U.S. Commission on Civil Rights

March 8, 2024

Public Briefing

Civil Rights Implications of the Federal Use of Facial Recognition Technology

Written Testimony of

Dr. Joy Buolamwini
Founder, Algorithmic Justice League
Dear Chairwoman Garza and commissioners,

Thank you for the opportunity to provide a written testimony for the U.S. Commission on Civil Rights on the federal government’s use of facial recognition. The focus on the Department of Justice (DOJ), Department of Homeland Security (DHS), and Department of Housing and Urban Development (HUD) is especially welcome.

My name is Dr. Joy Buolamwini. I am the founder and president of the Algorithmic Justice League\(^1\) (AJL), an organization that combines art and research to illuminate the social implications and harms of artificial intelligence (AI). I established AJL to create a world with more equitable and accountable technology after experiencing facial analysis software failing to detect my dark-skinned face until I put on a white mask. I have shared this experience widely in TED Talks, interviews, the Coded Bias feature-length documentary, and the book ‘Unmasking AI: My Mission to Protect What is Human in a World of Machines’ to help people understand what is at stake with AI.

Since I began sharing my experience and raising the alarm about AI’s real harms, there has been a sea change in the policy landscape around these technologies. The president’s executive order on AI\(^2\) and associated guidance were an important step in the right direction. Since then, many bills have been introduced to finally attempt to erect much-needed guardrails.\(^3\) However, because deployment of face-based biometric technologies, particularly by the government, has run so far ahead of regulation, there is much work to be done to re-center civil rights (along with biometric and creative rights) as the core of how we use — or choose not to use — AI now.

Let me be clear: these technologies are not a genie that has escaped from the bottle. Nonuse of AI that violates people’s civil rights or perpetuates discrimination remains a meaningful and implementable policy option, as I recently argued alongside renowned constitutional law scholar Barry Friedman.

---

\(^1\) Algorithmic Justice League. https://www.ajl.org/


This is especially true when both the technology and the way it is deployed pose risks to people's rights and liberties. Such is the case with how the U.S. Transportation Security Administration (TSA) has rolled out its pilot of facial recognition technology at airport security checkpoints. This can also be seen with the DHS' use of facial recognition systems which blocked asylum seekers from being able to file their claims based on the color of their skin. As we recently wrote in The New York Times, how law enforcement use of emerging AI-powered tools can cause serious, life changing consequences:

“Consider the cases of Porcha Woodruff, Michael Oliver and Robert Julian-Borchak Williams. All were arrested between 2019 and 2023 after they were misidentified by facial recognition technology. These arrests had indelible consequences: Ms. Woodruff was eight months pregnant when she was falsely accused of carjacking and robbery; Mr. Williams was arrested in front of his wife and two young daughters as he pulled into his driveway from work. Mr. Oliver lost his job as a result.”

In this written testimony, I will share:

1.) The importance of regulating facial analysis, facial recognition, and remote biometric identity technologies together and how using the FTC 2012 workshop definition of facial recognition technologies can provide broader protections against abuse and misuse of these technologies.

2.) Preliminary findings from an ongoing AJL project on traveler’s experiences with facial recognition use in US airports. Our preliminary results and what may be experienced as coercive consent practices.

3.) Why generative AI and the ability to reconstruct faces from faceprints or face templates pose cyber security and biometric privacy risks.

4.) The importance of transparency in brief and explain what we know about the reliability of these algorithms and why the metrics we have do not tell the whole story of the risks to our rights, liberties and dignity. In this section, my comments will not only relate to TSA, but will touch on the many pernicious uses of unreliable and invasive FRT by DHS, DOJ, HUD and others including the IRS.

5.) why biometrics should be considered a high priority for civil rights and privacy regulators and what can be done with specific recommendations.

---


1. The risks and harms of facial analysis, facial Recognition, and remote biometric technologies must be addressed together to avoid consequential loopholes.

Much ink has been spilled about what terminology to use when describing automated systems that extract data from human faces in some manner. Colloquial use of the term facial recognition does not typically match expert use of the technical term facial recognition. During the 2012 FTC sponsored Facing Facts workshop, the term facial recognition technologies (FRTs) was used as a catchall which AJL has adopted “to describe a set of technologies that process imaging data to perform a range of tasks on human faces, including detecting a face, identifying a unique individual, and estimating demographic attributes.” The Facing Facts workshop summary paper defined facial recognition as "any technology that is used to extract data from facial images.”

