ACLU

January 14, 2022

Via Email

Office of Science and Technology Policy
BiometricRFI@ostp.eop.gov

RE: Request for Information (RFI) on Public and Private Sector Uses of
Biometric Technologies (FR Doc. 2021-21975)

The American Civil Liberties Union writes in response to the Office of Science and Technology Policy's October 2021 Request for Information on Public and Private Sector Uses of Biometric Technologies. This submission surveys a number of concerns with use of biometric technologies by government and private actors, and presents policy recommendations. Due to space constraints, this submission can only touch on some of the ACLU's concerns with the adoption and use of biometric technologies.

I. General Concerns About Biometric Technologies

A. Biometric identification and tracking technologies

Because biometric identifiers are personally identifying and generally immutable, biometric technologies pose severe threats to civil rights and civil liberties by enabling privacy violations—including loss of anonymity in contexts where people have traditionally expected it, persistent tracking of movement and activity, and identity theft. Additionally, flaws in the use or operation of biometric technologies can lead to significant civil rights violations, including false arrests and denial of access to benefits, goods, and services. These problems disproportionately affect people of color and members of other marginalized communities.

1. Biometric technologies enable mass tracking and identification

Although the limited collection and use of certain biometrics, such as fingerprints, dates back many decades, the development of machine-learning-based biometric technologies, paired with the proliferation of digital-age network technologies, has resulted in categorically new powers in the hands of government and corporate actors to quickly identify, track, and surveil people. Prior to the digital age, collection and use of biometrics was slow and laborious, and thus not possible at scale. Today, however, machine-learning algorithms allow near-instantaneous collection and/or exploitation of an array of biometrics, including those drawn from physical or biological attributes (e.g., face recognition, voice recognition, iris or retina scans, fingerprints, and DNA) and activity (e.g., gait recognition and keystroke recognition). These capabilities can be used both to identify people in an instant, and to pervasively track their movements in the physical world and online, such as by using face recognition to track a person across a network of video surveillance cameras. The ability of these technologies to capture biometrics at a distance or from video footage can evade detection and can easily be carried out without knowledge or consent of affected individuals. Even biometric identifiers that traditionally had to be collected from individuals in-person, such as fingerprints, iris scans, and DNA, can now sometimes be captured remotely, raising newly pressing concerns.

2. *Failures of biometric technologies can result in civil rights violations and denials of access to benefits and services*

Because of design flaws, hardware limitations, and other problems, biometric technologies can fail to function as advertised, leading to failed identifications. When flawed technologies fail to accurately identify unknown individuals or verify the identities of people seeking access to benefits or services, these failures can result in civil rights violations. The harms of failed identifications disproportionately affect people of color, lower-income people, people with disabilities, and members of other marginalized groups.

While all biometric technologies are error-prone, problems with face recognition technology raise particular concerns in light of its rapid proliferation. Multiple studies show that face recognition algorithms have markedly higher misidentification rates for Black people, people of color, women, and children.[1] This bias is partly attributable to the fact that datasets used to train face recognition algorithms have been "overwhelmingly composed of lighter-skinned subjects." Additional sources of bias are introduced when face recognition systems rely on digital camera images because, when taking photos of darker-skinned faces, the cameras often fail to provide the degree of color contrast that the algorithms need to produce and match faceprints.

Even when face recognition technology functions well in controlled test conditions, it is prone to fail in real-world applications. The accuracy of face recognition is directly affected by the quality of the images being searched—error rates will be greater when two photographs contain different lighting, shadows, backgrounds, poses, or expressions. Face recognition can be extremely poor at identifying a person in a low-resolution image or a video, or at accurately finding matches when searching against a large database of images, in part because so many people within a given population look similar to one another.

Finally, even when biometric technologies work at a technical level, their adoption can create barriers to access to essential services for people living on low

[1] *See* NIST, *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software; John J. Howard, Yevgeniy B. Sirotin & Jerry L. Tipton, *Quantifying the Extent to which Race and Gender Features Determine Identity in Commercial Face Recognition Algorithms*, Dep't Homeland Sec. Sci. & Tech. (May 2021), https://www.dhs.gov/sites/default/files/publications/quantifying-commercial-face-recognition-gender-and-race_updated.pdf; K.S. Krishnapriya et al., *Characterizing the Variability in Face Recognition Accuracy Relative to Race* (2019), https://arxiv.org/abs/1904.07325; Joy Buolamwini et al., *Gender Shades*, MIT Media Lab, https://www.media.mit.edu/projects/gender-shades/overview; Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE Transactions on Info. Forensics and Sec. 6, 1789–1801 (Dec. 2012), https://ieeexplore.ieee.org/document/6327355; Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU Free Future (July 26, 2018), https://bit.ly/2OkETHe.

