Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
January 14, 2022

Via Electronic Mail
Office of Science and Technology Policy
Executive Office of the President
1600 Pennsylvania Ave NW
Washington, DC 20500

Re: Comments in Response to Request for Information on Public and Private Sector Uses of Biometric Technologies
86 Fed. Reg. 56300 (October 8, 2021)

To Whom It May Concern:

Brooklyn Defender Services ("BDS") submits these comments in response to the Office of Science and Technology Policy ("OSTP")’s Request for Information on Public and Private Sector Uses of Biometric Technologies, 86 Fed. Reg. 56300, issued on October 8, 2021.

Brooklyn Defender Services (BDS) is a public defense office whose mission is to provide outstanding representation and advocacy free of cost to people facing loss of freedom, family separation and other serious legal harms by the government. For over 25 years, BDS has worked, in and out of court, to protect and uphold the rights of individuals and to change laws and systems that perpetuate injustice and inequality.

We represent approximately 25,000 people each year who are accused of a crime, facing loss of liberty, their home, their children, or deportation. Our staff consists of specialized attorneys, social workers, investigators, paralegals and administrative staff who are experts in their individual fields. BDS also provides a wide range of additional services for our clients, including civil legal advocacy, assistance with educational needs of our clients or their children, housing and benefits advocacy, as well as immigration advice and representation.

We thank President Biden and the OSTP for the opportunity to provide information and feedback about the uses of biometric technologies within the many systems our clients and communities are forced to navigate. This comment will address topics #1 and 4.

Criminal Defense: Our criminal defense legal teams encounter biometric technologies routinely across cases and contexts. The NYPD frequently deploys facial recognition systems, latent prints, and DNA analysis, for example. This comment will focus on two recent troubling deployments in the criminal legal system context: unlawful local DNA databasing and voice printing.

DEFEND • ADVOCATE • CHANGE
I. Unlawful local DNA databasing

In 1997, the New York City Office of Chief Medical Examiner (OCME) implemented a system for collecting previously-typed DNA profiles into a searchable local database. Originally, the OCME’s local database was called LINKAGE. In 2014, the lab absorbed the LINKAGE database into the local level of the CODIS database, called the Local DNA Index System (“LDIS”).

At a state level, the New York State legislature created the State DNA Databank in 1994 with the passage of Executive Law § 995. The database became operational in 1996. By law, when it comes to known contributors, the New York database can only house DNA collected from people convicted of a crime. While the list of crimes for which a conviction permits DNA sample collection has grown five times since 1996, the New York State legislature has repeatedly rebuffed efforts to expand DNA collection to people who are arrested but never convicted of a crime.²

Despite New York State’s careful balance between the individual’s rights to genetic and basic privacy, as well as due process, and the State’s interest in crime solving, the City of New York’s agencies—the NYPD and the OCME—have chosen to operate a rogue DNA database that reaches samples taken from persons not authorized for collection. In other words, the OCME’s “LDIS” does an end run around New York State’s carefully prescribed scheme. Over the last five years, the OCME’s rogue database has been growing.³

---

¹ By way of brief background, CODIS (Combined DNA Index System) is actually the software databasing package developed and provided by the Federal Bureau of Investigation to DNA laboratories around the country. The CODIS database system consists of three levels: the National DNA Index System (NDIS); the State DNA Index System (SDIS); and the Local DNA Index System (LDIS). As the administrator of the CODIS database system, the FBI promulgates detailed regulations governing the types of samples that can be uploaded to NDIS, as well as quality assurance standards for labs conducting testing that feeds into NDIS.

² It is worth noting that, in 1999, the legislative record reflects that then-Mayor Rudy Giuliani even specifically requested that the legislature expand collection to arrestees. Mayor Giuliani asserted: “While the City enthusiastically supports this legislation and acknowledges the positive effect it will have on solving crime, it should be noted that the City of New York believes DNA testing upon arrest would allow for even greater efficiency and effectiveness in law enforcement. Examining DNA samples at the time of arrest would dramatically increase the ability of police to accurately identify or negate one’s potential culpability while under arrest.” The New York State Legislature refused to expand the database to arrestees.

a. Growth of the OCME’s Rogue Database

This unauthorized database has been fed in part by the surreptitious collection of individuals’ saliva samples by the NYPD. Self-regulation is not the answer here. What started as a self-regulated, unauthorized database has emerged into a vast invasion of the genetic privacy of thousands of New Yorkers, many if not most of whom, are impoverished people of color.

