UNITED STATES DEPARTMENT OF JUSTICE'S WRITTEN TESTIMONY IN CONNECTION WITH THE UNITED STATES COMMISSION ON CIVIL RIGHTS' EXAMINATION OF CIVIL RIGHTS IMPLICATIONS OF THE FEDERAL USE OF FACIAL RECOGNITION TECHNOLOGY

March 21, 2024

The Department of Justice (Department) is pleased to submit the following testimony for the record for the U.S. Civil Rights Commission (Commission) public briefing titled "Civil Rights Implications of the Federal Use of Facial Recognition Technology." The Department submits this testimony in support and aid of the Commission's inquiry, consistent with the Department's long-standing and collegial working relationship with the Commission.

Executive Order 14074, Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety (the "Policing EO")—and in particular, Section 13(e), Ensuring Appropriate Use of Body-Worn Cameras and Advanced Law Enforcement Technologies —requires the Attorney General, the Secretary of Homeland Security, and the Director of the Office of Science and Technology Policy to jointly lead an interagency process to study the use by Law Enforcement Agencies (LEAs) of facial recognition technology, other technologies using biometric information, and predictive algorithms, as well as data storage and access regarding such technologies. As mandated by the EO, this ongoing process will produce recommendations for "safeguarding privacy, civil rights, and civil liberties, and ensuring that any use of such technologies is regularly assessed for accuracy in the specific deployment context [and] does not have a disparate impact on the basis of race, ethnicity, national origin, religion, sex (including sexual orientation and gender identity), or disability." The Department is prepared to provide updates to the Commission as more information becomes available, including completion of the reports and guidance mandated by the Policing EO.

This testimony also addresses the Department's current efforts to balance use of cutting-edge technologies to support the Department's mission to promote public safety and national security with avoiding misuse of such technologies in a manner that would undermine the Department's mission to protect civil rights.

The Department's Facial Recognition Technology Working Group and Interim Policy

In February 2022, in order to foster Department-wide consistency in the use of facial recognition technology (FRT) and ensure effective internal controls, the Department

launched the FRT Working Group, co-chaired by the Department's Office of Legal Policy (OLP) and the Office of Privacy and Civil Liberties (OPCL). The FRT Working Group, comprised of legal and operational subject matter experts from across the Department, met regularly throughout 2022 and 2023 to develop a policy to govern the use of FRT by Department components.

The FRT Working Group was tasked with developing an interim FRT policy with a framework centered on oversight, accountability, equity, and transparency. Announced by the Deputy Attorney General in December 2023, this interim FRT policy is consistent with recommendations from a September 2023 Government Accountability Office Report on Facial Recognition Services, as well as a mandate in the House Subcommittee for Commerce, Justice, Science and Related Agencies Appropriations Bill of 2022. The FRT Working Group continues to meet monthly to discuss next steps to promote successful implementation of the policy, including helping components develop their own policies and implement training.

As mandated by the Policing EO, the Department is continuing to work with the Department of Homeland Security (DHS), the Office of Science and Technology Policy (OSTP), and the Executive Office of the President (EOP) to examine law enforcement agency use of FRT and other technologies using biometric information, and the resultant impact on privacy, civil rights and liberties, and disparate treatment. This examination will result in a Report and Recommendations that offer guidance to federal, state, local, tribal, and territorial law enforcement agencies who use or seek to use, biometric technologies. The Department will update its "policies regarding the use of facial recognition technology, other technologies using biometric information, and predictive algorithms, as well as data storage and access regarding such technologies." Department efforts in connection with this EO mandate are being implemented by the Department's Emerging Technology Board (ETB).

The Interim Policy and Safeguards for FRT Acquisition and Use

The Interim FRT Policy prohibits unlawful use of FRT, provides guardrails to ensure effective and compliant use, and addresses the Department's FRT governance structure, including scope of FRT use, implementation, procurement, training, protection of privacy and civil rights, accuracy, the approval process for FRT use, accounting and reporting, and data retention.

The Interim FRT Policy requires that Department FRT systems be assessed for risk to accuracy across demographic groups, bias, and unlawful discrimination; that personnel using or approving FRT systems must receive required training on relevant legal and policy requirements; and that mandated training must include at a minimum, the terms of the Interim FRT Policy, the mandates of relevant privacy, civil rights, and civil liberties laws, and discussion of discovery obligations related to FRT use.