incomes, people with disabilities, older people, and members of other marginalized communities. Biometric identity verification requirements that rely on access to, familiarity with, or ability to operate technology (such as smartphones, web cameras, or high-speed internet connections) can disproportionately harm individuals who lack access to or the ability to use those systems. And due to disparate rates of technology access by race, income, age, and disability status, these burdens will fall disproportionately on members of already marginalized communities.

B. Biometric technologies for inference of emotion, cognitive state, or intent

Biometric technologies also purport to be able to infer information beyond identity, but biometric inference technologies suffer from grave flaws—to the point of being, in many cases, nothing more than snake oil. These technologies are typically built on naive assumptions about the scientific objectivity and discoverability of internal mental states that simply do not hold up. For example, companies are increasingly promoting products that purport to detect emotion or affect, such as "aggression detectors." But psychologists who study emotion agree that this project is built on a bed of intellectual quicksand because there is no reliable or universal relationship between emotional states and observable biological activity.

The same faulty premise underlies other biometric technologies, such as products that purport to detect "suspicious activity" through video analytics and those that claim to detect lies or deception through eye movements. Lie detection is a notorious sinkhole of pseudoscience—despite a century of efforts, scientists have firmly refuted the scientific reliability of polygraphs. The link between high-level mental states such as "truthfulness" and low-level, involuntary external behavior is just too ambiguous and unreliable to be of use.

II. Use of Biometric Technologies by Law Enforcement and Immigration Authorities

A. Face recognition technology

Law enforcement use of face recognition technology poses a number of serious threats, making it dangerous both when it fails and when it functions.

Misidentifications resulting from law enforcement reliance on face recognition technology have resulted in multiple false arrests. Unsurprisingly, given the racially biased failure rates of the technology, documented cases of false arrests resulting from incorrect face recognition "matches" have disproportionately involved Black men. For example, three Black men in Michigan and New Jersey—Robert Williams, Michael Oliver, and Nijeer Parks—spent time in jail for crimes they did not commit after police relied on faulty face recognition 'matches' to arrest them. They are each now suing police.

Compounding the problem of false identifications by police-operated face recognition technology is the lack of transparency by police and prosecutors when face recognition has contributed to an individual's arrest or prosecution. In order to adequately test the reliability of identifications, defense attorneys are entitled to receive not only notice that face recognition technology was used, but also information about the error rates of the particular algorithm used (including any disparate error rates by race or other demographic categories) and the complete list of possible matches from which a human examiner selected the defendant as a match. Prosecutors rarely provide such information to defense teams, however.

The most common current use of face recognition technology by police involves trying to identify suspects from photographs or video. However, the threat of face recognition *surveillance* looms. Several 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 have piloted such technology. Deployment of face recognition or similar remote biometric tracking and surveillance capabilities would pose a catastrophic threat to privacy, by putting in the hands of government the ability to identify and track anyone or everyone as they go about their daily lives. Face recognition technology has been used to identify people attending Black Lives Matter and other protests, and the chilling effect of police deployments of biometric identification technologies that allow fast and pervasive monitoring of people cannot be overstated.

In recognition of these dangers, at least 23 jurisdictions—from Boston, to Minneapolis, to Jackson, Mississippi, to San Francisco, to the State of Vermont—have enacted legislation halting law enforcement or government use of face recognition technology. Others, such as the State of Maine, have enacted strict restrictions on law enforcement access to the technology.

Meanwhile, at the federal level, the FBI has gained access to hundreds of millions of Americans' driver's license photos to use in face recognition searches, and DHS has begun pursuing a sweeping vision of expanded use of face recognition in the air travel context. Indeed, DHS has already laid out—and begun following—a very specific, clear, and well-defined pathway for how its current programs (CBP use at airline departure gates and arrival checkpoints, and growing TSA use) will lead to a much broader implementations of face surveillance at the airport. And from there, this technology will be poised to expand far beyond the airport, following in the footsteps of other aviation security measures (such as bag searches, magnetometers, PreCheck, and CLEAR) that have spread beyond aviation contexts and into American life, threatening to create a checkpoint society the likes of which the U.S. has never known.

