ACLU
AMERICAN CIVIL LIBERTIES UNION

January 19, 2024

Submitted via e-mail

RE: 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))

The American Civil Liberties Union (ACLU) submits this comment to inform the interagency process required by Section 13(e) of Executive Order 14074 (Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety). As requested in the guidance document circulated on behalf of DOJ and DHS, this comment addresses civil rights and civil liberties concerns with law enforcement use of: face recognition technology (Part I); fingerprint and iris biometric technologies (Part II); DNA technologies (Part III); and predictive policing algorithms (Part IV).

As explained in detail below, law enforcement use of these biometric and predictive technologies 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 violating Americans' Fourth Amendment right to privacy. Although unique concerns exist regarding each technology, they also share broader problems. These include a pervasive lack of transparency in law enforcement use of these systems that violates the due process rights of people accused of crimes and frustrates the ability of courts, lawmakers, and the public to understand the technologies and implement effective protections against abuse.

DOJ's and DHS's policies should be strong and broadly scoped. As explained below, for some technologies, there is no safe use and law enforcement access should be banned. For other technologies, robust civil rights protections should govern law enforcement use, and DOJ and DHS should be clear that their policies encompass "mixed" or "dual" uses that may also implicate homeland security, national security, or immigration. As described below, the dangers associated with these technologies are wide-ranging, persistent, and extend to overlapping agency functions. As we have seen before, the adoption of carve-outs for vaguely defined categories like "national security" only creates incentives for agencies to relabel their activities to avoid complying with bedrock rules. DOJ and DHS should ensure essential protections apply to any law enforcement use of these technologies.

I. Face Recognition Technology

As the ACLU has previously explained,[1] law enforcement use of face recognition technology (FRT) 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

[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.

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—every publicly known wrongful arrest due to police reliance on an incorrect FRT result has been of a Black person. 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,[3] 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.

[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.

[3] 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.

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."[4] It will frequently produce possible matches that are incorrect.[5] 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). Most disturbingly, the technology continues to have markedly higher false match rates for people of color and women than for white people and men.

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.[6] 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.[7]

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.[8] It has become clear that ensuring more diverse representation in training datasets will not eliminate

[4] 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/.

[5] 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.

[6] 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/.

[7] 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.

[8] 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.

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 in underexposed images of darker-skinned people,[9] which reduces FRT accuracy when attempting to process and match those images.[10]

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.[11] 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."[12] In Detroit, all 129 FRT searches in 2020 were conducted on images of Black people.[13]

In light of these dynamics, it is unsurprising that 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. Concerns 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.[14] Federal agencies should implement equivalent bans.

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

[9] *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.

[10] *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.

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

[12] 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.

[13] Detroit Police Department, *Annual Report on Facial Recognition, 2020* (Jan. 27, 2021), https://detroitmi.gov/sites/detroitmi.localhost/files/2021-02/Facial%20Recognition%202020%20Annual%20Report.pdf.

[14] *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.").

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.

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.[15] 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. 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[16]—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,[17] that human review process is prone to error.[18]

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.[19] 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

[15] 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/.

[16] *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).

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

[18] 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.").

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

renderings of a witness's recollection of a face.[20] Even after this practice was widely discredited,[21] at least one FRT company, Cognitec, continues to encourage police to engage in it.[22]

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).[23] 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.[24] 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 who is a true match to the probe photo, every result returned by the search will necessarily be a false match.[25] 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

[20] *Id.*

[21] *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.").

[22] Cognitec, *Law Enforcement*, https://www.cognitec.com/law-enforcement.html (last visited Jan. 18, 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.").

[23] 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.").

[24] *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.

[25] *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.

similar-looking people occurring in a larger population.[26] 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.[27] 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.

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 alike. 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.[28] 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.[29]

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.[30] A focus on these kinds of performance metrics also risks overstating what was

[26] *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.

[27] *See,* 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).

[28] 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).

[29] *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").

[30] 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.,

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.[31] 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;[32] and the cognitive biases of those human examiners.[33] Although some FRT accuracy tests assess some variability in probe

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.

[31] *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).

[32] *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-23-105607.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).

[33] *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.").

image quality[34] 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 six cases of FRT-based wrongful arrests publicly known to date.

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,[35] in the documentation from companies that develop and sell FRT,[36] in law enforcement agency policies,[37] including the DOJ

[34] *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.

[35] 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").

[36] *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").

[37] *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

Bureau of Justice Assistance's 2017 FRT policy development template[38] and DHS's recently issued FRT policy,[39] and on face recognition search result forms provided to investigating officers.[40] 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.[41] In a New Jersey case, for example, a detective obtained an arrest warrant based 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."[42] 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."[43] Mr. Parks was subsequently arrested and jailed for 10 days for a crime he did not commit.[44]

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

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).

[38] 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.

[39] 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.

[40] *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.

[41] 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.

[42] 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.

[43] *Id.* at 290.

[44] 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.

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."[45] That investigation led to the wrongful arrest of Randal Quran Reid, a Georgia resident who had never even been to Louisiana.[46] 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."[47] 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."[48] Even more, the FRT-generated image in a photo array is likely to appear more similar 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.[49]

This problem contributed to all three known FRT-derived wrongful arrests by the Detroit Police Department.[50] 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

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

[46] 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.

[47] 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/.

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

[49] *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).

[50] *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).

(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.

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.[51] 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 is not in fact the suspect.[52] He announced an intent to implement policy changes to prevent similar failures in future investigations.[53]

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."[54] Because FRT searches lack reliability, FRT results can never constitute such "evidence-based grounds" for conducting a photo lineup.

[51] 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/.

[52] 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.

[53] *Id.*

[54] 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.

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 whether there is probable cause.[55] 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.[56] 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.[57]

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

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

[56] 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.

[57] 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.

scan of a fake driver's license,[58] 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."[59] The warrant application also misrepresented the FRT result as a "high profile comparison" rather than what it really was: a low-reliability investigative lead.[60] 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).[61] 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 unjustified probable cause findings.

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.[62] Information is material if it tends to undermine confidence in the result of the criminal case.[63] This disclosure obligation attaches whether or not the defense has requested it.[64]

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*;[65] 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

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

[59] *Id.* at 380.

[60] *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.

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

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

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

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

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

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."[66] But information about FRT use is very much material, including because it can negate guilt by showing how an initial incorrect FRT result may have tainted later investigative steps.[67] 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.[68] 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.[69] 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

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

[67] *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/.

[68] *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).

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

by the analyst who ran the search, and the qualification of the analyst who ran the search.[70] 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."[71]

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.

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.[72] 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.[73]

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. Deployment of FRT for video tracking and surveillance would pose a catastrophic threat to privacy, free speech, and freedom of

[70] *Id. at* 558.

[71] *Id.*

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

[73] *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.

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.[74] The federal government has heavily invested in improving the performance of FRT to analyze video, including for applications like public surveillance cameras and drones.[75] 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."[76] The program, called "Janus," aimed to enable face recognition surveillance of "millions of subjects" and support "partial, incomplete, and occluded views" of faces.[77] 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.

Although tests have shown high inaccuracy rates for use of FRT on surveillance video,[78] development and deployment of an even moderately accurate system would raise acute 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 more persons appearing in video recordings over time. This capability, which has already been used to devastating effect by some foreign governments,[79] 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

[74] 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.

