Digital Justice Initiative Comments to PCLOB Facial Recognition Roundtable

June 30, 2020

Thank you for the opportunity to participate in PCLOB's Facial Recognition Roundtable. The use of facial recognition technology (FRT) is fraught with civil rights and privacy risks, especially for people of color.

The Lawyers' Committee for Civil Rights Under Law is a nonpartisan, nonprofit organization, formed in 1963 at the request of President John F. Kennedy to involve the private bar in providing legal services to address racial discrimination. The Lawyers' Committee's Digital Justice Initiative works at the intersection of racial justice and technology, data, and privacy. It fights against predatory commercial data practices and invasions of privacy which have disparate impacts on communities of color, especially African Americans, immigrants, women of color, and LGBTQ people of color.

People of color suffer disproportionate harms from domestic surveillance, both because surveillance technologies are frequently infected with biases and because even facially neutral technologies are often used in a discriminatory fashion. When a neutral technology is used to make a discriminatory surveillance system operate more efficiently, the use of that technology is itself a discriminatory action.

In 2020, the risks of FRT are being scrutinized closer than ever. Earlier this month, three major tech companies announced that they would limit the use of their FRT—Amazon and Microsoft now disallow the use of their FRT by law enforcement and IBM has stopped the development of FRT for all purposes.[1] The companies have cited concerns about racial profiling, mass surveillance, and its misuse by police as reasons for the restrictions. Just this week, the Association for Computing Machinery, the world's largest educational and scientific computing society, has called for a moratorium on the use of FRT that can compromise human and other legal rights.[2]

Political demonstrations following in the wake of the murder of George Floyd have also brought concerns about the use of FRT into sharp focus, with some protesters worried

[1] Jay Greene, *Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM*, The Washington Post (June 11, 2020) https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.

[2] U.S. Policy Technology Committee, *Statement on Principles and Prerequisites for the Development, Evaluation and Use of Unbiased Facial Recognition Technologies*, Association for Computing Machinery (June 30, 2020) https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf.

that their images collected by police will be used against them.[3] They have good reason to be concerned. For example, in 2016, police used FRT to compare photos of demonstrators at the Freddy Gray protests to a database of millions of images from social media accounts.[4] In some cases, this led to arrests by Baltimore Police Department.[5]

Government entities are also concerned about FRT. Just this week, the city of Boston banned of the use of FRT by the Boston Police Department. The measure was unanimously approved by city councilors, finding that FRT was a "racially discriminatory technology."[6] Boston's decision was based, in part, by the unwarranted arrest of an African American man who was misidentified by FRT in Detroit.[7] Once again, concerns about bias in FRT has fueled calls to regulate its use.

The Lawyers' Committee does not have an official position on the use of facial recognition technology in airports, however we recognize that there are civil rights implications that reach beyond air travel. Historically, surveillance technologies are initially deployed abroad or at ports of entry to normalize their use and then creep into everyday use by law enforcement and other actors. Consequently, PCLOB should consider the impact of FRT not just within airports but on the whole of society.

Does your organization make a distinction between the use of FRT for identity verification vs. use for surveillance purposes? If yes, what are those distinctions?

Although limiting the use of FRT to identity verification carries less privacy and civil rights risks than the use of FRT for general surveillance, there are number of potential harms in either case. Consequently, it is imperative to have clear and comprehensive definitions of permissible and impermissible uses. Used either way, FRT has problems

---

[3] Geoffrey A. Fowler, *Black Lives Matter could change facial recognition forever — if Big Tech doesn't stand in the way*, Washington Post (June 12, 2020) https://www.washingtonpost.com/technology/2020/06/12/facial-recognition-ban/.

[4] Kevin Rector & Alison Knezevich, *Maryland's use of facial recognition software questioned by researchers, civil liberties advocates*, The Baltimore Sun (Oct. 18, 2016) https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html.

[5] Russell Brandom, *Facebook, Twitter, and Instagram surveillance tool was used to arrest Baltimore protestors*, The Verge (Oct. 11, 2016) https://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api.

[6] Sean Philip Cotter, *Boston City Council votes to ban facial-recognition technology*, Boston Herald (June 24, 2020) https://www.bostonherald.com/2020/06/24/boston-city-council-votes-to-ban-facial-recognition-technology/.