We have watched videos where our clients have asserted their right to counsel as they drink from a water bottle or smoke a cigarette offered to them by the police. NYPD has even been observed offering teenagers cigarettes in addition to juice bottles or water bottles for DNA collection. No person, let alone a child, would envision that accepting a cigarette to smoke in the middle of a public building with the blessing of the police would mean that their DNA profile would end up in perpetuity in a database. Then they are led out of the interrogation room, the cigarette butts and juice bottles are left in an intentionally placed ashtray or garbage bin. The police then collect the cigarette butts and bottles for evidence. This same little game plays out with water cups and juice or water bottles, and DNA profiles are collected by the thousands.

The local database is in contravention to Executive Law § 995-d, which dictates that the results of DNA testing are confidential, and which specifically protects the right of a defendant to nondisclosure of his or her DNA information.

As Dr. Howard Baum, former Technical Leader of the OCME and creator of the local database, has stated: he never envisioned that the database would become the repository of profiles that the NYPD dragnetted from Black and brown communities. Our clients have been directly impacted by dragnets – the systematic search for someone such as “a Black male in Brownsville” — practices that target our clients particularly because they are Black or because they are male or because they reside in a particular neighborhood.

Dr. Baum never envisioned that the database would include thousands of profiles from people who were tricked into handing over their DNA without consent or court-order. Even our clients who consented to have their DNA taken have told us that they had no real understanding that their cooperation meant that their DNA would stay in a government database forever.

Dr. Baum never envisioned that the local database would include people who were merely detained – sometimes never even arrested, and many never convicted of any crimes.

The local database was also set up long before the NYPD’s Domain Awareness System was created. The Domain Awareness System (“DAS”) is a software program created by the NYPD and Microsoft that aggregates data collected by the NYPD across the city. While the DAS’s role in aggregating surveillance camera video is well known, another DAS function is
its ability to inform officers whether or not an individual detainee’s DNA profile is in the database – thus making the detainee a target for DNA collection by individual police officers.

b. The OCME and NYPD DNA Collection and Storage Practice’s Threat to our Community’s Liberty is Growing.

The current practices of the NYPD mean that it is not only the countless numerical profiles of mainly people of color that are warehoused in an electronic database. For each of those warehoused profiles, the OCME maintains extracts of the DNA in tiny vials. As technologies emerge, law enforcement and the lab can go back to that vial and effectively interrogate the DNA to invade the genetic privacy of the individual’s genetic code in even deeper and more disturbing ways.

Genetic genealogy, which has been much reported-on in the news recently, is only the latest incarnation. This technique uses DNA analysis methods that mine more of the human genome for sensitive information than a traditional forensic DNA test and surveil not just the individuals’ DNA but also the DNA of that individual’s entire family line.

The DNA technique employed in genetic genealogy—Single Nucleotide Polymorphism (SNPs) testing or Next Generation Sequencing—is being considered for widespread forensic uses by the law enforcement community as we speak. Whereas traditional DNA testing—Short Tandem Repeat (STR) testing—only measures the lengths of certain segments of non-coding regions on our genome, SNPs and NextGen testing actually code the genome (revealing the specific As, Gs, Ts, and Cs we all learned about in high school) and potentially reveal deeply intimate details including things like predisposition to disease and susceptibility to addiction. And where STR testing only looks at a very small percentage of the overall genome, SNPs testing looks at huge percentages of the overall genome, revealing the most private elements of our selves.

In the face of this brave new world of genetic testing and the overall threat to privacy, as well as our First Amendment associational freedoms, we need to think about historically targeted communities when considering emerging technologies. The OCME and the NYPD, without oversight or regulation are effectively building a warehoused library of entire communities’ genetic extracts. With emerging technologies like genetic genealogy and so-called Next Generation Sequencing, the genetic privacy of not only the individual but the individual’s family will come under surveillance by law enforcement.

We now know that ‘Junk DNA’ is not really “junk” at all: it can by tied by inference to other areas on the human genome, that in turn can reveal sensitive information like susceptibility to disease. As technologies emerge and forensic profiles become even more

---

revealing of a person’s biological status, it is incumbent upon our elected officials to protect the genetic privacy of all people.

II. Voice printing

While the communities we represent are routinely having their genetic information collected and aggregated by law enforcement, its members often face the long-lasting and community-draining impact of periods of incarceration. Family and friends coordinate visits and phone calls, attempting to tend the connection between their incarcerated loved ones and the community they were torn from. On the other end of that tether, those incarcerated view access to outside phone calls to their family members, loved ones, counselors, and friends as a much-needed lifeline. But access to communication comes at a very real biometric cost.