[75] 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/.

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

[77] *Id*.

[78] *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.

[79] *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/.

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."[80] The Supreme Court has made clear that we do not "surrender all Fourth Amendment protection by venturing into the public sphere."[81] 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.[82] 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.[83] 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.[84] Federal agencies should immediately ban use of FRT on live or recorded video.

II. DNA Technologies

DNA collection and analysis has been part of criminal investigations for decades, and concerns around its use are well known.[85] The use of newer DNA technologies, such as familial searching and probabilistic genotyping software, raises some of the same issues, including concerns related to privacy and retention of DNA samples, while also making increasingly clear that those concerns are not hypothetical. These technologies also raise new concerns, including the lack of transparency around the functioning of proprietary or black-box algorithms.

1. DNA technology's privacy risks are high because of DNA's uniquely sensitive and personal nature.

Strict protections surrounding DNA technologies are necessary in part because analysis of DNA samples can reveal a great deal of sensitive information, such as medical conditions, disease

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

[81] *Id.* at 2217.

[82] *Id.* at 2212.

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

[84] *See, e.g.*, Mont. Code Ann. § 44-15-104; Mass. Gen. Laws. Ann. ch. 6, § 220(a); 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).

[85] *See, e.g.*, Matthew Shaer, *The False Promise of DNA Testing*, The Atlantic (June 2016), https://www.theatlantic.com/magazine/archive/2016/06/a-reasonable-doubt/480747; Naomi Elster, *How Forensic DNA Evidence Can Lead to Wrongful Convictions*, JSTOR Daily (Dec. 6, 2017), https://daily.jstor.org/forensic-dna-evidence-can-lead-wrongful-convictions.

predisposition, physical attributes, biological family relationships, and ancestry—including information people may not even know about themselves. This list will only expand as technology continues to evolve.

Traditionally, law enforcement use of DNA in investigations was limited to creating and comparing STR profiles. STR profiles calculate how many times "short, tandem, repeat" (STR) sequences occur at designated locations (called "loci") on the genome.[86] Privacy concerns with DNA analysis in criminal investigations have sometimes been met by arguments that STR profiles are akin to fingerprints, and can only be used to identify a person, not to learn private or sensitive information about them.[87] However, law enforcement practices themselves show that STR profiles reveal more than identity.

For example, investigators use STR profiles to conduct familial searches, which are designed to reveal information beyond the individual's identity, and thus unlock a slew of new privacy concerns. Whereas traditional DNA technology works by identifying an individual based on exact DNA profile matches, familial searches look for *partial* matches—the theory is that these partial matches are likely the individual's relatives, and provide the police an investigative lead that will guide them to the correct person.[88] Familial searching is thus "qualitatively different from more established DNA techniques: it is inherently less precise; it implicates people in criminal activity because of who their family is and the size of that family, rather than what they have done; and it focuses investigative attention on people who are known to be innocent."[89] This presents troubling constitutional problems. Traditional DNA matches are designed to identify only the person who might be guilty of the crime; familial searches, by definition, identify those who are *not* guilty of the crime.

Moreover, although the loci used in standard STR analysis (such as for the FBI's CODIS system) are sometimes misleadingly referred to as "junk DNA,"[90] recent studies have made clear that these regions of the genome can reveal sensitive information. Researchers in a 2016 study were able to identify information about ancestry from STR profiles, which could in turn be used to approximate a person's physical appearance.[91] A 2020 survey of existing research found that

[86] *See* Erin Murphy, *Inside the Cell: The Dark Side of Forensic DNA* 7–8 (2015).

[87] *See, e.g.*, *Maryland v. King*, 569 U.S. 435, 451–52 (2013).

[88] Peter Bibring, *"Grim Sleeper" Case Doesn't Justify Expanding the Reach of DNA Databases*, ACLU (July 15, 2010), https://www.aclu.org/news/national-security/grim-sleeper-case-doesnt-justify-expanding-reach-dna-databases.

[89] *Utilizing DNA Technology to Solve Cold Cases Act of 2011: Hearing on H.R. 3361 Before the H. Judiciary Subcomm. On Crime, Terrorism, & Homeland Sec.*, 112th Cong. 2 (2012) (statement of Michael T. Risher, Staff Attorney, ACLU of Northern California), *available at* https://www.aclunc.org/sites/default/files/asset_upload_file678_11986.pdf.

[90] *See* Jennifer K. Wagner, Letter to the Editor, *Out with the 'Junk DNA' Phrase*, 58 J. Forensic Sci. 292, 292 (2012).

[91] Bridget Algee-Hewitt et al., *Individual Identifiability Predicts Population Identifiability in Forensic Microsatellite Markers*, 26 Current Biology 935, 939 (2016), *available at* https://doi.org/10.1016/j.cub.2016.01.065.

57 studies have linked forensic STRs with a total of 50 unique traits, including schizophrenia, Parkinson's disease, and Down syndrome.[92]

Additionally, law enforcement has started using even more revealing single nucleotide polymorphism (SNP) profiles in some investigations. SNP profiles involve analysis of many thousands of locations on the genome, and focus on "the places in the genome where people differ" the most.[93] Genetics researchers, private labs, and companies like 23andMe and Ancestry.com use SNP profiles to "help predict an individual's response to certain drugs, susceptibility to environmental factors such as toxins, and risk of developing diseases."[94] Law enforcement agencies have started using SNP profiles to conduct forensic genetic genealogy (FGG) investigations, opening up a vast array of sensitive genetic information to government scrutiny.[95] Indeed, in some investigations police have used SNP profiles to try to generate information beyond even familial relationships, such as predicting phenotype and attempting to reconstruct facial attributes.[96]

Even greater privacy concerns loom as whole-genome sequencing rapidly becomes cheaper and faster. With whole-genome sequencing, the government could gain access to the full array of sensitive and private information contained in our genetic code, raising extraordinary privacy concerns. Even in contexts where use of more limited STR profiles is permitted, use of SNP profiles and whole-genome sequences should be barred.

As the Supreme Court has recognized, collection and retention of biological samples raises grave privacy concerns because of all the information these samples can reveal. Nearly 35 years ago, the Supreme Court recognized that "chemical analysis" of biological samples "can reveal a host of private medical facts."[97] More recently, it highlighted the concern with regard to DNA in particular, noting that even when it is "obtained . . . only for identification purposes, the process

[92] Nicole Wyner et al., *Forensic Autosomal Short Tandem Repeats and Their Potential Association with Phenotype*, 11 Frontiers in Genetics 1 (Aug. 6, 2020), https://www.frontiersin.org/articles/10.3389/fgene.2020.00884/full.

[93] *Single Nucleotide Polymorphisms (SNPs)*, Nat'l Human Genome Rsch. Inst., https://www.genome.gov/genetics-glossary/Single-Nucleotide-Polymorphisms (last visited Jan. 18, 2024).

[94] *What Are Single Nucleotide Polymorphisms (SNPs)?*, Nat'l Libr. Med., https://medlineplus.gov/genetics/understanding/genomicresearch/snp (last visited Jan. 18, 2024).

