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 6, 2022

Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

RE: Request for Information on Public and Private Sector Uses of Biometric Technologies, Doc. No. 2021-21975, 86 FR 56,300

The Office of the Ohio Public Defender (“OPD”) submits this response to the Office of Science and Technology Policy’s request for information about public and private sector uses of biometric technologies. The OPD is the Ohio government agency “responsible for providing legal representation and other services to people accused or convicted of a crime who cannot afford to hire an attorney.”1 Our clients and the communities from which they come are disproportionately impacted by biometric surveillance, giving OPD a vantage point to address the efficacy of various regulatory efforts. The comments below largely stem from the OPD’s participation in the Ohio Attorney General’s Facial Recognition Task Force (“Task Force”) that was formed in 2019.

I. Introduction.

The government’s use of facial recognition software and other biometric technology to surveil people is a topic that generated intense debate in the state of Ohio. In 2019, the Columbus Dispatch reported that Ohio’s facial recognition dataset—containing 24 million driver license photos that are searchable by law enforcement2—may be accessible to local, state, and federal officials.3 These officials face a very low

---

burden before being authorized to conduct a search; they must simply claim a reasonable belief, based upon the totality of circumstances, that the search may result in an investigative lead.\textsuperscript{4}

The outcry generated by this news led Ohio Attorney General Dave Yost to temporarily suspend access to the dataset and he established a Task Force responsible for recommending regulatory measures for facial recognition use.\textsuperscript{5} The OPD was given one of two public defender seats on this 29-member Task Force. In January 2020, the task force sent 13 recommendations to Attorney General Yost with the goal of balancing “people’s privacy interests with the need for public safety while providing scrutiny and increased oversight.”\textsuperscript{6} To date, none of these recommendations have been acted upon.

Ohio’s failure to institute reforms to its biometric surveillance system, even when under intense media scrutiny, demonstrates one problem with allowing law enforcement agencies to self-regulate their access to databases of information. Either they don’t do it or they do so in ways that do not factor in other stakeholders’ perspectives.

But there are more profound problems than that: local and state actors are only able to regulate the datasets of facial images that they control. Even if the Ohio Attorney General placed stringent regulations on access to its own data, local and federal officers could create or access other datasets without similar guardrails. When considering the federal role in regulating public use of biometric technologies, the Office of Science and Technology Policy should bear in mind the complicated and overlapping patchwork created by the reality that facial recognition datasets are controlled at the local, state, federal, and tribal levels, and not every dataset is subject to the sort of self-regulation on which the Task Force was commenting.

As members of both the Task Force and the indigent defense community, we write to relay the need for a more comprehensive regulation of facial recognition technology by agencies and offices at all levels of government. Below, we address the following questions for which comment was requested:

- #1 Descriptions of use of biometric information for recognition and inference;
- #4 Exhibited and potential harms of a particular biometric technology; and
- #6 Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use.


II. Unregulated facial recognition can produce harm to individuals and communities.

The Task Force recognized that the government’s use of facial recognition technology can pose significant risks to civil liberties. These risks have been well documented by others so this letter will only briefly summarize them.

A. Issues with validity systemically impact accuracy of identifications.

A facial recognition search is a “two-part machine-human process” involving facial recognition (which is software-based) and facial comparison (which is human-based). Both software issues and human factors can negatively affect the accuracy of a facial recognition search.

- **Software and algorithmic concerns:** The facial recognition software used in Ohio, NEC-3, has one of the most accurate algorithms on the market, as tested by the National Institute of Standards and Technology (“NIST”). This means that the software is relatively better than its competitors at correctly pairing a photo in a dataset of known faces with a photo of an unknown person (also known as a “probe photo”). However, despite these high marks, facial recognition software generates both false negatives and false positives. False negatives—when the software fails to recognize a face—can range from 0.5% to over 10% depending on the software. Similarly, false positives—when the software incorrectly associates two different faces—exist at rates two-to-five times higher for women than men. False positives and negatives increase when probe photos have bad lighting, uneven angles, and when subjects are not directly facing the camera.