Bad actors may find loopholes that undermine ongoing hard work to establish guardrails and restrictions on powerful biometrics tools, if we use too narrow a definition for technologies that extract data from human faces. If we focus on what technical experts categorize as face recognition or facial recognition technology with falls under facial identification (one-to-many matching) or facial verification (one-to-one matching),

restrictions and regulation will leave out instances where the extraction of face data can be used to perpetuate discrimination based on demographics, religious affiliation, or other information that can be extracted from a face. Guessing a person's age, race, or even the type of facial hair they have are technical capabilities that are often categorized under the umbrella of facial analysis. Failing to address facial analysis technologies has consequences. For example, the Intercept did an investigation alleging that IBM partnered with the NYPD to search for suspects by attributes such as skin tone, hair color, and facial hair. In this case, regulation and legislation which exclude facial analysis capabilities that make inferences about skin color, gender, facial hair, and more would provide a loophole for profiling and discrimination.

Finally, the TSA foregrounds the term biometric identity technologies in airport signage used to inform the traveling public about its use of facial recognition technology. Depending on the airport, my documented experience shows some of these signs are not fully visible. Additional language about face matching or facial recognition can be hidden from view. Thus if DHS is

---


foregrounding biometric identity technologies in its communication with the public regarding facial recognition, regulations and legislation should address biometric identity technologies. Because biometric identity technologies can also refer to systems beyond facial recognition including fingerprint verification technology, we recommend policies use the term remote biometric technologies which can include gait analysis, voice recognition, and with improved camera technology iris recognition. Facial Recognition and Remote Biometric Technologies as a banner to address harmful use of AI-powered surveillance technologies can help make sorely needed regulations and restrictions robust to future technological advances. Whether a vendor markets itself as doing face matching, biometric identity verification, demographic extraction, infrared authentication or more, ongoing effort to enact guardrails will continue to apply.

2. Facial recognition at U.S. airports: The #InPlaneSight campaign reveals lack of meaningful opportunity to offer informed, uncoerced consent.

At AJL, we launched the #InPlaneSight campaign in the summer of 2023 to 1.) raise awareness about the right for US citizens to opt out of facial recognition scans at U.S. airports. 2.) To learn about traveler experiences with facial recognition, consent practices and concerns about TSA pilot program as well as 3.) Provide decision-makers with qualitative and quantitative information about the encoded, or those excluded from systems not designed with them in mind and being negatively impacted by AI. The flying public should know that U.S. citizens can opt out of facial recognition that TSA or the U.S. Customs and Border Protection (CBP) are using.

We have received a substantial number of scorecard submissions via fly.ajl.org, and we continue to gather responses. Though CBP was not the initial focus of our study, we are consistently receiving concerns about CBP’s use of facial recognition for international flights as well.

The TSA scorecard elicits information about notice, signage and consent to compare TSA practices on the ground with written policies. We also seek to understand whether these practices can be improved to serve the traveling public. Our preliminary data indicates the overwhelming majority of respondents did not receive notice in line with TSA’s published best practices.

Notice

Question: Did you receive clear information about the facial recognition program at the airport?  
Preliminary Responses: Over 90% of respondents stated they did not receive notice about the use of facial recognition at the airport.

Signage

Questions: Did you see signage that indicated you could opt out?  
Preliminary Responses: Over 85% of respondents stated there was a lack of signage that made it clear opting out was an option.
Verbal Consent

**Question:** Were you verbally informed of your right to opt out?

**Preliminary Responses:** Over 95% of respondents stated that TSA agents did not ask for their participation.

Furthermore, a vast majority of respondents (~95%) stated they do not want the government to hold their face data. We are lacking clarity on what kind of data is being held and for how long.

The responses echo my own experience. In late February, I traveled through Boston Logan and SFO airports. In both airports, as a researcher who is aware of TSA policies, I had difficulties both locating and reading biometric technology signage in full. Signage alerting travelers that weapons are not allowed were clear. The contrast on the weapons signs made them hard to miss with red and black text on a white background (see Figure 1).