[95] In an FGG investigation, law enforcement will generate a SNP profile from DNA evidence collected at a crime scene, upload that profile to a vast genetic database, attempt to identify a partial match belonging to a distant relative of the crime-scene contributor, and scour public records to create detailed family histories in order to identify some set of biological suspects. *See, e.g.*, Rafil Kroll-Zaidi, *Your DNA Test Could Send a Relative to Jail*, N.Y. Times (Jan. 3, 2022), https://www.nytimes.com/2021/12/27/magazine/dna-test-crime-identification- genome.html.

[96] *See, e.g.*, Appellant's Brief at 7, *State v. Carbo*, No. A22-1823 (Minn. May 30, 2023) ("By analyzing that SNP profile, [law enforcement's contract laboratory] Parabon established that the person who left the DNA was a man of 83 percent Northern European ancestry who also had a 'great grandparent of Southern European ancestry.' Parabon determined the man almost certainly had brown eyes and dark hair, and very likely fair skin and few freckles. Parabon used the SNP profile to develop an image of what the man likely looked like at 25 years old." (citations omitted)).

[97] *Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S. 602, 616 (1989).

put[s] into the possession of law enforcement authorities a sample from which a wealth of additional, highly personal information could . . . be obtained."[98]

In light of these privacy concerns, the following protections are needed:

- At a minimum, collection of reference samples must be limited to those individuals who are charged with a crime of violence (*i.e.*, murder, rape, first-degree assault, kidnapping, arson, sexual assault, or other comparably serious offenses) or burglary.

- Collection and analysis of DNA must require a warrant. If the collection is connected to an arrest, the DNA sample should not be processed or the resulting profile placed in a database before a judicial officer ensures that there is probable cause to arrest the individual on a qualifying serious offense. If the arrest is unsupported by probable cause, the DNA sample should be immediately destroyed and the profile removed from any database in which it was uploaded. Otherwise, a search warrant must be required. To be clear, this warrant requirement should apply not only to reference samples taken directly from a suspect, but also to so-called "abandoned" DNA—more accurately termed unavoidably shed DNA—that is, the genetic material often harvested by law enforcement from items a person has touched, such as used drinking straws, water bottles, or facial tissues.

- In criminal investigations, DNA collection and processing, when permitted, should be available only for the specific purpose of identifying an individual. Any collection, analysis, and storage should therefore be in a form that minimizes retention of and access to extraneous information beyond identity. For example, government creation and retention of SNP profiles, as well as testing of the DNA sample or profile in a government database for familial matches, phenotyping, or medical predispositions, should be prohibited. Permissible uses and analysis must remain limited to identifying the contributor of a DNA sample even as technological advances enable more intrusive and revealing testing. Such limitations are essential because the government's retention of an individual's DNA sample leaves all such information potentially at its disposal.

- Database procedures must also assure that the use of the DNA sample is limited to its intended purpose. Access to any stored information should be limited to specifically designated law enforcement officials for identification purposes only. Any access to the database should be logged. Access should also be granted to defendants to defend against prosecution or collaterally attack conviction.

- Provision must be made for the destruction of the DNA sample and any record of information it contains once the purpose for the taking has been served (including the exhaustion of any appeals process), or if the criteria that justified the taking of the sample no longer apply. For example, the sample and record must be destroyed if the criminal proceeding against the individual does not result in conviction.

[98] *Birchfield v. North Dakota*, 579 U.S. 438, 463 (2016) (citing *Maryland v. King*, 569 U.S. 435, 462 (2013)).

> Maximum retention should not exceed 30 years. Finally, individuals should be guaranteed a right of access to their own DNA sample and any analysis or information record.

2. Transparency around DNA technology is necessary to ensure justice and accountability.

Transparency around DNA technology—both the technology itself and the use of it—is imperative to keep police, investigators, and other government actors accountable, and to ensure that the constitutional rights of people accused of crimes are protected. This includes probabilistic genotyping technology, which relies on complicated algorithms with tens of thousands of lines of code that may contain human errors or bias,[99] as well as any future DNA technologies the government will rely on in prosecutions. Criminal defendants have a constitutional right to access information about these programs; without it, they do not have a full and fair opportunity to mount a defense. Further, when probabilistic genotyping algorithms are used in criminal prosecutions, information about them must be disclosed not only to the defense, but also to the public; without public access, errors discovered in one case, which almost certainly impact other cases, may not be corrected or addressed elsewhere.

Due process requires that defendants have access to the DNA evidence used against them in criminal prosecutions. Probabilistic genotyping programs purportedly interpret results from complicated DNA mixture evidence that often includes DNA samples that are tiny, degraded, or mixed with genetic material from multiple other parties—specimens that would be impossible to use in traditional DNA forensics.[100] These programs then use complicated algorithms to generate potential matches.[101] Though some open-source programs exist, the programs typically relied on by U.S. forensic laboratories, STRmix and TrueAllele, do not share, even with the defense in criminal prosecutions, their algorithms, source code, parameters, population baselines, or other information about the inner workings of their programs, either at all or in ways that would enable independent testing and evaluation.[102] Nor do prosecutors who rely on these programs, instead claiming that the algorithms are proprietary and protected by trade secrecy. In some cases, this means defendants do not even know which program—including the specific version—was used to identify them.

These programs and algorithms are material to the prosecution and therefore must be disclosed to the defense. Moreover, they are designed, coded, and built by humans, and are thus subject to human error, bias, and bugs. For example, based on a probabilistic genotyping result,

[99] *See* Br. of American Civil Liberties Union and American Civil Liberties Union of Southern Cal. as Amici Curiae Supporting Defendant–Appellant Seeking Reversal at 10–19, *People v. Johnson*, No. F071640, 2019 WL 3025299 (Cal. Ct. App. July 11, 2019).

[100] *See* Br. of American Civil Liberties Union and American Civil Liberties Union of San Diego and Imperial Counties as Amici Curiae Supporting Real Party in Interest Seeking Dismissal at 13, *People v. Super. Ct.* (*Dominguez*), 239 Cal. Rptr.3d 71 (2018).

[101] *See id.*

[102] *See* Michael D. Edge & Jeanna Neefe Matthews, *Open Practices in Our Science and Our Courtrooms*, 38 Trends in Genetics 112, 113-115 (2022).

Billy Ray Johnson was sentenced to life in prison without the possibility of parole for a series of offenses he says he did not commit. The creator of the probabilistic genotyping company in that case, TrueAllele, had previously acknowledged that probabilistic genotyping programs "give different answers based on how an analyst sets their input parameters."[103] During Mr. Johnson's case, the TrueAllele creator and a separate analyst running the same program obtained wildly different results, demonstrating the imprecise nature and possible errors within the program.[104] Yet Mr. Johnson was still denied access to the underlying information needed to defend himself. And Mr. Johnson is not alone.[105]

Criminal defendants are constitutionally entitled to know how these programs work. The Sixth Amendment's Confrontation Clause grants defendants the right to "be confronted with the witnesses against him."[106] The Constitution's Fourteenth Amendment and Sixth Amendment also grant defendants the right to a fundamentally fair trial and the right to a meaningful opportunity to present a complete defense.[107] Without access to source code, training data, operation manuals, validation studies, configuration choices, population baselines, and other information about the program and how it was used, defendants cannot contest any problems of accuracy, bias, or error, and thus cannot build any sort of meaningful defense or exercise their Confrontation Clause rights.