B. DNA

Use of DNA for biometric technologies is particularly concerning because of its immutability and the depth of personal information it can reveal—including not only identity, but also family relationships, ancestry, and propensity for health conditions. Moreover, because many law enforcement databases are made up of samples collected through the criminal system—for example, at arrest or conviction—these databases are racially biased in that they have a higher proportion of samples from Black people than the proportion of Black people in the U.S. population. Further compounding the problem are situations in which people are compelled to give their DNA to these databases in exchange for a plea deal, asylum seekers not charged with a crime are compelled to give DNA samples, or even children are tricked into discarding DNA which is then added to databases. Thus, because of the realities of over-policing among Black and brown people, these law enforcement databases may create a feedback loop.

Moreover, the ability to acquire an individual's DNA without their knowledge or consent from an item they have touched—as law enforcement agents frequently do today—and use it to identify that person's past and future relatives, or to impute their facial geometry, calls for tight protections against abuse. Another area of concern is the ease with which law enforcement can access certain privately maintained genetic genealogy databases, which allow millions to be identified through their DNA because a distant relative used a direct-to-consumer genetic test.

Another area of concern in DNA biometric technology is error-prone or blackbox technologies that claim to analyze DNA rapidly, or to identify contributors in complex DNA samples that would be uninterpretable using traditional methods. Probabilistic genotyping algorithms claim to identify genotypes in mixed DNA samples, but because the software employing these algorithms is maintained by private companies, audits of this technology are infrequent or impossible—and when they do happen, can reveal errors affecting large numbers of criminal investigations. These examples represent clear failures of regulators to insist on rigorous scientific validation and accuracy standards for tools used in the criminal legal system.

III. Employment and Public Benefits

A. Identity verification for unemployment insurance and other public benefits

Identity verification using biometrics to access unemployment and other public benefits gained popularity during the pandemic and has since infiltrated essential government services. Specifically, ID.me, a private company, has contracts with at least twenty-seven states' unemployment agencies as well as numerous federal agencies to provide remote identity verification, with many agencies providing no in-person alternative. ID.me uses face recognition technology to compare uploaded images of a government identification with a mobile phone or webcam selfie. While touted as a means to prevent fraudulent claims and identity theft, there are many potential harms associated with using remote identity verification and face recognition in essential government services. ID.me keeps all biometric data, even after a person closes their account, and thus individuals are forced to choose between accessing the benefits they need and protecting their biometric data and privacy. Moreover, the ongoing concerns about the accuracy of face recognition technology when identifying people of color and inequities in technology access for low-income people and people of color mean that the individuals who most critically need unemployment support and public benefits may face the greatest barriers to accessing them.

B. Face and voice analytics during interviews

Face and voice recognition technology is being used to collect and analyze biometric data during employment interviews. Vendors of predictive interview hiring tools dubiously claim to measure an applicant's skills and personality traits through automated analysis of verbal tone, word choice, and facial expressions. This technology raises an enormous risk of amplifying employment discrimination and violating civil rights laws. Predictive hiring tools often rely on training data regarding who would be a successful employee that reflects existing institutional and systemic biases in employment. Predictive tools that rely on facial and audio analysis raise even more risk that individuals will be automatically rejected or scored lower because of accents, disabilities, skin color, or because they are transgender, nonbinary, or gender nonconforming. Indeed, the very traits that these tools purport to measure are often themselves proxies for disabilities, gender, race, or other protected characteristics, as opposed to traits that are causally linked to job success. The lack of transparency in the use of these tools only adds to the harm—applicants know that they are being subjected to an online recorded interview, but often do not know that the interview will be analyzed through automated means or the standards that will be used to assess the interview. As a result, applicants often do not have enough information about the process to know whether to seek a disability accommodation.

C. Monitoring employees for productivity/attention

Workplace surveillance systems collect data about employee activities using smart phones and other systems that collect biometric data. The data used in these systems power algorithmic management systems that have expanded as a standard in most sectors of the U.S. economy. This technology has created new challenges for workers regarding basic workplace conditions and employment insecurity. Constant workplace surveillance is highly psychologically stressful. It can also lead to an employer's demand for accelerated output without increased pay (worker speedups) and increased racial profiling and bias from algorithms used in the management system. Worker organizing may be restricted and the most vulnerable workers are subjected to constant stress of losing their jobs, exacerbating already existing economic inequalities. Further, there are few restraints on an employer's ability to surveil workers, who have limited privacy rights while on the job. Workers also do not always have the ability to challenge algorithmically derived employment decisions, including discipline or firing, because monitoring practices are often difficult to detect.