<table>
<thead>
<tr>
<th>Figure 1. No Weapons Sign</th>
<th>Figure 2. Biometric Identity Verification Sign</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="No Weapons Sign" /></td>
<td><img src="image2.png" alt="Biometric Identity Verification Sign" /></td>
</tr>
</tbody>
</table>

**Placement:**
- **Figure 1.** Sign is at the beginning of the line entrance and hard to miss.
- **Figure 2.** Sign is hard to read in full both when a traveler is in position to present ID and at the entrance of the line.
The signs about weapons were also near the front of the entrance of the line. The signage related to biometric identity and thus facial recognition was presented with less contrast with light-blue text on a dark-blue background (see Figure 2). These signs were near the TSA agents at the checkpoint computers, typically difficult to see if one is not actively looking for it and at times with key information covered. When I was departing from SFO some signage appeared to be a black and white 8 X 11 inch print-out. I dive into these details, because the reality of TSA deployment appears to risk uniformed and coercive consent. In the case of my flight from Boston Logan, there was a canine unit at the checkpoint along with a long line of travelers behind and in front of me. I not only experienced social and time pressure to catch my flight, I also felt financial pressure given the investment made to make the trip. Concerningly, in my observations, TSA officers told travelers to step up to the camera with no verbal indication that they can opt out. These conditions are not conducive for freely given consent. In fact, the lack of notice, hard to read signage, and authorities figures directing travelers to participate, instead create conditions for coerced consent. Ironically, the program is supposed to be voluntary for now according to TSA’s policies. In practice, many people do not know they can opt out. The TSA Biometrics Strategy for Aviation Security and the Passenger Experience released in July 2018 indicates plans to make biometric identity the default way to travel. Despite the TSA claims that face data information is not shared with law enforcement at present absent regulation, these policies can change at any time.

3. Biometric privacy and cybersecurity risk must be considered.

As governments increasingly put facial recognition and other biometric technology between people and critical services, we all have to weigh the profound risks to our privacy that the cybersecurity of these third party vendors plays. Our faces are unique. If our face data is leaked, a risk that has become a reality specifically in the context of federal contractor’s data practices, there is little chance to get it back. We have seen voice clones and deepfakes used for scams; but when our face data is put at risk, anything from our bank accounts to our benefits

---

10 https://www.tsa.gov/biometrics-technology
could be at risk. Even if the image capture date is deleted within minutes, hours, days, or months, we need to know whether and how the government or third-party vendors hold faceprints also known as face template data. Research shows that contrary to what some vendors claim, face template data can be reverse engineered to reconstruct an image of a person's face. Thus, it is not enough to delete face images alone. Given the rise of generative AI tools that can produce deepfakes, any data stored about a person presents risks for biometric privacy and cybersecurity. FRTs and remote biometric technologies pose a unique challenge because of their potential to be both pervasive and stealthy. This means that many of us may not either know that we have an option to opt-out or be aware that the technology is being used at all. Biometric privacy is yet another key factor we must weigh, especially as these tools are rolled out unevenly and with disproportionate impact. FRTs and remote biometric technologies should not be used if there is no affirmative proof that they will not perpetuate discrimination or violate people's rights.

4. **TSA and other government agencies including DHS and HUD should align with National Institute of Standards and Technology (NIST) metrics and reporting for commercial algorithms.**

The TSA and other initiatives from CBP, DHS and HUD have not fully disclosed the algorithms or the companies they use to deploy facial recognition. Error metrics vary depending on which type of facial recognition task is in question (i.e., 1:1 vs. 1:N). Why not share the vendors and algorithms that these agencies use? This is not an idle question — the numbers that are most relevant to understanding disparate impact are not currently available to the public or lawmakers. All government agencies that use FRTs when interacting with the public should release the exact demographic results that show error rates by race, gender, age and skin color and their intersections. Instead of putting it on lawmakers to figure out what to ask, agencies should share the data in the manner that NIST publicly shares. They do not have to start from scratch.

We are not only questioning the technology, but who is wielding it and to what purposes now as well as in the future. Please allow me to illustrate why full and complete disclosure of the algorithms being used and their performance is critical to understanding the disparate impact of these technologies.

Reliance on aggregate accuracy rates hide disproportionate harm.