This matters in part because, with access, errors may be revealed. For example, in New York, after a trial court ordered one of TrueAllele's competitors to release its source code, an expert witness for the defense discovered that "the program dropped valuable data from its calculations, in ways that users wouldn't necessarily be aware of, but that could unpredictably affect the likelihood assigned to the defendant's DNA being in the mixture."[108] In response, the prosecution withdrew the DNA evidence against the defendant.[109] "After denials in many cases, three judges have recently granted code review permission under protective orders."[110] In one of

[103] Letter from Mark W. Perlin, Chief Sci. and Exec. Officer, Cybergenetics, to Jerry D. Varnell, U.S. Dep't of Justice, Procurement Section, at 3 (Apr. 1, 2015), https://www.cybgen.com/information/newsroom/2015/may/Letter_to_FBI.pdf.

[104] Br. of American Civil Liberties Union and American Civil Liberties Union of Southern California as Amici Curiae Supporting Defendant-Appellant Seeking Reversal at 14–18, *People v. Johnson*, No. F071640, 2019 WL 3025299 (Cal. Ct. App. July 11, 2019).

[105] *See, e.g.*, Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System,* 70 Stan. L. Rev. 1343, 1354, 1346, 1372 (2018) (describing how requests to review TrueAllele's source code have been denied on the basis that it allegedly contains trade secrets).

[106] U.S. Const. amend. VI.

[107] "Whether rooted directly in the Due Process Clause of the Fourteenth Amendment or in the Compulsory Process or Confrontation Clauses of the Sixth Amendment, the Constitution guarantees criminal defendants a meaningful opportunity to present a complete defense." *Holmes v. South Carolina*, 547 U.S. 319 (2006) (quoting *Crane v. Kentucky*, 476 U.S. 683, 690 (1986)) (internal quotation marks omitted).

[108] Lauren Kirchner, *Traces of Crime: How New York's DNA Techniques Became Tainted*, N.Y. Times (Sept. 4, 2017), http://nyti.ms/2vJwxze.

[109] *Id.*

[110] *See* Michael D. Edge & Jeanna Neefe Matthews, *Open Practices in Our Science and Our Courtrooms*, 38 Trends in Genetics 112, 113–15 (2022).

those cases, "prosecutors chose to withdraw their TrueAllele evidence rather than undergo review."[111] Such access should be guaranteed, and it shouldn't require a court order.

In addition, access to information about these probabilistic genotyping tools shouldn't be constrained to a single case or defendant—the public should also have full access. When discovery about these tools is allowed, usually in the context of criminal prosecutions, the information is usually subject to a protective order. This means that defendants in other cases where the same programs were used will not learn of any defects that are discovered. And it also means that the programs—and defendants and other members of the public—will not benefit from broader public vetting, testing, and validation. For example, genetic biologists, computer programmers, scientists, researchers, and other experts on these technologies who could provide a meaningful review of these probabilistic genotyping tools are effectively shut out, cutting off any chance of public accountability and fairness.

Increasingly, cities and states are contracting with private providers of probabilistic genotyping technologies for use in criminal cases. If they decide to procure those technologies, at that moment, they have an opportunity to ensure that the constitutional rights of criminal defendants and the public are vindicated—and that shoddy technologies aren't used on their residents in the first place. At the acquisition and procurement stage, the government should require DNA technology companies to provide the public access to all of the information necessary for a meaningful review and accounting of the technology and its use. Only then can the constitutional mandate for access and transparency be satisfied.

III. Fingerprinting and Iris Technology

1. Extracting and analyzing fingerprints from individuals outside the jail booking context requires a warrant.

Although collection and analysis of fingerprints is a longstanding practice of law enforcement in certain contexts, newer fingerprinting technologies raise serious concerns about the possibility of low-cost, widespread collection and exploitation of people's biometric identifiers, and trigger a need for strong protections against abuse.[112]

When a government agent takes a person's fingerprints, that is a Fourth Amendment search. This is for two reasons. First, "[w]hen the Government obtains information by physically intruding on [a constitutionally protected area], a 'search' within the original meaning of the Fourth

[111] *Id.*

[112] This Comment focuses on Fourth Amendment privacy concerns with deployment of fingerprint technologies, but the ACLU notes its concern with inaccuracy problems in fingerprinting analysis. Fingerprint comparison is not a precise science, and there are documented cases in which incorrect fingerprint matches have led to wrongful detention, arrests, convictions, and imprisonment. *See* Simon A. Cole, *More than Zero: Accounting for Error in Latent Fingerprint Identification*, 95 J. Crim. L. & Criminology 985 (2005); Brief of Innocence Network as Amicus Curiae, *Johnson v. VanderKooi*, 983 N.W.2d 779 (Mich. 2022) (No. 160958).

Amendment has undoubtedly occurred."[113] When police take a person's fingerprint by applying their finger to an inkpad and print card, or by pressing their finger on a digital fingerprint terminal, the "fingerprinting . . . constitute[s] a physical trespass onto a person's body, a constitutionally protected area."[114] Because "the act of fingerprinting is done for the very purpose of obtaining information," it "constitutes a search under the Fourth Amendment."[115]

Second, fingerprinting is a search because people have a reasonable expectation of privacy against the nonconsensual taking of their immutable biometric identifiers, including fingerprints. It is well established that government collection of material or information from a person's body constitutes a search.[116] And there is an additional expectation of privacy in the biometric information extracted from the fingerprint. That information is both virtually unique to the individual and quite sensitive. Fingerprints not only reveal identity, but also are increasingly "used for many things beyond individual identification. People regularly use such biometric markers as a security measure for accessing electronic devices[,] . . . secured digital spaces[,] . . . or restricted places."[117] And researchers have begun to discover that fingerprints can reveal sensitive information beyond identity, including health information.[118] Nor are people's fingerprints exposed to the public in a way that vitiates this privacy expectation: "Without specialized training or advanced analytical software, the details of one's fingerprint structure are neither readily observable nor even very useful."[119] Thus, courts have described fingerprints as "private information," the nonconsensual taking of which is "an invasion of [one's] private domain, much like an act of trespass would be."[120]

When courts have permitted warrantless collection and analysis of fingerprints in defined contexts, such as fingerprinting arrestees as part of the jail booking process, it has been because a recognized exception to the warrant requirement applies.[121] And fingerprinting has rarely strayed beyond such circumstances because of the traditional unwieldiness of the procedure. For example,

[113] *Florida v Jardines*, 569 U.S. 1, 5 (2013) (quoting *United States v. Jones*, 565 U.S. 400, 406 n.3 (2012)) (internal quotation marks omitted).

[114] *Johnson v. VanderKooi*, 983 N.W.2d 779, 786 (Mich. 2022).

[115] *Id.* at 786–87.

[116] *See, e.g.*, *Birchfield v. North Dakota*, 579 U.S. 438, 455 (2016) (administration of a breath test); *Maryland v. King*, 569 U.S. 435, 463–64 (2013) (collection of saliva using minimally intrusive buccal swab); *Cupp v. Murphy*, 412 U.S. 291 (1973) (fingernail scrapings). "[W]hile nothing more than oils and dirt are being physically removed from a person's body when fingerprints are copied, the procedure itself is no less intrusive than [these contexts]." *Johnson v. VanderKooi*, 983 N.W.2d 779, 797 (Mich. 2022) (Welch, J., concurring).