D. Employee timecard systems and access to secure areas

Time and attendance systems may use fingerprint, face, and retina scans to record work time and give employees access to secure areas. Employers using this technology assert that this technology prevents time fraud and improves security. Although biometric time systems have become more widespread in recent years, very few states have laws governing how companies collect, store, and disclose employees' data or whether employees need to give informed consent when their data is collected. An employee who refuses to provide their biometric data may be terminated since employers are not obligated to provide an alternative method for workplace time and access systems.

IV. Housing

Face recognition is being used in both public and private housing to control who has entry access to buildings and communities. The use of face recognition raises serious concerns about privacy harms and racial discrimination. Use of face recognition technology in housing communities without the consent or knowledge of residents can result in residents' unwitting inclusion in a biometric database, and in the automated monitoring of the comings and goings of residents and their guests. Privacy harms may also arise when housing authorities make the system's data available to law enforcement or other third parties. This practice particularly subjects individuals who cannot afford alternative housing options to surveillance. Discriminatory inaccuracies in face recognition technology may create harm to residents of color and undermine safety and security. Additionally, many systems that offer the technology for entry access also double as general surveillance systems, which raise the same privacy and discrimination harms. Tenants have voiced concerns when housing authorities attempted to install security surveillance that uses face recognition technology in both public and private housing.

V. Education

Students are increasingly required to use devices and applications, or be in spaces, that subject them to collection of their biometric data.

Remote exam proctoring and monitoring, which has seen explosive growth during the Covid-19 pandemic, has been plagued by face recognition technology that fails to recognize students of color, monitoring software that tracks students' eye movements, head movements, and keystroke patterns to flag "suspicious behavior" in a manner biased against disabled students, and opaque retention practices surrounding these data. Software that does not recognize students of color can lock them out of crucial exams or incorrectly flag them as "cheating."

Biometric technologies also raise concerns in physical schools. Companies are marketing voice-analysis aggression detectors, which involve the installation of special microphones in school hallways and other spaces that constantly monitor the voices of students to "assess threats." This technology has not proven to be accurate, and has been triggered by coughing and other innocuous sounds. Additionally, Black students and special education students are disproportionately flagged as "threats."

Similar concerns arise from the use of face recognition in schools to monitor video feeds for individuals placed on a school or district watchlist. In addition to the risk of false alerts—which will disproportionately harm students of color—the accumulation of faceprint data and constant surveillance over time presents serious privacy concerns for students.

VI. Commerce, Credit, and Banking

Biometrics are also finding uses in commerce, credit, and banking. Some retail stores, as well as venues such as concerts and stadiums, are using face recognition to scan their customers. Though few stores will disclose what they're doing, and marketing could be a motivation, the main purpose seems to be security—specifically, looking for people who have been blacklisted from a company's property to ensure they don't return. This kind of secretive, unregulated watchlisting is an ominous descendant of a long history of private and quasi-private watchlists, going back to the labor battles of the early 20th century, when workers and organizers were blacklisted as "troublemakers" and could have trouble getting a job. Even more than the government's nightmarish system of watchlists, private-sector face recognition watchlists lack due process or other safeguards against abuse.

The collection of data about people's visits, characteristics, and behavior for marketing purposes is also being pitched by companies as a reason for stores to secretly use face recognition on their shoppers. Again, it's hard to know how widespread such uses are given the secrecy involved.

Biometrics are also being used by businesses such as banks for identity verification. Banks have built giant voiceprint databases, for example, and are also turning to technologies like fingerprints and "behavioral biometrics" such as keystroke analysis.

VII. Policy Recommendations

A. Government use of biometric technologies

As the ACLU and dozens of other organizations have previously explained, the twin dangers of highly consequential misidentifications and pervasive surveillance mean that government agencies should not be deploying face recognition technology. At a minimum, the White House should:

- Place a moratorium on all federal government use of face recognition technology and other forms of biometric technology so long as bias pervades these systems and Congress has not acted to authorize the use of the technology in specific circumstances and with sufficient safeguards to protect our privacy interests and prevent harms caused by this dangerous, unregulated technology;

- Prevent state and local governments from using federal funds to purchase face recognition technology or access face recognition technology; and

- Support the Facial Recognition and Biometric Technology Moratorium Act, introduced by Senator Markey. This bill would make a federal moratorium law and would place additional limitations on federal funding of these technologies.