[7] Sarah Rahal & Christine Ferretti, *Metro Detroiter battling 'flawed' facial recognition software*, The Detroit News (June 24, 2020) https://www.detroitnews.com/story/news/local/detroit-city/2020/06/25/wrongfully-accused-detroit-facial-recognition-software-michigan-aclu/3214958001/.

with racial and gender biases, deviating from the public's privacy expectations, a lack of algorithmic transparency, and increased harm from data breaches.

Depending on how it is implemented, when FRT is limited to verifying the identity of subjects, there are still a number of potential risks. FRT identity verification can create a chilling effect, interfere with political activism protected by the First Amendment, and produce a wealth of additional harms through the aggregation of FRT data. Each of these risks are discussed below.

It is also important to note that, subjecting airline travelers to facial recognition scans would affect a large percentage of the American population seeking to exercise their constitutional right to freedom in interstate travel. The use of airports is ubiquitous and effectively mandatory for many travelers. Eighty-eight percent of Americans have flown commercially at some point in their lives and almost 50 percent fly each year.[8] Last year, 927 million American passengers flew within the United States.[9] Given the incredible number of travelers who would be subject to identity verification via FRT, its widespread use could be considered more akin to general surveillance. It would also raise concerns about secondary uses of FRT data collected at airports—will it be available to law enforcement for use in other contexts?

What are your assessments of any potential civil rights harms related to using biometric algorithmic determinations to inform identity verification?

There are wide variety of civil rights impacts associated with the use of facial recognition identity verification systems. Some of these concerns apply to the use of FRT for surveillance purposes; we are explicitly including such concerns because we believe that if FRT is implemented for identity verification, law enforcement will inevitably use it for surveillance as well.

Racial & gender bias

It is well-documented that facial recognition systems are less accurate at identifying women and people of color—particularly women of color. Research shows that FRT works well at identifying white men, is somewhat inaccurate at identifying white women, is inaccurate at identifying men of color, and is extremely inaccurate at identifying

[8] Jacob Metcalf, *When Verification is Also Surveillance*, Data & Society Research Institute (Feb. 27, 2018) https://points.datasociety.net/when-verification-is-also-surveillance-21edb6c12cc9.
[9] Bureau of Transportation Statistics, *Final Full-Year 2019 Traffic Data for U.S. Airlines and Foreign Airlines U.S. Flights*, U.S. Department of Transportation (Mar. 19, 2020) https://www.bts.dot.gov/newsroom/final-full-year-2019-traffic-data-us-airlines-and-foreign-airlines-us-flights.

women of color. A recent study conducted by NIST found that Asian and African American people were frequently misidentified as much as 100 times more than white men.[10] Another study from MIT found that light-skinned men were correctly identified 99% of the time, while only 65% of darker-skinned women were correctly classified.[11] Much of this disparity can be attributed to the fact that the data used to train facial recognition algorithms underrepresent darker-skinned people.[12] Moreover, this disparity could grow worse over time because accuracy decreases as the size of the database increases when attempting to match an individual to a database.[13]

FRT bias is particularly harmful to juveniles of color. It is well-documented that young Black and Latino males are far more likely to be detained by the police.[14] When racially discriminatory FRT is used, juveniles of color are more likely to be incorrectly—and permanently—placed into law enforcement databases. Together, FRT will make a bad situation even worse, exacerbating the over-policing of young people of color.

When facial recognition is used in airports, it will have a disparate impact on women and people of color, leading to more discriminatory detentions and police actions against people of color, unwarranted interrogations, confrontations with security officers, and more missed flights and inefficiency.

Profiling of activists

The use of FRT is especially troubling when used to surveil civil rights activists, union organizers, and protesters. These populations are particularly vulnerable to the risks of discriminatory policing, retaliation, chilled speech, and government coercion. We are particularly concerned that FRT would be used to track racial justice advocates.

There is a long, tragic, history of law enforcement using surveillance to disrupt civil rights movements. For example, the FBI program, COINTELPRO, systematically surveilled Dr. Martin Luther King Jr., blackmailing him with information that was

---

[10] Patrick Grother, Mei Ngan & Kayee Hanaoka, *Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects*, National Institute of Standards and Technology (Dec. 2019) https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[11] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings of Machine Learning Research 1–15 (2018).

[12] *Id.*

[13] Electronic Frontier Foundation, *Street Surveillance* (Oct. 24, 2017) https://www.eff.org/pages/face-recognition.

