] the government would be obligated to disclose the identification of alternate suspects and information relating the witness' confidence in their identification. FRT should not be subject to a lower standard. To comply with its obligations under *Brady* and related disclosure rules, the prosecution must give defendants access to, at a minimum: (1) information about the FRT system itself (source code, training data, operating manual and other documentation, executable version of the software, validation studies); (2) information about the application of FRT in their specific case (including other possible matches generated by the software, the similarity scores assigned to them, and the similarity threshold used in the search and how it was chosen); and (3) information about the officer or analyst that ran the search and their interactions with the technology (whether the officer or analyst manipulated the probe image, how the officer or analyst interpreted the FRT results, how they acted on the results, whether they ran multiple searches, whether they were trained to use the software, etc.).

Prosecutors regularly refuse to release this information to defendants. Prosecutors have tried to justify lack of disclosure on the basis that they are "not seeking to introduce the facial recognition technology as evidence of the Defendant's guilt," and that the technology "was merely a tool, among many other investigative tools that law enforcement use daily to identify potential suspects."[75] But information about FRT use is very much material, including because it can negate

[70] *See* Dep't of Homeland Sec., Directive No. 026-11, *Use of Face Recognition and Face Capture Technologies* (Sept. 11, 2023), https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_026-11-use-face-recognition-face-capture-technologies.pdf.

[71] *See Brady v. Maryland*, 373 U.S. 83 (1963).

[72] *See United States v. Bagley*, 473 U.S. 667, 682 (1985)

[73] *United States v. Agurs*, 427 U.S. 97, 110–11 (1976)

[74] *See Kyles v. Whitley*, 514 U.S. 419, 453–54 (1995).

[75] State's Brief (Amended) at 9, *State v. Arteaga*, 296 A.3d 542 (N.J. App. Div. 2023).

guilt by showing how an initial incorrect FRT result may have tainted later investigative steps.[76] Similarly, if an FRT search was conducted in a given case and did *not* identify as an investigative lead the suspect who was ultimately arrested, this is potentially exculpatory information that must be turned over to a defendant—just as prosecutors would be required to inform defense counsel if a witness had picked another person out of a lineup or if they had received an anonymous tip that a different person committed the crime in question.

In an unknown number of cases, the government fails to even notify defendants of the fact that FRT was used in the investigation, much less details of that use. Even when the fact of FRT use is disclosed, the prosecution often continues to withhold key details that are critical to mounting a defense. In a Florida case, for example, police submitted a low-resolution, off-angle photo of a suspect for an FRT search and used the result of the search to prosecute Willie Allen Lynch.[77] But despite the centrality of the FRT search to the investigation, the government refused to turn over critical information that would have allowed Mr. Lynch to challenge the reliability of the purported match, including the other possible matches generated by the FRT search. Mr. Lynch was convicted and sentenced to eight years, without having been able to adequately challenge the reliability of the FRT result and its role in driving the rest of the investigation.

In a New Jersey case, after the prosecution was similarly resistant to disclosing critical information about the FRT search that inculpated Francisco Arteaga, an appeals court held that prosecutors violated Mr. Arteaga's constitutional rights when they refused to disclose information about the FRT system and search used in the case against him.[78] The court ordered the prosecution to turn over detailed information about the technology used, including source code, error rates, the candidate list returned from the search, information about the photo database, the report produced by the analyst who ran the search, and the qualification of the analyst who ran the search.[79] Rejecting the government's argument that it needn't disclose this information because it did not intend to introduce the FRT result as evidence at trial, the court explained that the "[d]efendant must have the tools to impeach the State's case" and that "the items sought by the defense have a direct link to testing FRT's reliability and bear on the defendant's guilt or innocence."[80]

Courts are just beginning to adjudicate challenges to the lack of disclosure about FRT searches and practices in criminal cases. Without robust rules binding police and prosecutors and ensuring disclosure of information bearing on the details and reliability of FRT searches, people accused of crimes will be unable to mount robust defenses, in violation of their due process rights.

---

[76] *See* Clare Garvie, *A Forensic Without the Science: Facial Recognition in U.S. Criminal Investigations* at 41–43, Geo. L. Ctr. on Privacy & Tech. (2022), https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/.

[77] *See Amici Curiae* Brief of ACLU et al., *Lynch v. State*, No. SC2019-0298 (Fla. Sup. Ct. 2019), https://www.aclu.org/sites/default/files/field_document/florida_face_recognition_amici_brief.pdf; *Lynch v. State*, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018).

[78] *State v. Arteaga*, 296 A.3d 542 (N.J. App. Div. 2023).

[79] *Id. at* 558.