[117] *Johnson*, 983 N.W.2d at 796 (Welch, J., concurring).

[118] *See, e.g.*, Fabiane Pertille et al., *Fingerprint Patterns in Women with Type 2 Diabetes Mellitus: Computerized Dermatoglyphic Analysis*, 45 Acta Scientiarum (2022), https://www.researchgate.net/publication/373562924_Fingerprint_Patterns_in_Women_with_Type_2_Diabetes_Mellitus_Computerized_Dermatoglyphic_Analysis.

[119] *Johnson*, 983 N.W.2d at 796 (Welch, J., concurring).

[120] *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 624 (7th Cir. 2020).

[121] *See Maryland v. King*, 569 U.S. 435, 441 (2013).

fingerprinting people during brief investigative stops on the street (often known as *Terry* stops) is virtually unheard of, in part because collecting fingerprints using traditional means, with inkpads and cardstock, is time consuming, messy, and delicate work. Perhaps the only American law enforcement agency to have implemented such a practice at scale is the Grand Rapids, Michigan, police department. But in a challenge brought by the ACLU of Michigan and the national ACLU, its policy was ruled a Fourth Amendment violation by a unanimous Michigan Supreme Court.[122]

The proliferation of mobile digital fingerprint terminals lowers the cost and difficulty of taking people's fingerprints outside the controlled environment of a police station, however, and raises the specter of police attempts to collect people's fingerprints as they go about their daily lives. Some mobile fingerprinting devices are simple fingerprint readers that plug into a smartphone or tablet via cable.[123] Others are small handheld devices that can include several additional features. These devices are marketed to law enforcement as low-cost, convenient options for officers out on patrol, enabling "quick, accurate biometric finger identification of suspects at the scene."[124] Some, such as M2Sys's RapidCheck device, are equipped with cameras, barcode scanners, Bluetooth, NFC, and RFID.[125] Others, such as Feitian Technology's handheld biometrics device, include features such as a breathalyzer and narcotics detector, and can even issue tickets.[126] Police may also soon be able to employ contactless fingerprint applications on their handheld smartphones. One fingerprinting technology company, Tech5, was recently granted a patent for contactless fingerprinting detection and identification software capable of running on standard smartphones, targeted towards law enforcement.[127]

Further technological advances raise even more sobering concerns. In 2015, the FBI invested $500,000 in research "to collect fingerprints from peoples' Facebook, Twitter and other social media posts" by analyzing photos that include people's fingers and hands.[128] Nobody expects that a casual snapshot posted online will expose their immutable biometric fingerprints to extraction. Because of the expectation of privacy in this biometric information, even the "nontouching/nontrespassory harvesting of biometric information for investigative purposes"

[122] *Johnson v. Vanderkooi*, 983 N.W.2d 779 (Mich. 2022).

[123] *See, e.g.*, *HID® NOMAD™ 30 Pocket Reader*, HID, https://www.hidglobal.com/products/nomad-30-pocket-readers (last visited Jan. 18, 2024).

[124] *Ident 2.0*, IDEMIA, https://www.idemia.com/ident-20 (last visited Jan. 18, 2024).

[125] *See, e.g.*, *RapidCheck™ Mobile Fingerprint Scanner for Handheld Use*, M2SYS, https://www.m2sys.com/rapidcheck-mobile-fingerprint-scanner (last visited Jan. 18, 2024).

[126] *See* Tyler Choi, *Feitian Unveils Portfolio of Handheld Android Biometric Devices*, BiometricUpdate.com (May 20, 2022), https://www.biometricupdate.com/202205/feitian-unveils-portfolio-of-handheld-android-biometric-devices.

[127] *See* Chris Burt, *Tech5 Contactless Mobile Fingerprint Biometrics Capture System Patented*, BiometricUpdate.com (Aug. 18, 2023), https://www.biometricupdate.com/202308/tech5-contactless-mobile-fingerprint-biometrics-capture-system-patented.

[128] Thomas Brewster, *Inside America's Secretive $2 Billion Research Hub*, Forbes (July 13, 2020), https://www.forbes.com/sites/thomasbrewster/2020/07/13/inside-americas-secretive-2-billion-research-hub-collecting-fingerprints-from-facebook-hacking-smartwatches-and-fighting-covid-19.

raises similar Fourth Amendment concerns to more traditional fingerprint extraction through physical touch.[129]

In light of these technological advances that make collection of biometric information "remarkably easy, cheap, and efficient compared to traditional investigative tools,"[130] strong protections are needed. It is critical that federal policy require officers to obtain a search warrant before collecting or analyzing fingerprints from people not under arrest unless some other recognized exception to the warrant requirement (such as exigent circumstances) applies. This warrant requirement must apply regardless whether the fingerprint is taken through physical contact with the hand, or through remote analysis of video or photographs, as the intrusion on privacy in either scenario is the same.

2. Iris recognition technology raises significant privacy concerns.

Although iris recognition has captured less public attention than other biometric technologies, it has been widely deployed by some agencies, from federal agencies like Customs and Border Protection, to local police like the Los Angeles County Sheriff's Department.[131] As of February 2023, the Federal Bureau of Investigation's Next Generation Identification Iris Service had more than 2.7 million sets of iris images.[132] The Department of Homeland Security had 9 million.[133]

Extracting biometric information from people's irises raises equivalent concerns about intrusion on expectations of privacy as nonconsensual extraction and analysis of fingerprints. In the absence of a recognized exception to the warrant requirement, collection and analysis of iris scans requires a warrant. This is true of attempts to scan irises during regular patrol or during *Terry* stops, as was apparently planned by border sheriffs several years ago.[134] And it is a critical protection as technology continues to develop.

Research into long-range iris scanning technology is particularly alarming. In 2015, researchers at Carnegie Mellon demonstrated iris recognition scanners that could capture and identify irises from up to 40 feet away.[135] They demonstrated this technology through a simulated traffic stop scenario: a driver sits in a pulled over car, the long-range iris recognition system behind the car automatically captures the reflection of the driver's eyes in the car's side-view mirror, runs

[129] *Johnson v. Vanderkooi*, 983 N.W.2d 779, 798 (Mich. 2022) (Welch, J., concurring).

[130] *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018).

[131] *See* Chris Burt, *Iris Biometrics Make Inroads with US Law Enforcement: Iris ID*, BiometricUpdate.com (Feb. 8, 2023), https://www.biometricupdate.com/202302/iris-biometrics-make-inroads-with-us-law-enforcement-iris-id.

[132] *Id.*

[133] *Id.*

[134] *See* George Joseph, *"Show Me Your Papers" Becomes "Open Your Eyes" as Border Sheriffs Expand Iris Surveillance*, The Intercept (July 8, 2017), https://theintercept.com/2017/07/08/border-sheriffs-iris-surveillance-biometrics.

[135] *See* Brooks Hays, *Iris Scanner Can ID a Person from 40 Feet Away*, UPI (May 22, 2015), https://www.upi.com/Science_News/2015/05/22/Iris-scanner-can-ID-a-person-from-40-feet-away/7071432303037.

it through an iris recognition system, and identifies the purported match. Warrantless deployment of remote iris scanning technology during an actual traffic stop would be cause for serious concern. And expansion to other settings—at protests, in schools, in public parks—would threaten to follow. Compared to fingerprints, iris scans have much more potential to become a biometric that can be collected without a subject's knowledge, permission, or participation, while being more accurate than face recognition. In that sense they have the potential to combine the worst features of face recognition and fingerprints. A warrant requirement is a critical protection against unjustified deployment of such technology at scale.