[14] *See* Radley Balko, *There's overwhelming evidence that the criminal justice system is racist. Here's the proof.*, The Washington Post (June 10, 2020) https://www.washingtonpost.com/graphics/2020/opinions/systemic-racism-police-evidence-criminal-justice-system/.

obtained about his personal life.[15] Using this information, the FBI sent at least one anonymous letter, threatening Dr. King with public exposure unless he committed suicide.[16] Even as recently as 2017, the FBI was widely criticized for using surveillance against racial justice activists, fabricating a categorization for non-existent "Black Identity Extremists," and spying on them through the bureau's IRON FIST program.[17]

COINTELPRO gathered information to blackmail Dr. King with traditional methods—bugging his hotel rooms and physically following him around. Technologies such as facial recognition identification systems would provide more information about activists that are targeted by the government, at a fraction of the cost. FRT would enable civil rights violations against activists at a scale that far exceeds surveillance programs such as COINTELPRO.

Chilling effects on speech and assembly

As the use of facial recognition technology becomes more prevalent, people may be deterred from First Amendment-protected activities. In *NAACP v. Alabama*, the Supreme Court upheld the privacy of civil rights activists against oppressive state intrusion, recognizing "the vital relationship between freedom to associate and privacy in one's associations."[18] This chilling effect is harmful to society and will disproportionately impact marginalized communities at greater risk of persecution. In *United States v. Jones*, Justice Sotomayor observed that "awareness that the government may be watching chills associative and expressive freedom," and that pervasive surveillance "may alter the relationship between citizen and government in a way that is inimical to democratic society."[19] Other scholars have advanced that pervasive surveillance will "incline choices toward the bland and the mainstream."[20]

---

[15] Carl T. Rowan, *Breaking Barriers: A Memoir* 260 (1991).
[16] *Id.*
[17] Alice Speri, *The FBI Spends a Lot of Time Spying on Black Americans*, The Intercept (Oct. 29, 2019) https://theintercept.com/2019/10/29/fbi-surveillance-black-activists/.
[18] *National Association for the Advancement of Colored People v. Alabama*, 357 US 449 at 462 (1958). *See also id.* (Surveillance of activists can expose them to "economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility.")
[19] *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (citing *United States v. Cuevas-Perez*, 640 F. 3d 272, 285 (CA7 2011) (Flaum, J., concurring)).
[20] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 506–07 (2006).

Pervasive surveillance has been linked to heightened levels of stress and anxiety.[21] It has been found to promote distrust between the public and the state.[22] Perhaps most concerning, surveillance promotes conformity—a powerful deterrent to the freedom of speech and assembly.[23] This is pernicious because conformity is often used as a weapon to entrench discriminatory power structures, especially in a society that often treats "white, straight, cis-male" as its image of a default person.

Another consideration when considering the use of FRT is mission creep. If facial recognition technology is adopted by airports, it becomes normalized which, in turn, justifies its use in other venues. For example, in the Netherlands, a smart camera designed to assist in enforcing migration law is now used for law enforcement, as well.[24] In India, government biometric ID cards—originally intended to provide identification to the country's poorest citizens—are now used for security monitoring, to track welfare transactions, and to verify employment.[25] Law enforcement use of FRT may incubate in airports, but it will not end there.

Exceeds reasonable expectations of privacy

Facial recognition technology exceeds reasonable privacy expectations. Much of society's presumptions about privacy are based on traditional forms of surveillance which have significant practical limitations.[26] People know they can be observed while out in public, but they don't expect someone to be watching and recording their every move. This is what allows patients to visit their therapists, protesters to attend political demonstrations, and churchgoers to visit their places of worship, without the fear of facing societal stigma.

---

[21] *See e.g.*, Emina Subašić, et al., *Leadership, Power and the Use of Surveillance: Implications of Shared Social Identity for Leaders' Capacity to Influence*, 22 The Leadership Quarterly 170–181 (2011); M.J. Smith et al., *Employee Stress and Health Complaints in Jobs With and Without Electronic Performance Monitoring*, 23 Applied Ergonomics 17–27 (1992).

[22] Marie-Helen Maras, *The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the 'Others'?*, 40 International Journal of Law, Crime and Justice 65–81(2012).

[23] *See* Dominic Abrams et al., *Knowing What to Think by Knowing Who You Are: Self-Categorization and the Nature of Norm Formation, Conformity and Group Polarization*, 29 British Journal of Social Psychology 97–119 (1990).

[24] Tim Dekkers, Technology Driven Crimmigration? Function Creep and Mission Creep in Dutch Migration Control, Journal of Ethnic and Migration Studies 1849–1864 (Oct. 25, 2019). https://doi.org/10.1080/1369183X.2019.1674134.