---


The widely cited Massachusetts Institute of Technology research that AJL\textsuperscript{18} did on facial analysis showed that even a company that boasts 93.7\% accuracy overall on a benchmark dataset still had a 20.8\% accuracy gap between light males and darker females. For a different task — facial verification (1:1) — the latest numbers from 2023 show that regional, gender, and age disparities are apparent even for the top-listed algorithms when it comes to false positive matches.

Look at the top-listed algorithm (recognition 001 at the time of my writing) on the government NIST leaderboard.\textsuperscript{19} The ratio of the best performance to the worst performance shows that West African women (65 years of age and older) were over 3,000 times more likely to have a false positive match than Eastern European men (20 - 35 years of age) in the worst case. These women were also 15 times more likely to have a false positive match than the average case across all demographics.\textsuperscript{20} Algorithms with lower listings on the leaderboard (cloudwalk Mt 007 for example) have substantially higher performance on West African women than the top-listed algorithm. This tells us that aggregate numbers like what the TSA has publicly provided are insufficient. We need disaggregated data. We are unclear why the TSA has shared an overall accuracy number but has not shared a disaggregated number by region, gender, and age as NIST has done. I also caution the TSA and other agencies on generalizing metrics across a national context. In countries with diverse populations, the high performance of majority groups can overshadow poor performance on minority groups.

Accuracy is not the only metric — the risk of automating profiling.

Tests of facial recognition technologies show improving performance metrics on many demographics. But even flawless facial recognition (which, let me be clear, does not exist) would still be dangerous. From a privacy and rights perspective, more accurate facial recognition systems strengthen the surveillance state apparatus.\textsuperscript{21} The ability to track individuals precisely can lead to abuse and targeting based on race, gender, creed, religious association, proximity to abortion clinics and more. It can also lead to breaches of privacy or be used to enforce rules in unfair or unjust ways. For example, just last year, The Washington Post reported\textsuperscript{22} that Mealnie Otis was nearly evicted because cameras and facial recognition systems purchased with HUD dollars seemed to indicate she committed the minor infraction of


\textsuperscript{20} Small numbers matter. The .0189 false match rate of West African women [65-99] would mean that in 1,000,000 instances 18,900 faces would be impacted.


lending her fob to another person. Otis, as the Post notes, has vision loss, and was allowed to stay after she explained the visitor was a friend bringing her groceries.

Facial recognition, and especially 1:N matching,\textsuperscript{23} whether on drones, military or police robots, or as a gatekeeper to essential services can also perpetuate digital dehumanization and systematic violations of people’s rights. Take, for example, efforts\textsuperscript{24} at the Internal Revenue Service (IRS) to require taxpayers to verify their identity through facial-recognition software that would have infringed on privacy and digital rights concerns.\textsuperscript{25} Pressuring individuals to engage with facial recognition to easily access essential public services is another avenue for coercive consent.

5. An agenda for action.

In the long term, the proliferation of facial recognition technologies risks normalizing surveillance technology, perpetuating discrimination, and invading privacy. I would recommend the federal government move away from adopting facial recognition technologies as a default or preferred option for access to government service and traveler identity checks.

As I stated in a recent TIME op-ed,\textsuperscript{26} understanding of different measures of performance matters because the government should not knowingly deploy FRTs that have been documented to be discriminatory and give preferential treatment to one protected class over another. Even more important than accuracy is agency — people must have a voice and a choice regarding facial recognition technologies. At AJL, we are calling on the TSA to share:

- Disaggregated demographic data across its two-year study, showing results by race, gender, age and color and their intersections per airport with the change in numbers month by month.
- A third-party auditor needs to independently verify this data.
- What mechanism the TSA uses to ensure its officers consistently notify travelers of their right to opt out of facial recognition.
- What policies and penalties are in place for TSA officers who violate a passenger’s right to opt out.
- Exact data (all data — not just images but metadata about faceprints/face templates, demographics, behavioral analysis) that the TSA has collected on U.S. citizens, how

\textsuperscript{23} Gerchick, M. & Cagle, M. (2024, February 7). When it comes to facial recognition, there is no such thing as a magic number. \textit{ACLU of Florida}. 

\textsuperscript{24} Cioffi, K. & Adamant, V. (2022, February 14). The IRS’s Abandoned Facial Recognition Is Just the Tip of a Harmful Biometric Iceberg. \textit{Slate}. 

