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.
Public Comment to RFI on Public & Private Sector Uses of Biometric Technologies

Respondent: Jonathan Barry-Blocker, Esq.
Respondent Type: Member of the Public
Respondent’s Professional Roles: Law professor, civil rights advocate

I submit this Comment in my personal capacity. My professional experiences inform my analysis. I practiced law for a decade in varied roles like state prosecutor, legal services attorney, and most recently as an impact litigator in Alabama with a prominent southern civil rights organization. Currently I teach and research law at a southern public university. My academic work focuses on civil rights and trial skills. Consequently, my Comment highlights biometric technology use and potential for abuse in the Deep South.

I will focus on biometric technology in correctional settings as incarcerated citizens are some of the least protected Americans. This comment neither disputes nor critiques the efficacy of biometric technologies. Instead, I discuss the lack of oversight and regulation in correctional settings in the Deep South, particularly Alabama.

I. Use of Biometrics in Correctional Settings to Identify & Control People

Alabama has the highest incarceration rate of any democratic government. And to sidestep substantial criminal justice reform or repair its aging prisons, the state plans to construct three (3) mega prisons. The state prison system suffers from severe understaffing with a 50% vacancy rate in June 2020. By June 2021, staff attrition increased the vacancy rate to 52%. Judge Myron Thompson confronted this issue in a recent 600-page opinion where he ordered the Alabama Department of Corrections (ADOC) to [again] boost staffing levels and protect incarcerated residents from violence. The state’s chronic failures precipitated the U.S. Department of Justice to file a separate suit against ADOC in 2020. But Alabama is perennially broke. It is unlikely ADOC will ever recruit sufficient people to operate the prisons, much less the mega prisons. Thus, I believe state leaders will rely heavily on biometric technologies to compensate for deficient staffing in these forthcoming facilities.

The use of biometrics in correctional settings is not new. Since 1999, some Florida jails relied on retinal scanners to track and confirm identities of incarcerated persons. In 2006 a “successful experiment” at Charleston’s naval brig recommended expanding biometric use in civilian correctional facilities to better track people. By 2015, a Georgia jail installed biometric locks that confirmed correctional officers’ fingerprints and heartbeats before they opened doors.

Alabama’s corrections facilities use these technologies. The Calhoun county jail added facial recognition to its arsenal of fingerprint and iris scan technology in 2012. That same year, ADOC extracted fingerprints from all visitors to state prisons, ostensibly to “verify identity at the door.”1 Years later the Madison county jail relied on Clearview AI’s systems to collect visual and auditory data. Most recently, the Etowah County jail in Alabama outfitted all cells and pods with fish-eye lens

---

1 Alabama was the first state to demand such biometric information from people not incarcerated.
cameras and hanging microphones in order to participate in a reality television show. After the show finished taping and aired, the jail did not remove the cameras and microphones. Neither residents incarcerated at the jail nor community members know whether they continue to operate. As one detainee shared with me, if the cameras and microphones still worked, the violence or inhumane conditions they recorded did not spur correctional staff to protect her and other women. And the jail has not updated its policies to account for the collection, retention, and use of this biometric information.

The technologies’ increased presence raise exploitative surveillance concerns. For example, consider voice prints. The Intercept reported:

[A]uthorities are acquiring technology to extract and digitize the voices of incarcerated people into unique biometric signatures, known as voice prints. Prison authorities have quietly enrolled hundreds of thousands of incarcerated people’s voice prints into large-scale biometric databases. Computer algorithms then draw on these databases to identify the voices taking part in a call and to search for other calls in which the voices of interest are detected. Some programs, like New York’s, even analyze the voices of call recipients outside prisons to track which outsiders speak to multiple prisoners regularly.

The article recounts corrections departments in Florida, Texas and Arkansas use the technology. Georgia’s prison system recently contracted for the technology. Even the Alachua county (Gainesville), Florida jail surveils jail calls. These technologies capture, analyze, and track all voices in a conversation. This includes non-incarcerated speakers, folks not subject to continuous government control. While all speakers may consent to having the prison/jail calls recorded, they do not consent to their voice patterns being seized, stored, and used for investigatory purposes ad infinitum and without limitation.