- **Human errors:** Humans impact a facial recognition search at multiple points in the process. First, humans choose the probe photo to run through a facial recognition dataset. Later, humans compare the probe photo to the database photo to confirm a putative match. Errors can exist at every point of human intervention. Law enforcement may manipulate probe photos before running a facial recognition search—in fact, officers have photoshopped out tattoos and even replaced a suspect’s photo with that of a celebrity lookalike. These manipulations may

---

7 Task Force Report, supra note 6, at 7 (Recommendation 1).
11 Id. at 7.
12 Garvie et al., supra note 8, at 47.
exacerbate algorithmic error. But this does not end the impact of human error. Humans must evaluate a probe photo against a menu of database photos of known people that are algorithmically generated as potential matches. Even with training in facial comparison, humans perform poorly at the task.\textsuperscript{15}

\textbf{B. The burdens of inaccuracy rest disproportionately on marginalized populations.}

The accuracy problems described above do not have equally distributed effects. The accuracy of facial recognition varies depending on sex, age, race, and skin color.\textsuperscript{16} If the software was not trained on diverse enough faces, the technology can struggle to identify a wide array of faces. For example, false positives are highest when analyzing Black and East Asian faces.\textsuperscript{17} False positives also tend to be higher for younger and older faces.\textsuperscript{18} False negative rates tend to be higher for Asian and Native American people, women, and younger people.\textsuperscript{19} False negatives are also generally higher for Black faces when the probe photo is low quality.\textsuperscript{20} Issues with the accuracy of facial recognition software compound the disproportionate and racialized impact of other policing practices.

\textbf{C. The speed at which facial recognition technology expands creates risks of additional unregulated surveillance in real time.}

Currently, facial recognition use in Ohio is limited to investigating events that happened in the past. But live, real-time facial recognition tools have emerged and are in use around the country.\textsuperscript{21} Use of real-time biometric technology amplifies accuracy concerns because of the risk that identification errors will be accompanied by split-second thought-processes on decisions including the choice to use lethal force. Additionally, the use of real-time facial recognition software has profound chilling effects on core constitutional rights including the right to assemble and protest.\textsuperscript{22}

\textbf{III. Our current patchwork system of regulating facial recognition is inadequate to protect against these harms.}

The OPD appreciated the opportunity to raise some of the harms articulated above as a member of the Task Force. But, in a regulatory space that has not yet been shaped by constitutional guardrails, even

\begin{itemize}
  \item \textsuperscript{16} \textit{See, e.g.}, Nat’l Inst. of Stds. & Tech., \textit{supra} note 10, at 2.
  \item \textsuperscript{17} \textit{Id.}
  \item \textsuperscript{18} \textit{Id.}
  \item \textsuperscript{19} \textit{Id.}
  \item \textsuperscript{20} \textit{Id.}
  \item \textsuperscript{22} Task Force Report, \textit{supra} note 6, at 8.
\end{itemize}
rigorous gatekeeping for access to a single state-run dataset of facial images will not materially shape law enforcement use of biometric surveillance in Ohio. And that has profound consequences for our clients, who are indigent, disproportionately people of color, more likely to live in communities subject to significant government surveillance, and at greater risk of suffering the harms generated by unregulated facial recognition use. Federal guidance can limit state overreach.

A. There is a lack of currently articulated constitutional guardrails in this space.

There is a nascent recognition in Fourth Amendment doctrine that digital surveillance is different from other government action, and that it requires more robust regulation. Most recently, the United States Supreme Court held that the government must obtain a warrant to obtain more than seven days of cell site location information (“CLSI”).\(^{23}\) This holding acknowledged the “deeply revealing nature of CLSI” and the “depth, breadth, and comprehensive reach” it provides into a person’s life.\(^{24}\) There are undoubted similarities between CLSI and facial recognition searches: both are deeply revealing about people’s whereabouts and are only possible because of the digital world in which we live. But Fourth Amendment jurisprudence has not yet reached biometric surveillance, and there is no guarantee that it will, let alone that it will do so in a way that considers the needs, rights, and civil liberties of people like the OPD’s clients.\(^{25}\)

B. In this constitutional murkiness, self-regulation is inadequate.

If the Constitution and courts are unable to effectively constrain use of biometric surveillance, self-regulation by executive agencies at local and state levels is equally unlikely to be effective. This is true for two major reasons. First, self-regulation is a wholly voluntary act. Second, even rigorous self-regulation by some executive actors is an ineffective way to regulate the law enforcement community.

1. Voluntary self-regulation is not an adequate check on executive power.

The Ohio Attorney General’s Task Force made consensus-driven recommendations after a deliberative process that included law enforcement officials, legislators, judges, professors, community stakeholders, and defense attorneys.\(^{26}\) One example of how compromise and consensus were reached is the Task Force’s recommendation regarding the amount of cause needed to authorize a facial recognition search. The existing standard requires only a reasonable belief that the search will lead to an investigative lead.\(^{27}\) The OPD argued for adoption of Michigan’s standard, which requires a showing of probable


\(^{24}\) Id. at 2223.

\(^{25}\) See, e.g., United States v. Tuggle, 4 F.4th 505 (7th Cir 2021); Andrew Gutherie Ferguson, Facial Recognition and the Fourth Amendment, 105 Minn. L. Rev. 1105 (2021).