\textsuperscript{25} Buolamwini, J. (2022, January 27), The IRS Should Stop Using Facial Recognition. \textit{The Atlantic}. 

\textsuperscript{26} Buolamwini, J. (2023, November 21). The Face is the Final Frontier of Privacy. \textit{TIME}. 
many facial scans, how long the data was held, what proof is in place that data has been deleted.

- Who authorized the collection of this data.
- What third-party vendors have had access to this data.

In the short term, because we are hearing from many travelers that they were not aware of the right to opt out, we also recommend that the TSA:

- Issue over airport intercoms periodic messages in English and Spanish about individuals’ right to opt out and to do so especially during busy travel times when there is more pressure to process travelers.
- Improve the placement, contrast, and language of TSA biometric identity signage. Specifically foreground the term “facial recognition” or “face recognition” — not just “biometric-identity” — because the public is still being introduced to technical terms. Affirmative consent requires the knowledge of what potential harms or privacy implications are linked to the use of FRTs.

TSA says its officers are trained to treat each passenger with dignity and respect. The dismissive comments one of the high-ranking officials at TSA has made about traveler concerns with facial recognition does not appear to adhere to this standard.

On the TSA’s Biometrics Technology webpage,27 the organization states: “Additionally, TSA does not tolerate racial profiling. Profiling is not an effective way to perform security screening, and TSA personnel are trained to treat every passenger with dignity and respect. The concerns and guidelines above should serve as guideposts for scrutiny of facial recognition within other government agencies.”

The ability to opt out of FRTs is critical in other areas of public domain, and a great opportunity for the government to advance the recent Presidential Executive Order on AI. Individual agency when interacting with government apparatuses like the TSA or DHS is a core component to achieving equitable digital privacy that also makes way for crucial biometric rights. Notice of use, right of refusal, and disclosure of incidents of harm or failures are crucial to establishing transparency with the public about their biometric rights and agency.28

Facial recognition and remote biometric technologies can amplify inequalities and violate civil rights and liberties. Facial recognition technologies pose unprecedented privacy risks because the face is a largely immutable high-visibility identifier. Finally, peer-reviewed academic studies show technologies that extra face data from facial images are susceptible to bias across protected categories including gender, race and age. Given these factors, any government use of

facial recognition technologies should be held to an extremely high standard that clearly demonstrates that the systems are not causing harm or perpetuating discrimination. Without such proof, these systems should not be deployed. Moreover, we must preserve meaningful alternatives and access to redress — including a mechanism for deleting personal data. Absent that, I fear that people’s rights will continue to be violated, avenues for redress will not be established and the face will indeed be the final frontier of privacy. Thank you for the opportunity to share preliminary findings from the Algorithmic Justice League and our recommendations.

Sincerely,

Dr. Joy Buolamwini
Dr. Joy Buolamwini is the founder of the Algorithmic Justice League, a groundbreaking MIT researcher, and an artist. She is the author of the national bestseller *Unmasking AI: My Mission to Protect What Is Human in a World of Machines*. Dr. Joy advises world leaders on preventing AI harms. Her research on facial recognition technologies transformed the field of AI auditing and has been covered in over 40 countries. To date, her “Gender Shades” paper is one of the most cited peer-reviewed AI ethics publications. and her TED talk on algorithmic bias has been viewed over 1.7 million times.

Dr. Joy lends her expertise to congressional hearings and government agencies seeking to enact equitable and accountable AI policy. As the Poet of Code, she creates art to illuminate the impact of AI on society. Her art has been exhibited across four continents. Her writing and work have been featured in publications like *TIME*, *The New York Times*, *Harvard Business Review*, *Rolling Stone* and *The Atlantic*. She is the protagonist of the Emmy-nominated documentary *Coded Bias* which is available in 30 languages to over 100 million viewers.

She is a Rhodes Scholar, Fulbright Fellow, and recipient of the Technological Innovation Award from Martin Luther King Jr. Center. *Fortune Magazine* named her the "conscience of the AI." *Time magazine* names her to the Inaugural list of 100 most influential people in AI. She holds two masters degrees from Oxford University and MIT; and a bachelor's degree in Computer Science from the Georgia Institute of Technology. Dr. Joy earned her Ph.D. from MIT and was awarded an honorary Doctor of Fine Arts degree from Knox College.