When other biometric technologies are used, they should only be used if they have a demonstrably negligible failure rate in real-world applications; a lack of differential accuracy rates for people of different races or ethnicities, gender, or any other protected characteristics considered individually and intersectionally; rely on training data that was collected in a manner that did not violate the privacy of the data sources; and include strict safeguards that protect the privacy of individuals subject to those technologies.

1. Law enforcement uses of biometric technologies

As explained above, law enforcement agencies should not be permitted to use face recognition technology. To the extent other biometric technologies threaten to permit pervasive mass tracking of people's movements and activities, law enforcement should likewise be barred from using them. Any biometric technology that law enforcement seeks to use to identify particular individuals should be subject to strict standards for accuracy and reliability and subject to rigorous accuracy testing. Tests of some biometric technologies currently run by the National Institute of Standards and Technology are a positive model for such testing. Additionally, police should not be permitted to collect known individuals' biometrics without a search warrant or, in some circumstances, following an arrest based on probable cause.

Law enforcement sequencing of DNA in investigations should not use SNP profiling or whole-genome sequencing, which reveals significantly more information about a person's ancestry, medical proclivities, and other private details than traditional methods. Local law enforcement agencies that receive federal funding should also be prohibited from maintaining their own DNA databases, which often lack the security protections and quality standards of the FBI's CODIS database.

2. Non-law enforcement government uses of biometric technologies

As explained above, the federal government should halt use of face recognition technology. If face recognition technology or other biometric technologies are ever to be properly used for identity verification in unemployment insurance or other benefits-eligibility determinations, they must be strictly regulated, including ensuring accuracy, reliability, and privacy as outlined above. Government agencies procuring such technologies from private vendors must conduct due diligence on these technologies, and require vendors to produce records disclosing their training data and detailing all studies that have been conducted on the technology's failure rates and differential accuracy rates. Once a biometric technology is deployed for identity verification, government agencies should gather anonymized, individual claimant-level data showing outcomes for attempts to verify identity, mode of verification, specific reason for identity verification failures, and claimant demographic information. The records collected as part of the agency's pre-procurement due diligence and the post-deployment anonymized claimant information should be published on the agency's website.

Agencies using biometric technologies for identity verification should ensure that they provide plain-language notice describing the identity verification process, available in as many languages as is feasible, as well as plain-language notice of the reasons for any denial and the corrective steps that can be taken. They should also provide an easy and obvious means of submitting alternative evidence of identity. Appeals processes for denials must be reliable and easily accessible. Agencies must also provide reliable and easily accessible in-person alternatives to biometric identity verification processes for people with limited technology access or who have privacy concerns.

B. Private uses of biometric technologies

Private entities should be barred from capturing or using biometric identifiers without first providing detailed, plain-language notice and obtaining express consent, and may not disparately treat people based on their withholding consent. The Illinois Biometric Information Privacy Act has successfully provided a base minimum of such protection for more than a dozen years, and the White House should support similar protections at the federal level.

The use of biometric information by private entities in the areas of employment, housing, credit, education, or any other areas protected by federal civil rights laws should be strictly regulated by agencies tasked with civil rights enforcement. Agencies should use the full scope of their authority to:

- Gather and publicize information on private uses of these technologies in the spheres under their purview;

- Issue regulations and guidance that set auditing requirements for processes using biometric information, including requiring regular auditing for discriminatory effects on protected classes as well as intersectional identities throughout a technology's conception, design, implementation, and use; proactively looking for and adopting less-discriminatory alternatives; assessing how training data was sourced and whether it is representative and accurate; ensuring that the technology is measuring lawful and meaningful attributes; ensuring clear and effective notice and recourse processes, and that people with disabilities are provided reasonable accommodations; and providing for public release of internal and external audit reports; and

- Aggressively engage in enforcement actions against private actors whose technologies violate federal civil rights protections.

* * * * *

Thank you for your consideration of these comments. The ACLU would welcome the opportunity to further discuss these critical issues. Please contact Nate Wessler (nwessler@aclu.org) and Olga Akselrod (OAkselrod@aclu.org) with any queries.