\(^{26}\) Task Force Report, supra note 6, at 6.

\(^{27}\) OHLEG Rules, supra note 3.
cause before a facial recognition search.\textsuperscript{28} The Task Force ultimately recommended that facial recognition searches be authorized upon a showing of reasonable suspicion that the person to be identified has committed a crime.”\textsuperscript{29}

Because of the compromise-driven nature of the recommendations, significant gaps in the Task Force’s regulatory framework remain. The OPD has identified three fundamental concerns with the Task Force’s recommendations:

- The Task Force’s recommendations fail to require training for law enforcement users of facial recognition on cognitive biases. Such training should recognize that feature comparison methods that partially rely on human judgment remain vulnerable to the similar reliability concerns found in traditional eyewitness identification.\textsuperscript{30} Training alone will not render facial comparisons completely accurate, but these training efforts are consistent with current best practices for mitigating human errors during facial recognition processes.\textsuperscript{31}

- The Task Force’s recommendations do not provide strategies for mitigating the higher rates of mistaken matches among the young, women, and people of color.\textsuperscript{32}

- The Task Force’s recommendations do not propose an appropriate legal framework for facial recognition use that adequately respects the privacy interests of Ohioans, particularly given the sheer number of Ohioans whose photos are being searched. The modest limit proposed still permit law enforcement to run facial recognition searches for misdemeanors.\textsuperscript{33}

Highlighting the relatively lax guidelines proposed by the Task Force identifies part of the problem with self-regulation. The other reality is that these recommendations are unenforceable. The Ohio Attorney General published the Task Force’s recommendations nearly two years ago but has not acted on them. And even if the recommendations were adopted, they remain wholly voluntary. Absent legislative action

\textsuperscript{28} Task Force Report, \textit{supra} note 6, at 31.

\textsuperscript{29} Task Force Report, \textit{supra} note 6, at 4.

\textsuperscript{30} See President’s Council of Advisors on Sci. & Tech. (PCAST), \textit{Report to the President on Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods} 5, 31–32 (2016), \url{https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf}; see also \textit{In Focus: Eyewitness Misidentification}, Innocence Project (Oct. 21, 2018), \url{https://innocenceproject.org/in-focus-eyewitness-misidentification/}.


\textsuperscript{33} Task Force Report, \textit{supra} note 6, at 14.
or other checks and balances, even adopted recommendations could be rescinded administratively after a single high-profile crime.

2. *In a world where facial recognition searches can be done by using multiple private and government-owned data sets, regulation by data set is inadequate.*

Even if self-regulation had teeth, it would not meaningfully limit the impact of facial recognition on our clients’ lives. We represent clients all over the state of Ohio, in all stages of criminal cases. Our clients’ cases can involve state, local, and federal law enforcement, across several jurisdictions in a single case. The Ohio Attorney General’s regulations place limits only on how the OHLEG facial recognition dataset can be used. There are countless other databases of facial images that can be purchased or created by local law enforcement or used by federal law enforcement.\(^{34}\) State-level regulation may effectively articulate a set of political values, but it will have little impact on the use of facial recognition software on the ground in our clients’ cases.

A hypothetical can clarify this point further. Imagine that the Columbus Police Department, the Ohio Bureau of Criminal Investigation, and federal agents from the FBI and ATF work together in a multi-jurisdiction guns-and-drugs task force.\(^ {35}\) Imagine further that agents who work for the state government are bound by regulations that limit use of the OHLEG system to circumstances where there is reasonable suspicion that an unidentified, but photographed, person engaged in a gun or drug crime. Finally, imagine that the Columbus Police Department has no internal regulations and its own contract with a company, such as Clearview AI, that has access to private photo databases and an algorithm capable of searching those databases. Under these circumstances, the task force does not need reasonable suspicion to run a facial recognition search. It can simply use Clearview AI via the Columbus Police Department rather than the OHLEG database.

This holds true even outside multi-jurisdiction law enforcement teams. Even when the Columbus Police Department or federal agencies are working alone within the state of Ohio, they may access any database that is not controlled by the Attorney General without complying with OHLEG regulations. Any limitations imposed by a single jurisdiction can be easily circumvented.

IV. Conclusion.

It is an unqualified good thing that state government actors, including the Ohio Attorney General, are considering regulation of biometric technology such as facial recognition. Further, the inclusion of stakeholders like public defenders—whose clients are directly and harmfully impacted by this technology—should be applauded. But executive agency self-regulation in a space that includes private

---


databases, public databases, and multiple overlapping jurisdictions will have limited impact on the practical use of the technology. We write this comment to ensure this office has the perspective of public defenders and the clients we represent on this critical issue.

Sincerely,

Timothy Young
Ohio Public Defender