[80] *Id.*

c) Public reporting on FRT use is necessary for transparency and oversight

Additional needed transparency should take the form of regular public reporting of aggregate data about FRT use. State and local jurisdictions that have begun to regulate FRT use have imposed such reporting requirements.[81] Public reporting of this data has enabled critical public and legislative oversight, including shedding light on the technology's lack of efficacy and how it is used to disproportionately target people of color.[82]

Until federal law enforcement use of FRT is fully curtailed, there should be robust annual or semi-annual reporting of basic data about FRT searches. Any agency that uses FRT should be required to report, at a minimum: (1) aggregate information on the use of FRT, including (A) total number of facial recognition search requests, (B) number of facial recognition search requests that generated leads, and (C) demographic breakdown of individuals in probe photos by race and sex; (2) information about the FRT system and algorithm(s) used, including vendor, version, and similarity threshold; and (3) a log of facial recognition searches, including (A) the requesting agency or field office; (B) the crime under investigation; (C) the race and sex of individual in the probe photograph; (D) whether the search generated results; (E) whether a facial recognition lead was provided to the requesting agency, field office, or officer; and (F) whether any individual appearing as a possible match in the FRT search was subsequently arrested or charged.

4. FRT surveillance of live or recorded video poses a critical threat to civil liberties.

The predominant current use of face recognition technology by police in the United States involves trying to identify suspects from photographs or from still frames extracted from video. However, the threat of video face recognition surveillance looms, with one U.S. jurisdiction recently deploying a FRT-enabled surveillance camera network.[83] Deployment of FRT for video tracking and surveillance poses a catastrophic threat to privacy, free speech, and freedom of movement, by putting in the hands of government the ability to identify and track anyone or everyone as they go about their daily lives.

U.S. cities have purchased software that purports to be able to run face recognition searches on live or stored video, and several law enforcement agencies, including at the federal level, are known to have piloted such technology.[84] The federal government has heavily invested in

---

[81] *See, e.g.*, Mont. Code Ann. § 44-15-111; Mass. Gen. Laws Ann. ch. 6, § 220(d); Va. Code § 52-4.5(F); New Orleans Code of Ordinances § 147-2(i); Detroit Police Department Directive No. 307.5, Facial Recognition §§ 6.2–6.3 (Sept. 19, 2019).

[82] *See, e.g.*, Alfred Ng, '*Wholly Ineffective and Pretty Obviously Racist': Inside New Orleans' Struggle with Facial-Recognition Policing*, Politico (Oct. 31, 2023), https://www.politico.com/news/2023/10/31/new-orleans-police-facial-recognition-00121427.

[83] Sara-Megan Walsh, *LDDA is Tracking 'People of Interest' in Downtown Lakeland Using Facial Recognition*, Lakeland Ledger (Mar. 21, 2024), https://www.theledger.com/story/news/local/2024/03/21/ldda-using-new-cameras-to-track-people-of-interest-in-downtown/73052094007/.

[84] Clare Garvie & Laura M. Moy, *America Under Watch*, Geo. L. Ctr. on Privacy & Tech. (May 16, 2019), https://www.americaunderwatch.com/; Jay Stanley, *Secret Service Announces Test of Face Recognition System Around White House*, ACLU (Dec. 4, 2018), https://www.aclu.org/news/privacy-technology/secret-service-announces-test-face-recognition.

improving the performance of FRT to analyze video, including for applications like public surveillance cameras and drones.[85] In a 2019 presentation released to the ACLU through a Freedom of Information Act lawsuit, a program manager at the Intelligence Advanced Research Project Agency (IARPA) detailed a collaboration between government agencies and researchers to "dramatically improve face recognition performance in massive video collections."[86] The program, called "Janus," aimed to enable face recognition surveillance of "millions of subjects" and support "partial, incomplete, and occluded views" of faces.[87] The presentation detailed tests conducted so far, including testing on surveillance video captured at a Department of Defense training facility. Other documents summarized plans to transition the project to other government agencies.

Just last month, the Lakeland Downtown Development Authority (LDDA), a governmental entity in Lakeland, Florida, began installing a network of 14 face-recognition enabled surveillance cameras throughout the city's downtown.[88] LDDA staff uploaded photos of several "people of interest" into the FRT system, and the "cameras [were] equipped with a facial recognition software to detect and record when those individuals move through a camera's field," allowing officials to "follow some of [their] patterns of behavior" and send alerts to police.[89] To the ACLU's knowledge, such government deployment of networked FRT surveillance cameras in an American city is nearly unprecedented,[90] raising acute civil liberties and civil rights concerns. The LDDA turned off the FRT capability in response to criticism from the ACLU and others,[91] but the implementation of the FRT surveillance system even for a couple weeks showed that the concern with this technology is far from hypothetical.