I believe Alabama, and likely other southern states, will use biometric technologies to track, manage, and investigate people housed in their prisons. These states will over rely on the technology due to chronic staffing shortages. And the state will provide scant oversight of ADOC’s use of biometric technologies.

II. Dearth of Security; Deficient Stakeholder Engagement in Policymaking and Lawmaking

States too poor to build prisons do not possess resources to protect sensitive biometric information. In 2012 U.S. Supreme Court Justice Sonia Sotomayor intuited it “may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily

---

2 The show – 60 Days In – is an A&E docuseries that plants volunteers as undercover detainees at a jail. The show records their interactions with incarcerated residents, jail staff, and visitors. The volunteers are tasked with obtaining evidence of questionable or illegal activities within the jail that correctional officers or surveillance systems may miss.

3 It is worth noting the Etowah county jail also doubles as an immigrant detention center.
disclosed to third parties.” Federal and state lawmakers, though, largely ignore her warning, especially in the Deep South.

In 2018, Alabama was the last state to enact a data breach notification law. A high-level cyber security professional with the city of Birmingham affirmed the state’s cavalier attitude. The official conceded the city lacked adequate protection against cyberattacks stemming from years of insufficient appropriations and political disinterest. Last year hackers proved him right when they breached surveillance systems at the Madison County jail in Alabama’s second largest city. The jail cameras used facial recognition to track detainees and correctional staff. Hackers viewed live footage and audio of detainees and interviews between law enforcement and suspects. Now, Mobile, the state’s third largest city, uses Clearview AI’s facial recognition technology. It is unknown if the city of Mobile suffered a similar breach. Authorities never addressed or mitigated the threat to exposed citizens’ privacy rights.

Disturbingly, Alabama refuses to enact consumer biometric and privacy protection measures like Illinois, Texas, California, and Virginia. Even though the state deployed biometric technologies for more than a decade in correctional settings. In late 2019 the state legislature authorized an artificial intelligence (AI) commission, the closest it has come to examining biometrics, to explore the presence and use of AI within the state. The commission’s report would guide lawmakers in regulating the technologies. However, as of early 2022, the commission has not issued a report. And even if it does in the future, the report would not lead to substantive lawmakers or equitable laws to protect Alabama citizens.

As an aside and further example, Alabama’s parole agency uses two risk assessment algorithms to determine parole decisions. The agency adopted these algorithms around 2016. State law requires the parole board audit these algorithms every three (3) years. Industry best practices recommend the state calibrate these algorithms to their incarcerated populations before use. Alabama flouts these laws and recommendations. I know the parole board never audited its algorithms. Nor did the parole board calibrate the risk assessment tools to the state’s populations. Nevertheless, the parole board continues to use these algorithms in parole decisions. Furthermore, ADOC also uses one of these risk

---

5 Birmingham is Alabama’s most populous city. Alabama Power and Regions Bank are headquartered there. The city is also home to the state’s best (and most) hospitals and specialty medical facilities.
6 Clearview AI has a well-documented history of violating privacy rights and exploiting biometric data. In 2021 Canada classified their biometric technology illegal after the company impermissibly collected Canadians biometric information. The country censured its national law enforcement for using the technology. Australia subsequently held the company violated national privacy laws when it covertly collected facial biometrics and incorporated them into its AI-powered identify matching service sold to law enforcement. And Britain’s data privacy authority fined Clearview AI $22.6 million for failure to comply with data protection laws.
7 Alabama had a Drone Task Force in 2014. The task force never issued a report. Instead it requested a state agency take over its tasks. The state agency seemingly abandoned the investigation. And the legislature never enacted any laws to regulate drones.
8 The AI commission’s membership is dominated by banking and business interests. A few academics and scientists are members. No consumer protection, indigency, or civil rights interests are represented in the membership.

Though the state legislature never enacted laws responsive to the drone task force, it recently proposed prohibitions on advocacy groups using drones to monitor unlawful pollution.
assessment algorithms on residents newly admitted to the state prisons. ADOC likely committed comparable regulatory violations. This is par for the course in Alabama.

Thus, the federal government should not presume states or localities in the Deep South will protect biometric information. And federal guidance or intervention is warranted given Alabama’s likely reliance on these technologies in its forthcoming mega prisons.