IV. Predictive Policing Technology

Predictive policing technology includes tools that are built using a wide array of inputs, including historical crime data, and that are used to "to help decide where to deploy police" (place-based) or "to identify individuals who are purportedly more likely to commit or be a victim of a crime" (person-based).[136] While the request for comment only solicits input on person-based predictive policing, both person-based and place-based predictive policing tools raise serious civil rights and civil liberties concerns.[137] The ACLU believes place-based predictive policing deserves equal scrutiny, and thus this section will discuss both. As explained below, there must be transparency and accountability at every link in the chain involving these technologies, including but not limited to the decisions to build the tools in the first place, the training data used to build these models, the structure of the tools themselves, details about how the tools are evaluated in terms of costs and benefits as well as accuracy, reliability, and fairness, and police practice and protocols in using these tools. With technologies ever changing, and given so much room for abuse, the best course of action is to resist the use of predictive policing tools. We join technology-focused organizations that call for halting new predictive technologies—and not funding them—unless and until they are proven to be nondiscriminatory.[138]

[136] Tim Lau, *Predictive Policing Explained*, Brennan Ctr. for Justice (Apr. 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.

[137] *See, e.g.*, Kristian Lum & William Isaac, *To Predict and Serve?*, 13 Significance 14 (2016). https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x; Danielle Ensign et al., *Runaway Feedback Loops in Predictive Policing*, 81 Procs. of Machine Learning Rsch. Conf. on Fairness, & Transparency 1 (2018), https://proceedings.mlr.press/v81/ensign18a/ensign18a.pdf; Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 NYU L. Rev. Online 15 (2019).

[138] *See, e.g.*, Electronic Privacy Information Center, Letter to Attorney General Garland Re: Executive Order 14074 and Title VI Compliance (July 6, 2022), https://epic.org/documents/epic-letter-to-attorney-general-garland-re-title-vi-compliance-and-predictive-algorithms/#_ftn10; Matthew Gaurigula & Jason Kelley, *Cities Should Act Now to Ban Predictive Policing Technologies . . . and Shotspotter Too*, EFF (Oct 2, 2023), https://www.eff.org/deeplinks/2023/10/cities-should-act-now-ban-predictive-policingand-stop-using-shotspotter-too.

1. Predictive policing tools are built on "dirty" data[139]—data that reflects historically racist police practices, and sometimes data that is unlawfully acquired—leading to inaccurate or arbitrary results.

To build these systems, developers generally train algorithms using datasets that may include historical crime data amassed by police departments over the course of many years, sometimes decades.[140] Alarmingly, some police departments use as training data information collected from unlawful practices, such as arrest records legally mandated to be sealed, raising questions of constitutionality. And even if datasets are technically lawful, they still reflect a long history of racist policing. Building models off data that inherently contain bias results in biased tools, creating a feedback loop that serves to further oppress Black and brown communities.

a) Predictive policing tools should never be trained on unlawfully acquired or retained data.

What we know about the training and use of predictive policing technologies is limited due to a lack of transparency. But there is reason for concern that police are using unlawfully acquired and retained data in their predictive policing tools and that this misuse will persist unless there is external intervention.

New York City provides an example of why we should be concerned. New York has strong privacy laws that protect people accused of but not convicted of crime.[141] Under the plain terms of these statutes, records related to an arrest that resolves in favor of the accused—such as where a prosecutor declines to pursue charges or a jury acquits—"shall be sealed and not made available to any person or public or private agency."[142] New York law is clear that this means the police may not use or disclose sealed arrest information even within the police department, except for specific reasons enumerated in the statutes themselves, such as for assessing employment applications.[143] This prohibition is for good reason: arrest records include a trove of sensitive personal information like address history, affiliations, and Social Security Numbers—not to mention details of dismissed charges, which might be embarrassing or stigmatizing.[144] Yet despite these strong privacy protections, the New York City Police Department (NYPD) has been using

[139] *See* Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 NYU L. Rev. Online 15 (2019).

[140] *See* Tim Lau, *Predictive Policing Explained*, Brennan Ctr. for Justice (Apr. 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.

[141] *See* N.Y. C.P.L.R. §§ 160.50, 160.55.

[142] N.Y. C.P.L.R. § 160.50(1)(c).

[143] *See R.C. v. City of New York*, 64 Misc. 3d 368 (N.Y. Sup. Ct. 2019).

[144] *See* Complaint, *R.C. v. City of New York*, No. 153739/2018 (N.Y. Sup. Ct. Apr. 4, 2018), https://www.bronxdefenders.org/wp-content/uploads/2018/04/R.C.-v.-The-City-of-New-York-Complaint-4-24-18.pdf.

millions of sealed arrest records in more than a dozen interconnected technologies including at least one predictive policing tool known as Patternizr.[145]

Specifically, Patternizr is a machine-learning model created by the NYPD that is trained on complaint and arrest reports that were generated between 2006 and 2015.[146] The corpus of data used to train Patternizr includes sealed records—a fact only revealed in the course of litigating a class action against the NYPD for violating state sealing laws.[147] A detective can query Patternizr by submitting a new crime complaint, known as a "seed."[148] Patternizr's algorithm will then identify prior complaints purportedly related to the seed, or prior complaints from purportedly related crime patterns.[149] Because Patternizr's output of prior complaints effectively suggests specific individuals for detectives to investigate, a person might find themselves suspected of a crime based solely on Patternizr's selection of their sealed arrest record in response to a detective's query.

Notably, the NYPD's misuse of statutorily protected information is not the only problem with Patternzr's data set. The corpus of data on which Patternizr was trained is from the height of the NYPD stop-and-frisk program, which targeted Black and Latinx people and was ruled unconstitutional.[150] Hundreds of thousands of people stopped under that racially biased program were arrested,[151] often on specious allegations later dismissed, thus creating records that may well populate Patternizr.

In response to the class action lawsuit, which was brought by The Bronx Defenders on behalf of millions of people whose sealed arrest records the NYPD unlawfully uses, a judge ordered the NYPD to reform its practices and specifically banned the use of sealed records in predictive policing tools: "Predictive Technologies may not use Sealed Records or Information either as inputs to train the model, or as potential outputs. The NYPD shall adjust their existing Predictive Technologies to remove Sealed Records and Information that have previously been used."[152] This specifically covers Patternizr.[153] This ban is a victory—but the NYPD's use of these records in their predictive policing tools was only uncovered by the lawsuit in the first place. This raises the question as to how many other police departments are using unlawful, ill-gotten data in their predictive policing tools. The lack of transparency about data sources means that the public cannot assess the lawfulness of the data used, nor seek remedies for the data's use and abuse.

[145] *See id. See also*, *R.C. v. City of New York*, No. 153739/2018, 2021 WL 4427369 (N.Y. Sup. Ct. Sept. 27, 2021) (granting preliminary injunction).