Although tests have shown high inaccuracy rates for use of FRT on surveillance video,[92] development and deployment of an even moderately accurate system would pose severe civil liberties concerns. Use of FRT on live or recorded video threatens to allow police to efficiently track one or many individuals across multiple video feeds, or to pull up every instance of one or

---

[85] Drew Harwell, *FBI, Pentagon Helped Research Facial Recognition for Street Cameras, Drones*, Wash. Post (Mar. 7, 2023), https://www.washingtonpost.com/technology/2023/03/07/facial-recognition-fbi-dod-research-aclu/.

[86] [Redacted], Program Manager, Intel. Advanced Rsch. Project Agency, Janus: Unconstrained Face Recognition (Feb. 4, 2019) (on file with authors) [hereinafter Janus Presentation].

[87] *Id*.

[88] Sara-Megan Walsh, *LDDA is Tracking 'People of Interest' in Downtown Lakeland Using Facial Recognition*, Lakeland Ledger (Mar. 21, 2024), https://www.theledger.com/story/news/local/2024/03/21/ldda-using-new-cameras-to-track-people-of-interest-in-downtown/73052094007/.

[89] *Id.; see also* LDDA, *Cameras*, https://downtownlkld.com/cameras/ (last visited Apr. 5, 2024).

[90] In 2001, the Tampa Police Department deployed a network of several dozen face recognition-enabled surveillance cameras, but shut down the experiment after a few months. Jay Stanley & Barry Steinhardt, *Drawing a Blank: The Failure of Facial Recognition Technology in Tampa, Florida*, ACLU (Jan. 3, 2002), https://www.aclu.org/wp-content/uploads/publications/drawing_blank.pdf.

[91] LDDA, *Cameras*, https://downtownlkld.com/cameras/ (last visited Apr. 5, 2024).

[92] *See* Vikram Dodd, *UK Police Use of Facial Recognition Technology a Failure, Says Report*, The Guardian (May 14, 2018), https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure; *see also* Janus Presentation.

more persons appearing in video recordings over time.[93] This capability, which has already been used to devastating effect by some foreign governments,[94] threatens to chill exercise of First Amendment rights of free speech and assembly. Members of the public, aware they are being watched, might alter their behavior and self-censor.

Such surveillance would also infringe on our basic right to privacy protected by the Fourth Amendment. This technology threatens to give the government the unprecedented ability to instantaneously identify and track anyone as they go about their daily lives; such invasive tracking would easily reveal an individual's "familial, political, professional, religious, and sexual associations" by tracking her as she moves through "private residences, doctor's offices, political headquarters, and other potentially revealing locales."[95] The Supreme Court has made clear that we do not "surrender all Fourth Amendment protection by venturing into the public sphere."[96] When it comes to pervasively tracking people's movements using modern technologies, the Fourth Amendment's protections fully apply. In *Carpenter v. United States*, for example, the Supreme Court held that targeted government access to a particular individual's historical cell site location information requires a warrant.[97] And courts have further held that dragnet tracking—for example, using wide-angle aerial cameras to capture the movements of pedestrians and drivers across a whole city—constitutes an unconstitutional general search.[98] Not even a warrant could authorize such mass surveillance. Applying FRT to networks of surveillance cameras that already cover many U.S. cities would raise similar concerns.

In recognition of the acute threat to civil liberties posed by FRT video surveillance, even jurisdictions that allow some use of FRT by police to attempt to identify individuals in still images have banned FRT video surveillance.[99] Federal agencies should immediately ban use of FRT on live or recorded video.

---

[93] *See* Nat'l Acad. of Scis., *Facial Recognition Technology: Current Capabilities, Future Prospects, & Governance* 25–26 (2024), https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-and-governance.

[94] *See, e.g.*, Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. Times (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; Lena Masri, *How Facial Recognition Is Helping Putin Curb Dissent*, Reuters (Mar. 28 2023), www.reuters.com, https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/; Daniel Salaru, Int'l Press Inst., *Russia: Facial Recognition Software Used to Target Journalists*, International Press Institute (June 23, 2022), https://ipi.media/russia-facial-recognition-software-used-to-target-journalists/.

[95] *Carpenter v. United States*, 138 S. Ct. 2206, 221 (2018).

[96] *Id.* at 2217.

[97] *Id.* at 2212.

[98] *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 348 (4th Cir. 2021) (en banc).