III. The U.S. has Tenuous Governance Regimes

Unregulated biometric technologies facilitate unlawful searches and seizures in correctional settings in contravention of the Fourth Amendment of the U.S. Constitution. A “search” occurs whenever the government or a government-assisted third party intrudes upon an individual's subjective expectation of privacy. A “seizure” occurs whenever the government or a government-assisted third party captures and retains an object or information possessed by an individual. For example, voice print technologies exploit ill-defined parameters of Constitutional and privacy laws. Neither federal nor southern state courts have addressed searches and seizures via these technologies in correctional settings. And most southern states have few, antiquated laws to “guide” technology users. Consequently, authorities and third parties must look to various Fourth Amendment decisions for guidance.

For example, in Ferguson v. City of Charleston, 532 U.S. 67 (2001), the U.S. Supreme Court repudiated the collection and selective drug testing of urine from pregnant [Black] women for forensic purposes. Hospital staff would test urine from women under suspicion of – but not arrested for – drug use. The hospital had a written agreement with local police, as well as supporting hospital policies, to surveil and report these pregnant women. The Court ruled searching urine for drug use was outside the scope to which women consented for their urine to be collected and tested at the hospital.

9 Though the U.S. Supreme Court decision Hudson v. Palmer, 468 U.S. 517 (1984) held incarcerated residents have no reasonable expectation of privacy in their jail cell, the Court did not address their bodily privacy rights. “Hudson merely concluded that the Fourth Amendment affords no protection for the prisoner's privacy interest in his cell or his possessory interest in his effects kept there, and thus arguably has no application to searches and seizures of the person of a prisoner.” See Wayne LaFave, Search And Seizure: A Treatise on the Fourth Amendment (5th ed. 2018), § 10.9(b), p. 416.

10 United States v. Dionisio, 410 U.S. 1 (1973) concerned voice exemplars collected in a grand jury investigation. The mass collection of voice files in correctional settings does not support ongoing or exigent criminal investigations.

11 Alabama is one of the few states without strong wiretapping laws. For the past few legislative sessions, the state Attorney General sought to pass expansive surveillance measure. It would authorize law enforcement to collect, track, and analyze aural and digital communications of any person or entity with suspected ties to illicit drugs. Civil rights organizations and their allies managed to stymie the bill. Also, most southern states refuse to enact strong privacy protection laws like Illinois’ Biometric Information Privacy Act (BIPA). Virginia’s new Consumer Data Protection Act is an anomaly.

12 These decisions have limited application to correctional settings. Each decision concerns arrest or pre-trial issues. Courts have not addressed biometric regulation/rights in correctional institutions.

13 Nearly all the surveilled women were Black and poor. Despite the common knowledge that Black people do not consume illicit substances at rates greater than other racial or ethnic groups.

14 As an aside, Alabama is the only state with a law that criminalizes pregnant women suspected of illicit drug use. Consequently, several county jails actively – and in the case of Etowah County aggressively – surveil the bodily fluids of women arrestees and detainees. Officers and jail nursing staff will collect and conduct warrantless pregnancy and drug tests on the women’s urine. These tests are done for forensic purposes solely. Unlike the South Carolina hospital in Ferguson, Alabama authorities largely target poor White women.
Like urine, voices are biometrics expelled from the human body. Voices should be protected from discriminatory warrantless seizure when participating speakers are not the subjects of open and active criminal investigations.

A decade later the Court seemed less sure of Fourth Amendment protections for biometrics. In *Maryland v. King*, 569 U.S. 435 (2013) the Court permitted police to obtain an arrestee’s DNA (via swabbing the inside of his cheek) and run it through the FBI’s DNA database. Authorities sought to identify Mr. King in other criminal matters. The Court minimized the invasion of privacy because law enforcement used minimally invasive means and did not reveal the arrestee’s genetic traits.

Not a year later the Court did an about face and conferred greatest protection to cell phones, which contain substantial biometric information. In *Riley v. California*, 573 U.S. 373 (2014) the Court prohibited law enforcement from conducting warrantless searches of a cell phone’s contents incident to arrest. Modern phones contain “the privacies of life” and are unlikely to contain information pertinent to immediate officer safety, destruction of evidence, or current criminal investigations. The Court foresaw warrantless searches would lead to pretextual searches and seizures of other private information, such as the trove of biometric information stored within the phone.