[25] Alicia P.Q. Wittmeyer, Mission Creep, Foreign Policy (Apr. 29, 2013) https://foreignpolicy.com/2013/04/29/mission-creep/.

[26] Elizabeth E. Joh, *The New Surveillance Discretion*, Harvard Law & Policy Review 23 (2016).

Before the advent of new technologies like facial recognition systems, information about an individual's whereabouts was technically public but remained in practical obscurity.[27] FRT allows individuals to be precisely tracked over a long period of time, easily and cheaply replacing forms of surveillance commonly regarded as practically impossible to conduct.

Limiting the use of FRT to just verifying passenger's identities may help it remain within the reasonable expectation of privacy, but there are significant concerns that FRT would later be used in ways that would exceed those boundaries.

Sharing of biometric data increases risks

Data collected from FRT, if not discarded immediately after use, can easily be cross referenced with other databases, leading to a host of civil rights and privacy risks. This differs from traditional forms of identity verification, which are generally confined to merely confirming if an ID matches the person. When discrete bits of data are compiled over time or aggregated with other datasets, it creates a detailed profile of individuals that is greater than the sum of its parts, far exceeding a reasonable expectation of privacy.[28] For example, identifying an individual at a particular airport at a particular time has mild privacy risks, but combining that information with other data can create a map of their movements over a long period of time, revealing intimate details such as their religious beliefs, sexual habits, and political affiliation.[29]

Sharing FRT data can also lead to increased civil rights and privacy risks when used by outside organizations that do not share the same values as the original, collecting entity. We are particularly concerned about the potential for this data to be used by law enforcement and immigration agents in secondary contexts. Studies have shown that data collected for one purpose are rarely restricted to just that purpose.[30] Digital content is often retained indefinitely; it may end up in the hands of irresponsible actors and used in unanticipated or improper ways.

In the context of identity verification in airports, FRT may exceed a reasonable expectation of privacy by allowing security officials to aggregate a passenger's identity

[27] *See United States v. Jones*, 132 S. Ct. at 963 (Alito, J., concurring) ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken.").
[28] *See United States v. Jones*, 132 S.Ct. at 954–55 (Sotomayor, J., concurring); *Riley v. California*, 134 S. Ct. 2473 at 2489–91 (2014).
[29] *See Jones*, 132 S.Ct. at 954–55 (Sotomayor, J., concurring).
[30] Karen Levy & Solon Barocas, *Privacy at the Margins*, 12 International Journal of Communication 1166–1188 (Feb. 8, 2017) https://ijoc.org/index.php/ijoc/article/view/7041/2302.

with other databases. While passengers expect to have to show identification, they probably would not expect that their picture is cross referenced with state and federal criminal databases, motor vehicle records, social media accounts, and retail store customer tracking.[31]

Lack of transparency or testing

The use of biometric algorithms involves a high degree of opacity that can conceal innate biases in their decision-making processes.[32] FRT uses machine learning to provide accurate outputs, but the automated methods used to achieve those outputs are often immune to human review. Without the ability to audit how algorithms operate, data subjects are unaware of the biases baked into the system and are unable to safeguard their civil and privacy rights.

Furthermore, even if FRT could be proven to be unbiased, demonstrating that it improves security is extremely difficult to demonstrate. Predicting criminal behavior through identity-based security methods, such as FRT, is problematic because it makes complex conclusions about human behavior, outside social context, without human oversight.[33] Once again, these decisions are made without the ability to audit the algorithmic reasoning. This creates a security system that cannot be tested for its effectiveness.

Increased harm from data breaches

Whenever information is collected, data breaches are always a risk. Last year, 165 million sensitive records were exposed through data breaches.[34] However, when biometric data is compromised, the harm is especially great. Biometric data, such as those produced by FRT, is particularly vulnerable because the data are unique and cannot be changed. Unlike a username or password, FRT subjects cannot change their face. If FRT data falls into the wrong hands, the affected subject has little recourse. When harms related to FRT are already skewed to affect marginalized communities, the increased risk of data breaches disparately impacts them.