[99] *See, e.g.*, Mont. Code Ann. § 44-15-104; Mass. Gen. Laws. Ann. ch. 6, § 220(a); Va. Code § 52-4.5(D); Detroit Police Dep't Directive No. 307.5, Facial Recognition §§ 3.1–3.2 (Sept. 19, 2019); L.A. Cnty. Regional Identification System, Facial Recognition Policy ¶ E (Sept 1, 2021); Orlando Police Dep't Policy & Procedure 1147.2, Facial Recognition § 5.3 (June 6, 2022).

II. Face Recognition Technology in Immigration Enforcement

The same concerns with accuracy, bias, and surveillance that plague use of FRT in law enforcement investigations also apply in the immigration enforcement context.

Additionally, immigration authorities have deployed FRT for identity verification of people seeking entry to the United States, including at ports of entry and as part of internet applications controlling access to immigration benefits. Disparate failure rates of this technology by race and skin tone are of particularly acute concern in this context. For example, reports last year indicated that darker skinned migrants attempting to use the CBP One app to schedule asylum interviews at the U.S. border have had persistent difficulty using the app because its face recognition feature failed to recognize their faces.[100] And even when FRT systems are able to register the presence of a person's face, they may produce false negatives at higher rates for members of some demographic groups.[101]

Even when FRT identity verification works relatively well at a technical level, its adoption can create barriers to access to essential services for people living on low incomes, people with disabilities, older people, and members of other marginalized communities. FRT identity verification requirements that rely on access to, familiarity with, or ability to operate technology (such as smartphones, web cameras, or high-speed internet connections) can disproportionately harm individuals who lack access to or the ability to use those systems. And due to disparate rates of technology access by race, income, age, and disability status, these burdens will fall disproportionately on members of already marginalized communities. Even FRT applications that do not rely on users' own access to technology can produce high failure rates in practice "owing to poor usability. This is especially true in systems that are not used regularly—like border control gates—where subjects will not be habituated to the process."[102]

Use of FRT in contexts such as border checkpoints also raises privacy concerns. Identity verification systems should not lead to government retention of sensitive biometric information, which can be vulnerable to data breaches and can enable mass surveillance. And binding policy should provide alternative options for identity verification.

---

[100] Melissa del Bosque, *Facial Recognition Bias Frustrates Black Asylum Applicants to US, Advocates Say*, The Guardian (Feb. 8, 2023), https://www.theguardian.com/us-news/2023/feb/08/us-immigration-cbp-one-app-facial-recognition-bias.

[101] *See* Nat'l Acad. of Scis., *Facial Recognition Technology: Current Capabilities, Future Prospects, & Governance* 57–59 (2024), https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-and-governance

[102] *Id*. at 50.

DHS purports to allow U.S. citizens "the right to opt-out and ensures alternative processing is available," for non-law enforcement uses of FRT such as border processing,[103] but there are significant questions about whether this policy is being observed in practice. For example, U.S. citizens have reported being denied the ability to opt out of facial recognition scanning at the border.[104]

DHS policy also provides that, for non-law enforcement uses, "FR technology for verification may not be the sole basis for denial for an administrative determination" and "alternative processing [must be] available to resolve match or no match outcomes."[105] These are important protections, and it is critical that DHS employees are rigorously trained to understand how to adhere to these requirements. But there is a serious risk that even with training, the cognitive bias toward trusting machine outputs will predispose DHS employees toward overly deferring to FRT outputs, thus subjecting travelers to lengthy delays or Kafkaesque ordeals as they seek to prove their identity. DHS must collect detailed data about how non-match results are handled, and must ensure that "alternative processing" is not any more burdensome than processing would be in the absence of FRT. DHS should also be required to collect and publish data on the failure rate of FRT verification systems by demographic categories. If FRT systems are producing false no-match results at higher rates for travelers of color, women, or members of other groups, use of those FRT systems should be immediately ended. Otherwise, DHS will end up subjecting travelers in these groups to more burdensome ordeals as they seek to enter the country or obtain other administrative determinations.

III. Face Recognition Technology in Housing

Face recognition technology is being used in both public and private housing to control who has entry access to buildings and communities,[106] and to surveil residents and guests.[107] These uses of FRT raise serious concerns about privacy harms and racial discrimination.

Use of face recognition technology in housing communities without the consent or knowledge of residents can result in residents' unwitting inclusion in a biometric database, and in

---

[103] Dep't of Homeland Sec., Directive No. 026-11, *Use of Face Recognition and Face Capture Technologies* 6 (Sept. 11, 2023), https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_026-11-use-face-recognition-face-capture-technologies.pdf.