Here, in New York City, the Department of Correction has contracted with the private company Securus Technologies to provide phone services within the City’s jails. Far from a basic phone company, however, Securus is more aptly described as a surveillance-tech-company-turned-phone-service-provider. One piece of Securus’s phone surveillance apparatus relies on the universal use of voice printing.

a. The Technology.

Securus Technologies’ phone system in an institution like those on Rikers Island audio records every phone call made. The call recordings are housed in an investigational database and are accessible to Corrections’ law enforcement officers. To sort this vast amount of unstructured data, Securus offers several products. One offering relies on the collection of a voiceprint database to identify the participants in audio-recorded calls.

In 2014, the City's Department of Correction entered into its first contract with Securus. Under that agreement, every person brought to a city jail and anyone on the outside who receives a call from DOC phones has their voiceprint taken. The voiceprint is merely a visual representation of an individual’s speech pattern. But available reporting indicates that the voice print database maintained by Securus includes speech patterns for all of those incarcerated, as well as those who have been incarcerated at any point in the past. It also houses voice prints from everyone who received a call from a Securus phone, including mothers, children, spouses, loved ones, siblings, friends, counselors, lawyers, spiritual advisors, and social workers.

The voiceprint database is run in conjunction with the audio recording database to analytically determine who participants are in recorded calls. The data aggregation and analytics tools allow law enforcement to identify recordings by voice print. For example, an investigator could search the recording database with my voice print and return all files that record my phone conversations, regardless of who originally placed the call or what number originally received it.
b. The Impact.

Just as the City’s local DNA database results in a community dragnet, housing the biometric intimacies of entire communities’ lives and identities, the voice print database results in a community dragnet of vocal identity, relationship, and intimate communication.

The repeated targeting of specific communities for such programs of mass surveillance reemphasizes the need for lawmakers to take seriously the task of legislative protection. If our lawmakers do not act soon, the rise of biometrics, big data analytics, and machine-driven surveillance will fundamentally destroy our bedrock First and Fourth Amendment principles.

**Unemployment Insurance Benefits:** Outside of the criminal legal system, our clients are encountering biometric surveillance in diverse arenas. Our family defense, immigration, and civil legal services teams encounter biometric technology use in a number of different contexts and use cases. This comment will focus on a recent troubling deployment in the employment benefits context.

BDS’s employment practice assists BDS clients by removing barriers to employment created by court-involvement. Our interdisciplinary team helps to fight employment discrimination, ensure clients are paid a fair wage, receive employment benefits, like time-off, and are free from workplace abuses. Our staff also provide legal representation and informal advocacy to clients seeking Unemployment Insurance Benefits.

Over the past year, BDS has seen a dramatic increase in need for those seeking assistance with accessing unemployment insurance benefits. Specifically, our clients have encountered two recurring problems. First, we have received countless calls from unemployed New Yorkers whose unemployment insurance payments had suddenly stopped without them understanding why they had stopped or what to do about it. Second, we also heard from newly unemployed New Yorkers that although they had filed applications and were claiming every week, they were not receiving benefits and did not understand why.

Through our work with those clients, BDS has come to understand that these claimants have run headlong into the deployment of a new technological solution for identity verification. In response to concerns around fraudulent unemployment claims, a near majority of states onboarded the web-based identity verification program ID.me beginning in the spring of 2020. New York State was one of several states that bypassed the traditional RFP process and contracted for ID.me’s services in that time period.

The web-based product deploys “machine vision” and AI, as well as facial recognition technology, to provide identity verification services to the New York State Department of Labor (“NYSDOL”).
I. The Technology.

ID.me self-reports that they implement a four-step process to verify identity:

- **STEP 1:** Remote Document Verification
  - Scan driver's licenses, state IDs, and passports, and apply machine vision and AI to verify authenticity of document.

- **STEP 2:** Face Match
  - ID.me uses facial recognition to match the user's selfie to their uploaded government ID.

- **STEP 3:** Mobile Phone Verification
  - Verify that the SIM in the mobile device used for the verification is associated with the applicant's identity and screen for potential indicators of fraud.

- **STEP 4:** Multi-Factor Authentication
  - Secure accounts with Multi-Factor Authentication (MFA) options designed to accommodate all kinds of users.

The company publicly touts that it is in compliance with NIST 800-63-3’s identity proofing and authentication standards. The company has not publicly verified what facial recognition algorithm it is using for its 1:1 face matching, and has not publicly provided verification and validation data supporting either its document verification function or its facial recognition program.

Additionally, when a person is instructed to use ID.me to verify their identity, they are faced with a potential security risk. A google search for “ID.me” returns the company’s generic website. Through this website, New Yorkers are able to enter all of the required personal information—including identity documents and faceprints—into the generic ID.me website. The site does not warn visitors that it will not interface with that visitor’s relevant state agency.