[146] Alex Chohals-Wood & E.S. Levine, *A Recommendation Engine to Aid in Identifying Crime Patterns* (Mar. 29, 2019), https://nparikh.org/assets/pdf/sipa6545/week10-police/policing/nypd-patternizr.pdf.

[147] *See* Complaint at 2, *R.C. v. City of New York*, 153739/2018 (N.Y. Sup. Ct. Apr. 4, 2018).

[148] Alex Chohals-Wood & E.S. Levine, *A Recommendation Engine to Aid in Identifying Crime Patterns* 2 (Mar. 29, 2019), https://nparikh.org/assets/pdf/sipa6545/week10-police/policing/nypd-patternizr.pdf.

[149] *Id.* at 6–8.

[150] *Floyd v. City of New York*, 959 F. Supp. 2d 540 (S.D.N.Y. 2013).

[151] *See id.* at 573.

[152] *R.C. v. City of New York*, No. 153739/2018, 2023 WL 7929127, at *4 (N.Y. Sup. March 29, 2023).

[153] *Id.*

Moreover, the NYPD is fighting the order in the sealed records class action and seeking to continue using sealed records in Patternizr,[154] even though its use of sealed records in Patternizr is contrary to longstanding state law. Without external controls, there is no assurance police departments will prevent the use of private or biased data in their predictive policing tools.

b) Even when training data is not collected or retained unlawfully, it still reflects decades of racism and bias in policing, thus perpetuating and reinforcing racist policing.

Place-based predictive policing illustrates the glaring problem of racial bias inherent in using tools built off historical crime data. Predictive policing tools are necessarily built on top of historical data—and the history of policing is a deeply racist one.[155] Historical crime data is not an objective history of all crime: it does not capture unreported crime, officer discretion in investigations and arrests, or the series of racist decisions that lead to a conviction in some cases and not others. Analyzing police behavior and crime data have revealed racial disparities in every stage of the criminal process.[156] To paint the picture, a Black person is more than twice as likely to be arrested than a white person, and five times more likely to be stopped without cause than a white person.[157] And when place-based predictive policing tools spit out results that direct police to patrol a certain area, it can bring a whole swath of people, mostly from Black and brown communities, under even greater scrutiny. Geolitica (formerly known as PredPol), a leading place-based predictive policing company, boasts on their website, "[a] key part of managing your officers is just making sure they are spending time in the areas where they are supposed to patrol. Geolitica helps with that by allowing you to set patrol guidance for specific locations down to a very granular level of a 500x500-foot box."[158] In densely populated urban neighborhoods, an area of 250,000 square feet (more than five acres) will capture a lot of people—who are then subject to more policing and surveillance, and potentially even deadly violence. In 2016, the LAPD shot and killed

[154] *See* Brief for Appellants at 53 n.7, *R.C. v. City of New York*, No. 2023-02267 (N.Y. App. Div. Sept. 5, 2023).

[155] *See* Connie Hassett-Walker, *The Racist Roots of American Policing: From Slave Patrols to Traffic Stops*, The Conversation (June 2, 2020), https://theconversation.com/the-racist-roots-of-american-policing-from-slave-patrols-to-traffic-stops-112816.

[156] Ezekiel Edwards, *Predictive Policing Software Is More Accurate at Predicting Policing Than Predicting Crime*, ACLU (Aug. 31, 2016), https://www.aclu.org/news/criminal-law-reform/predictive-policing-software-more-accurate ("Time and again, analysis of stops, frisks, searches, arrests, pretrial detentions, convictions, and sentencing reveal differential treatment of people of color. From racial bias in stops and frisks in New York, Boston, and Baltimore, to unwarranted disparities nationwide in arrests of Blacks and whites for marijuana possession (despite comparable usage rates), to disparities in the enforcement of minor offenses in Minneapolis, New Jersey, and Florida, as sure as the sun rises police will continue to enforce laws selectively against communities of color.").

[157] Will Douglas Heaven, *Predictive Policing Algorithms Are Racist. They Need to Be Dismantled.*, MIT Tech. Rev. (July 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice.

[158] *Data-Driven Community Policing*, Geolitica (last visited Jan. 18, 2023), https://geolitica.com/public-safety.

a total of six Black and Latinx men in areas identified by Operation Laser, their program utilizing predictive policing.[159]

These issues can affect both the inputs used by predictive policing algorithms to generate predictions as well as the labels—or outcomes—the tools purport to predict, and we should be wary of claims from vendors or others that these systemic issues can be resolved through technical or statistical fixes.[160] Predictive policing tools also lead to a pernicious feedback loop.[161] As computer scientist Suresh Venkatasubramanian succinctly stated, "If you build predictive policing, you are essentially sending police to certain neighborhoods based on what they told you—but that also means you're not sending police to other neighborhoods because the system didn't tell you to go there. . . If you assume that the data collection for your system is generated by police whom you sent to certain neighborhoods, then essentially your model is controlling the next round of data you get."[162]

Increasing evidence suggests that the outputs of predictive policing systems both perpetuate bias in policing and are highly inaccurate at the tasks they purport to be able to assist. For example, a recent analysis of Geolitica's place-based predictive policing software in Plainfield, New Jersey found that over several months in 2018, for more than 23,000 predictions output by Geolitica's systems, less than 100 predictions could be linked to a reported crime in the predicted category and area—meaning that by that definition, the system's accuracy was less than half of a percent. The Plainfield Police Department ultimately abandoned the software.[163]

[159] Johana Bhuiyan, *LAPD Ended Predictive Policing Programs Amid Public Outcry. A New Effort Shares Many of their Flaws*, The Guardian (Nov. 8, 2021), https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform.

[160] *See, e.g.*, Sharad Goel et al. *The Accuracy, Equity, and Jurisprudence of Criminal Risk Assessment*, in *The Handbook on Big Data Law* (Roland Vogl ed., 2018), available at https://www.elgaronline.com/edcollchap/edcoll/9781788972819/9781788972819.00007.xml (discussing how biases that affect the outcomes or labels used for predictive risk assessments in the criminal legal system are difficult to resolve with statistical means); *see also* Laurel Eckhouse et al., *Layers of Bias: A Unified Approach for Understanding Problems with Risk Assessment*, 46 Crim. Just. & Behavior 185 (2019), https://journals.sagepub.com/doi/abs/10.1177/0093854818811379 (discussing how biases in the data cannot be resolved with technical means alone and are compounded by other issues with predictive tools in the criminal legal system).

[161] *See* Oakland City Council, Ordinance No. 13635 (2021) ("Predictive Policing Technology uses arrest data that can encode patterns of racist policing behavior and as a result, are more likely to predict a high potential for crime in minority neighborhoods or among minority people and several studies have shown that these tools perpetuate systemic racism, leading to disparate arrest rates."). *See also* Kristian Lum & William Isaac, *To Predict and Serve?*, 13 Significance 14 (2016). https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x; Danielle Ensign et al., *Runaway Feedback Loops in Predictive Policing*, 81 Procs. of Machine Learning Rsch. Conf. on Fairness, & Transparency 1 (2018), https://proceedings.mlr.press/v81/ensign18a/ensign18a.pdf.

[162] Caroline Haskins, *Academics Confirm Major Predictive Policing Algorithm Is Fundamentally Flawed*, Vice (Feb. 14, 2019), https://www.vice.com/en/article/xwbag4/academics-confirm-major-predictive-policing-algorithm-is-fundamentally-flawed.