---

[31] Suparna Goswami, *Facial Recognition: Balancing Security vs. Privacy*, Data Breach Today (Sep. 25, 2019) https://www.databreachtoday.com/facial-recognition-balancing-security-vs-privacy-a-13145.
[32] Future of Privacy Forum, *The Privacy Expert's Guide to Artificial Intelligence and Machine Learning* 17 (Oct. 2018) https://fpf.org/2018/10/18/fpf-release-the-privacy-experts-guide-to-ai-and-machine-learning/.
[33] Jay Stanley, *How the TSA's Facial Recognition Plan Will Go Far Beyond the Airport*, ACLU (Oct. 23, 2018) https://www.aclu.org/blog/privacy-technology/surveillance-technologies/how-tsas-facial-recognition-plan-will-go-far.
[34] J. Clement, *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2019*, Statista (Mar. 10, 2020) https://www.statista.com/statistics/273550.

Do you think that bias and other potential harms are more likely to occur with review by a face-matching algorithm or by a human security officer?

Bias and other harms are possible when verifying a subject's identification by either algorithm or by human review. Both systems are imperfect. However, algorithmic decision making has several disadvantages over traditional human review.

In addition to the civil rights and privacy risks discussed in the previous section, harms related to the use of FRT are more likely to occur because of the exponential nature of technology.[35] Like any emerging technology, the costs of operating FRT will decrease and its use will become more and more ubiquitous, eventually supplanting traditional human review. When this occurs, the problems of racial and gender bias, societal chilling effects, algorithmic opacity, and the other risks discussed above, will be multiplied across every system. Certainly, many of these risks are still possible with human review, but because technology spreads exponentially and humans do not, the risks associated with FRT will also increase substantially.

This problem is compounded by the fact that there may be little to no variance between FRT systems, ensuring that an existing error or bias is present across all sites. Once again, comparing FRT with human review, while human officers may possess flaws, not every officer will make the same mistakes. In addition, as discussed above, it may be more difficult to identify and redress biases in a black box algorithm vs. the retraining of human officers.

In your opinion, what is the appropriate balance between aviation security, and privacy, civil rights, and civil liberties?

We can and must have security, privacy, civil rights, and civil liberties. Risk calculations should account for the potential level of harm as well as the likelihood that injury will occur. But civil rights, civil liberties, and privacy are of equal importance, not secondary, to security. We know, from long historical experience, that surveillance technologies frequently are deployed in a manner that has a disproportionate impact on communities of color. As previously discussed, the potential harms from FRT are substantial and its benefits appear speculative. Moreover, in the aviation security context, if the intelligence community has specific information about a specific risk or threat, they should not need to compromise the privacy and civil rights of people of color as a whole in order to respond to it.

[35] *See* Ray Kurzweil, *The Law of Accelerating Returns*, Accelerating Intelligence (Mar. 7, 2001).

To what extent does your organization believe that there are transparency issues related to the use of facial recognition at airports for identity verification purposes? What steps could be taken to address those issues?

If FRT is used at airports for identity verification, transparency will be critically important. Transparency facilitates the trust of the public, exposes embedded biases, and allows candid evaluation of the effectiveness of the technology.

There are several ways to ensure transparency in FRT systems. First, an entity that employs algorithmic decision making should be held accountable for any flawed mechanisms used to produce an output. In many cases this is impossible to audit, especially in complex machine learning models such as multilayer neural networks. However, without some degree of algorithmic transparency, biases present in the data input cannot be detected and are amplified and passed to the output. Efforts should be made to mitigate this "black box" problem. Training data should also be available to assess input biases.

Second, data collected via FRT should follow standard privacy principles. Before implementing FRT identity verification, travelers should be given answers to the following questions:

- Can subjects opt out of FRT scanning?
- What is the FRT data being used for?
- Who, if anyone, is the FRT information being shared with?
- What data is actually being collected?
- How long is the FRT data is retained?
- What are the data security practices being followed?
- Can subjects update or delete their data? How?
- What protections are there against discriminatory uses?
- How can subjects assert their rights or file complaints of abuse?

Third, when an FRT system is used, the outcomes of its use should be routinely audited (with public reports) to assess the effectiveness of the program:

- How many false positives were made? How many false negatives?
- Which travelers were subject to more errors? Is there a disparate impact on certain races, genders, or other protected characteristics?
- How many dangerous or fraudulent passengers were detained?
- How does the use of FRT compare to traditional methods?
- How many cameras are employed? How many scans were made? Where has FRT been used?

What does your organization believe are the most significant civil rights impacts and/or potential harms related to the use of facial recognition technology for identity verification at airports?

As a racial justice organization, the deployment of racially-biased and difficult-to-audit technologies, the potential for discriminatory use and profiling by law enforcement and immigration authorities, and the disparate impact FRT has on people of color are our most important concerns.