In fact, numerous New Yorkers we work with, who proactively attempted to comply with the ID.me verification requirement, later learned that the generic site is not linked in any way with NYSDOL. Despite having submitted large amounts of private and biometric information to the government-designated private corporation, those New Yorkers experienced significant delays in identity verification, waited weeks or months to receive benefits they were owed, and were ultimately required to resubmit their information to a specific NYSDOL ID.me. Where all of that originally-submitted private and biometric information went has not been answered.

II. The Impact.

Unfortunately, the use of ID.me for identity verification has resulted in delays and denials causing New Yorkers serious financial and personal harm.

---

5 [https://www.id.me/business/government](https://www.id.me/business/government)

DEFEND • ADVOCATE • CHANGE
Document verification failures. ID.me’s process appears to apply an overly restrictive list of acceptable identity documents, but also fails to publicly provide the list of identity documents it will accept. Two examples:

a. ID.me provides no submission opportunity for name change orders. The failure to do so prevents transgender and gender-nonconforming claimants from verifying their identities.

b. ID.me rejects validly-issued but expired passports or identification documents, despite barriers to renewal posed by the COVID pandemic. This rejection has been specifically detrimental for claimants with foreign identity documents. Nothing in state or federal law prevents the acceptance of a validly-issued, but expired identity document as proof of identity.

Facial recognition failures. ID.me’s 1:1 facial recognition process appears to disproportionately reject the identity of women, transgender or gender-nonconforming, and BIPOC claimants. Two examples:

a. We have had to work with a number of claimants with darker skin tones to lighten their identity documents in order for ID.me’s algorithms to accept those documents. Similarly, we have had to work with claimants to ensure high levels of light in their spaces when attempting to interface with ID.me’s face scanning function. This failure of ID.me’s face recognition suite is not specific to ID.me, but a known risk for facial recognition projects. Despite this, ID.me has not publicly released any information about the actual performance of its face recognition suite.

b. We have heard from a number of claimants that they have been rejected by the face match scan with no explanation or instruction for correction. The vast majority of claimants experiencing these rejections have been Black women, transgender and nonconforming claimants, and people with darker skin tones. Without providing any data, verification/validation, or other studies, ID.me claims its algorithms are 99.9% efficacious. This kind of bald statistical salesmanship is both offensive and misleading to those who are being rejected by the system.

Error correction failures. ID.me allegedly provides access to a “Trusted Referee” via a mobile app to address any technical failures encountered in interfacing with the algorithms. The wait times for reaching these Trusted Referees have been days-to-weeks long.

---

Outright exclusionary barriers. ID.me’s process imposes exclusionary barriers to those in need of accommodation due to disability, language and literacy, or technology access and age.

a. Disability barriers: ID.me’s technological process does not provide appropriate accommodations for those with physical or mental disabilities. Reliant on text-based instructions, visual interaction, and technological literacy, ID.me’s identity verification becomes an insurmountable barrier for those requiring accommodation.

b. Language and literacy barriers: New York law and the NYSDOL’s own Language Access Plan require agencies to offer adequate translation and interpretation services for limited English proficiency (“LEP”) claimants. Although various languages are purportedly supported by ID.me, the available list is quite restrictive and many claimants who speak even the most common non-English languages in New York await an ID.me representative in their language for weeks.

Similarly, ID.me provides detailed written instructions, but those instructions are inaccessible for those who are illiterate, as well as for those whose English is limited. The only other available instructions available are a very brief outline in Spanish alone. As a result, LEP claimants and those with literacy barriers are more likely to experience wrongful delays or terminations of their benefits.

c. Technology access and age barriers: ID.me’s web-based process relies on a level of technological access and literacy that is inaccessible for many New Yorkers, particularly lower income New Yorkers and older individuals. State and federal law and administrative guidance consistently require public programs and services to be meaningfully accessible. We have repeatedly worked with claimants for whom the technological navigation of the system was a real and, at times insurmountable, struggle. As a result, lower income

---

and older claimants are more likely to experience wrongful delays or terminations of their benefits.

We have repeatedly seen claimants struggle to complete the ID.me process. The requirement to verify ID through a web-based platform without offering reasonable alternatives excludes these individuals from receiving benefits in a timely manner.

Please do not hesitate to contact us if you have questions regarding our comments. Thank you for your attention and considering our concerns.

Sincerely,

/s/ Elizabeth Daniel Vasquez
Elizabeth Daniel Vasquez
Director, Science & Surveillance Project