[163] Aaron Sankin & Surya Mattu, *Predictive Policing Software Terrible at Predicting Crimes*, The Markup / WIRED, https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes.

Ultimately, Black and brown communities will suffer the most harm from all of these issues.

2. Predictive policing tools use "black box" algorithms and are rife with human error and bias, requiring transparency as a necessary but not sufficient step towards ensuring respect for constitutional rights.

Predictive policing programs are often shrouded in secrecy, denying the public an understanding of exactly how these technologies work. The algorithms and models used by predictive policing tools are designed and developed by humans, and humans err. The "black-box" nature of some machine-learning algorithms further obfuscates the technology. And because these tools are only as good as the data they are trained on, if polluted data is fed in, polluted predictions will come out. In order to assess the degree to which these factors may lead to lack of reliability in the algorithms' results, public access and third-party validation and review is essential. As the ACLU and fifteen other civil rights, privacy, and technology focused organizations wrote in 2016, "[a] thorough and well-informed public debate, and rigorous, independent, expert assessment of the statistical validity and operational impact of any new system, are essential."[164] Without it, people facing criminal prosecution and the public are left in the dark.

Family policing algorithms provide an illuminating example of why transparency into automated decision-making systems that are used in high-stakes areas is critical to understanding how these systems impact civil rights. In 2016, Allegheny County, Pennsylvania, deployed a predictive tool, the Allegheny Family Screening Tool (AFST), to "estimate[] the probability that a child will be removed from their home by DHS [Department of Human Services] and placed in foster care within two years of being referred to the agency."[165] The ACLU requested data and documents related to the AFST; in collaboration with researchers from the Human Rights Data Analysis Group, the ACLU found that the data used by the algorithm and the predictions generated produce disparities between Black versus non-Black families, as well as potential disparities between families with members who have disabilities versus families with no disabled members.[166] The researchers' key findings included that the "AFST's algorithm, or the way its conclusions about a family were conveyed to a screener, could have been built in different ways that may have had a less discriminatory impact. And this alternative method didn't change the algorithm's 'accuracy' in any meaningful way."[167] Access to information and third-party review was crucial to these findings, but transparency alone, even when it allows for robust analysis of

[164] ACLU & 16 Civil Rights, Privacy, Racial Justice, & Technology Organizations, *Predictive Policing Today: A Shared Statement of Civil Rights Concerns* (Aug. 31, 2016), https://www.aclu.org/documents/statement-concern-about-predictive-policing-aclu-and-16-civil-rights-privacy-racial-justice.

[165] Marissa Gerchick et al., *The Devil is in the Details: Interrogating Values Embedded in the Allegheny Family Screening Tool*, Procs. of the 2023 ACM Conference on Fairness, Accountability, & Transparency (FAccT '23) 1292 (2023), https://dl.acm.org/doi/pdf/10.1145/3593013.3594081.

[166] Marissa Gerchick et al., *How Policy Hidden in an Algorithm Is Threatening Families in this Pennsylvania County*, ACLU (Mar. 14, 2023), https://www.aclu.org/news/womens-rights/how-policy-hidden-in-an-algorithm-is-threatening-families-in-this-pennsylvania-county.

[167] *Id.*

potential civil rights concerns, is not enough to guarantee accountability around the use of automated systems.

3. Law enforcement agencies must ensure they do not rely on the results of predictive policing tools to engage in unlawful policing.

a) Police officers should not rely on the results of predictive policing tools as a substitute for reasonable suspicion or probable cause.

Predictive policing tools generate probabilistic results, sometimes from unlawfully obtained data. Because their outputs are only a statistical or algorithmic *prediction*, and may reflect flaws in the underlying data and in the algorithm's programing and design, those results can never constitute reasonable suspicion or probable cause.[168] Because predictive policing tool outputs are not reliable indicia of individualized suspicion, relying only on the results of such tools as a basis for stopping, detaining, or interrogating an individual is an unconstitutional violation of that individual's rights. There have been instances in which police officers have substituted a facial recognition search result as probable cause in a warrant application, leading to wrongful arrests;[169] it is not hard to imagine police doing the same with predictive policing search results. Without strict procedural safeguards, police may misinterpret or misuse these tools, particularly in light of heavy marketing campaigns, targeted at police departments, that claim these tools are scientifically rigorous.[170] Strict protections against unjustified reliance on these tools' outputs is critical.

b) Police officers may be primed by predictive policing tools to, in the best case, presume criminality, and in the worst, use excessive or deadly force.

Predictive policing tools also translate into different behavior on the ground. When police patrol an area identified by a place-based predictive policing tool, they may be more likely to think that any given individual is a criminal. They may rush into the area mentally prepared for conflict. And given law enforcement's demonstrated propensity to use excessive force against members of Black and brown communities,[171] combined with predictive policing's racial bias problem, these tools will likely result in police being more reactive and violent towards these communities.

This is a documented problem. Chicago deployed SoundThinking (then known as ShotSpotter), a tool that purports to accurately identify gunshot sounds, in predominantly Black

[168] *See* Molly Griffard, *A Bias-Free Predictive Policing Tool?: An Evaluation of the NYPD's Patternizr*, 47 Fordham Urb. L.J. 43, 70–71 (2019).

[169] *See, e.g.*, 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; 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.

[170] *See, e.g.*, *Technology*, Geolitica (last visited Jan. 18, 2024), https://geolitica.com/technology ("Geolitica represents a significant investment of over 70 research-years of PhD-level analysis, modeling and development. It has been tested and proven in dozens of departments of all sizes in multiple countries around the world.").

[171] *See* Jenn Rolnick Borchetta & Brandon Chapman, *State and Local Governments Must Take Responsibility for Police Violence*, ACLU (June 22, 2023), https://www.aclu.org/news/criminal-law-reform/state-and-local-governments-must-take-responsibility-for-police-violence.

and Latinx communities.[172] A review of almost two years of data about ShotSpotter use revealed a record of dangerous and ineffective policing: “On an average day . . . the ShotSpotter system sends police out on more than sixty dead-end searches for gunfire. Every one of these deployments creates a dangerous, high-intensity situation where police are primed by ShotSpotter to expect to find a person who is armed and has just fired a weapon.” [173] These deployments create unnecessary risk: they “create an extremely dangerous situation for residents, prompting unnecessary and hostile police encounters, and creating the conditions for abusive police tactics that have plagued Chicago for decades.”[174] To be sure, ShotSpotter is not a traditional predictive policing tool—it only targets gunshots and uses sensors, not historical crime data, to identify these alleged gunshots. But this case study still highlights the problem: police will be primed by technological tools that inform them that an individual or a location is potentially dangerous or criminal, and the consequences can be severe.

* * *

The ACLU appreciates the opportunity to provide input on these important topics. 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

[172] Brief of Chicago Community-Based Organizations as Amici Curiae at 3, *Illinois v. Williams*, No. 20 CR 0899601 (Ill. Cir. Ct. Cook Cty. 2021), https://endpolicesurveillance.com/documents/2021-05-03-Motion-for-Leave-to-File-Brief-as-Amici-Curiae-with-Ex.-A-Amicus-Brief-attached.pdf.

[173] *Id.* at 2.

[174] *Id.* at 3.