[104] *See, e.g.*, Shaw Drake, *A Border Officer Told Me I Couldn't Opt Out of the Face Recognition Scan. They Were Wrong.*, ACLU (Dec. 5, 2019), https://www.aclu.org/news/immigrants-rights/a-border-officer-told-me-i-couldnt-opt-out-of-the-face-recognition-scan-they-were-wrong.

[105] Dep't of Homeland Sec., Directive No. 026-11, *Use of Face Recognition and Face Capture Technologies* 6 (Sept. 11, 2023), https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_026-11-use-face-recognition-face-capture-technologies.pdf.

[106] *See, e.g.*, Rebecca Heilweil, *Tenants Sounded the Alarm on Facial Recognition in their Buildings. Lawmakers are Listening*, Vox (Dec. 26, 2019), https://www.vox.com/recode/2019/12/26/21028494/facial-recognition-biometrics-public-housing-privacy-concerns.

[107] Douglas MacMillan, *Eyes on the Poor: Cameras, Facial Recognition Watch Over Public Housing*, Wash. Post (May 16, 2023), https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/.

the automated monitoring of the comings and goings of residents and their guests. Privacy harms may also arise when housing authorities make the system's data available to law enforcement or other third parties.[108] This practice particularly subjects individuals who cannot afford alternative housing options to surveillance.

A major investigation by the Washington Post last year identified public housing authorities across the country that have used HUD grant funding to purchase and operate surveillance camera systems that include face recognition capability.[109] In addition to the chilling effect of such surveillance on residents' ability to go about their lives without being pervasively monitored, the Post's investigation demonstrated that face recognition and other video analytics technology was resulting in draconian enforcement against tenants for alleged violations of minor housing rules. Such surveillance-driven enforcement can cause several harms. As in the policing context, when FRT misidentifies people, it can lead to enforcement action being taken against the wrong person. And even when the technology "works," it can generate overenforcement of technical rules in a way that penalizes residents for trivial infractions that would previously have gone unnoticed.

Biometric entry systems, including FRT cameras that control access to residential buildings, can also cause harms. For one, discriminatory inaccuracies in face recognition technology can refuse entry to residents of color or force them to try multiple times to access their residences when initial face scans fail. Additionally, buildings that require face scans or other biometric authentication, without providing an alternative means of entry (like a key or keycard) can frustrate residents' ability to rely on friends or family to help with necessities of life—whether taking care of a pet during a resident's unexpected absence or bringing groceries when a resident is sick. Additionally, many systems that offer the technology for entry access also double as general surveillance systems, which raise the privacy and discrimination harms discussed above. Tenants have voiced concerns when housing authorities attempted to install security surveillance that uses face recognition technology in both public and private housing.[110]

Presumably in response to such concerns, last year HUD barred use of Capital Fund Emergency Safety and Security Grants to purchase "[a]utomated surveillance and facial recognition technology."[111] That was an important step, but it did not restrict use of already-

[108] *See* Letter from Sen. Ron Wyden et al, to Sec. Ben Carson, U.S. Dep't of Hous. & Urb. Dev. (Dec. 18, 2019), https://www.wyden.senate.gov/imo/media/doc/121819%20Wyden-led%20letter%20to%20HUD%20RE%20facial%20recognition%20technologies.pdf.

[109] Douglas MacMillan, *Eyes on the Poor: Cameras, Facial Recognition Watch Over Public Housing*, Wash. Post (May 16, 2023), https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/.

[110] *See, e.g.*, Tanvi Misra, *The Tenants Fighting Back Against Facial Recognition Technology*, Bloomberg CityLab (May 7, 2019), https://www.bloomberg.com/news/articles/2019-05-07/when-facial-recognition-tech-comes-to-housing; Lola Fadulu, *Facial Recognition Technology in Public Housing Prompts Backlash*, N.Y. Times (Sept 24, 2019), https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html.

[111] U.S. Dep't of Hous. & Urb. Dev., Notice PIH 2023-10, *Emergency Safety and Security Grants Annual Funding Notification and Application Process* 6 (Apr. 21, 2023), https://www.hud.gov/sites/dfiles/PIH/documents/2023PIH10.pdf.

purchased FRT systems by housing authorities. HUD should more broadly and strictly restrict use of FRT in public housing.

* * *

The ACLU appreciates the opportunity to provide input on this important topic. If you have any questions about these comments, please do not hesitate to contact Senior Policy Counsel Kia Hamadanchy and Speech, Privacy, and Technology Project Deputy Director Nathan Freed Wessler at KHamadanchy@aclu.org and nwessler@aclu.org.

Sincerely,

Nathan Freed Wessler
Deputy Director, Speech, Privacy, & Technology Project

Kia Hamadanchy,
Senior Policy Counsel