Four years later the Court went a step further in *Carpenter v. United States*, 585 U.S. __, 138 S.Ct. 2206 (2018). It extended Fourth Amendment protections to cell site location data generated by third-party cell phone providers. While this decision does not concern a biometric technology, it shows the Court’s willingness to protect personal information from government encroachment.

Like mobile phones, recorded conversations contain voice information of more than the person under government supervision. Other parties in a recorded call can include the non-incarcerated caller, children, and non-participants to the call.15 Analogous to the *Riley* decision, law enforcement and third-party contractors should not have unfettered authority to seize these voices from a recorded conversation.

Unfortunately, these high court decisions provide porous boundaries for government and government-assisted use of biometric information. The opinions do not address how citizens can access biometric data seized by the government or third parties. An issue that will paramount for people incarcerated, working in, or visiting Alabama’s three (3) new mega prisons.

One appellate decision from Florida touches on citizens’ access to biometric data. In *Lynch v. State*, 260 So. 3d 1166 (1st DCA 2018) (per curiam) an appellate court held a defendant is not entitled to comparison photos from a facial recognition software. Mr. Lynch sought the photos as potentially exonerating evidence pursuant to discovery rights conferred by the Fourteenth Amendment of the U.S. Constitution and *Brady v. Maryland*, 373 U.S. 83 (1963). He doubted the software sufficiently determined he was the man selling drugs in police photos. The photo identification was the basis for his arrest days after the drug transaction occurred. This was an issue of first impression for the state.

---

15 For example, food service personnel in a drive thru or eatery, business greeters, or other folks in the same room as a caller. None of these folks consented to a recorded phone conversation. None of them should have their voices searched and seized by authorities and third parties.
and possibly the nation. Even so, the court laconically and without noticeable precedential support reasoned since Mr. Lynch “cannot show that the other photos the database returned resembled him, he cannot show that they would have supported his argument that someone in one of those photos was the culprit.” The court further elided over the basis for arrest by highlighting “the jury convicted only after comparing the photo the officers too to Lynch himself and to confirmed photos of Lynch.” The Florida Supreme Court denied Mr. Lynch’s petition for discretionary review because the lower appellate decision did not conflict with other Florida appellate court decisions.16

The appellate court’s decision flew in the face of relevant state and federal case law regarding Brady material.17

Mr. Lynch could not have met this contrived burden without hacking the state’s files or receiving information from a mole within the police station. But the court conveniently ignored this reality. Victor Holder, Mr. Lynch’s appellate attorney, highlighted how lack of regulation permitted the outcome. “Florida law enforcement agencies currently use facial recognition technology with little to no public awareness, no uniform standards governing its use, and no public oversight by the Florida Legislature.”

While, no other court has relied on Lynch to determine a citizen’s right to biometric information do not presume other states will disregard the opinion. Alabama courts consistently adopt decisions from other southern or conservative states whenever controlling precedent is absent from Alabama’s common law.

IV. Conclusion

This Comment warns against relying on southern states to adequately regulate and protect biometric information.Too often these states treat emerging technologies as expediency measures. Even if the technology benefits the citizenry as well as the government, these states never enact protective laws. Alabama especially has a deplorable record of ineptly using biometric technologies. And their state lawmakers are prone to legislating emerging technologies (if at all) in an inequitable fashion. I do not believe the Alabama legislature will regulate biometric technologies once the mega prisons are constructed. Therefore, the federal government must establish clear guidelines for biometric technology use and the retention of any data.

17 See Floyd v. State 902 So. 2d 775 (Fla. 2005) (finding witness interviews that indicated an alternative perpetrator was Brady material; Rogers v. State, 782 So. 2d 373, (Fla. 2001) (finding that undisclosed police reports were “bedrock Brady materials;” as they “could have been used to show that another person” committed the crime, as reflected by the many witness descriptions matching an alternate suspect.”). See also United States v. Jernigan, 492 F.3d 1050 (9th Cir. 2007) (finding a Brady violation where prosecution failed to “disclose the existence of a phenotypically similar bank robber who had been robbing banks in the same area after Jernigan’s incarceration); Bradley v. Nagle, 212 F.3d 559 (11th Cir. 2000) (discussing Brady’s underlying policy and that even inadmissible evidence could lead to strong exculpatory evidence and therefore does not justify withholding it).