Notably, the Interim FRT Policy mandates that activity protected by the First Amendment may not be the sole basis for the use of FRT. This would include peaceful protests and lawful assemblies, or the lawful exercise of other rights secured by the Constitution and laws of the United States. Additionally, under this policy pursuant to the Department's anti-discrimination policies and other anti-discrimination laws, Department personnel "shall never use FRT to engage in or facilitate unlawful discriminatory conduct." Further, FRT systems must comply with the Department's policies on artificial intelligence. And "FRT results alone may not be relied upon as the sole proof of identity. An individual's identity must be confirmed through other analysis and/or investigation."

The Interim FRT Policy also requires any component that deploys FRT systems to develop a process to account for and track system use and provide an annual report to the ETB and the Department's Data Governance Board. Without compromising law-enforcement sensitive or national security information, each of these annual reports will be consolidated into a publicly released summary on the Department's FRT use. OPCL will report to the FRT Working Group, the ETB, and the Office of the Deputy Attorney General any complaints received through the existing privacy complaint process about use of FRT. These complaints will also be reported in the publicly released annual report summary.

In addition to the Interim FRT Policy, the Department has numerous policies that apply generally to the use of technology by the Department's components, including DOJ Order 0903, Information Technology Management, DOJ Order 0601, Privacy and Civil Liberties, and the Department's Artificial Intelligence Strategy. Some components, like the Bureau of Justice Assistance (BJA) in the Office of Justice Programs, have developed guidance documents with participation and support from stakeholders, including privacy advocates. As just one example, the 2017 Face Recognition Policy Template for State, Local, and Tribal Criminal Intelligence and Investigative Activities, which provides law enforcement, fusion centers, and other public safety agencies a framework for developing face recognition policies that comply with applicable laws, reduce privacy risks, implement minimum required training for authorized users and examiners, and establish entity accountability and oversight. Also, specific to BJA's Edward Byrne Memorial Justice Assistance Grant (JAG) Program, the largest grant-making activity in the Department, BJA employs a special condition in its awards to states, tribes, and local government for funding FRT projects.[1]

[1] Dep't of Just., Bureau of Justice Assistance Edward Byrne Memorial Justice Assistance Grant (JAG) Program Frequently Asked Questions (FAQs) p. 52 (June 2023), https://bja.ojp.gov/doc/jag-faqs.pdf ("[For] JAG funds to be used for Facial Recognition Technology (FRT), the recipient must have policies and procedures in place to ensure that the FRT will be used in an appropriate and responsible manner that promotes public safety; and protects privacy, civil rights, and civil liberties; and complies with all applicable provisions of the U.S. Constitution, including the fourth amendment's protection against unreasonable searches and seizures, the first amendment's freedom of

Furthermore, in deploying new technology, all Department components--including those involved in law enforcement—must comply with all applicable constitutional provisions, laws, regulations, and established policies. For example, the use of FRT is subject to Section 208 of the E-Government Act, and certain information acquired or generated attendant to use of FRT is governed by the Privacy Act of 1974.

AI Executive Order and the Emerging Technology Board

As referenced above, the Department established an Emerging Technology Board (ETB) to coordinate and govern artificial intelligence (AI) and other emerging technology issues across the Department. The ETB brings together designated officials from, among other components, the Department's Civil Rights Division, Office of Privacy and Civil Liberties, Office of Legal Policy, Executive Office for United States Attorneys, and law enforcement components to implement Executive Order 14110, issued on October 30, 2023, entitled "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (the "AI EO") by acting as the Department's "Artificial Intelligence Governance Board" mandated by the EO and guidances on its implementation from the Office of Management and Budget. The ETB also implements Executive Order 13960, issued on December 3, 2020, and entitled "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," by developing an AI use case inventory and evaluating use cases for consistency with principles of AI governance.

The ETB, which is chaired by the Department's recently appointed Chief AI Officer, will drive implementation of the above-identified Executive Orders, support coordination and governance of AI and other emerging technology issues across the Department, provide guidance to Department leadership, and advance information sharing across the Department regarding emerging technology-related best practices and use cases. It will ensure that we have a strategic plan to leverage the positive uses of AI to maximal effect while attending to its associated risks.

Additionally, consistent with AI EO's focus on implementation and enforcement of existing Federal laws to address civil rights and civil liberties violations and discrimination related to AI and other emerging technologies, starting in January 2024, the Civil Rights Division has begun convening regular meetings with the heads of civil rights offices and senior officials from multiple federal agencies to discuss the critical intersection of emerging technologies like AI and civil rights. During these meetings, agency representatives explore ways to leverage shared resources to address discrimination or other adverse impacts associated with AI and other advanced technologies.

---

association and speech, and other laws and regulations. Recipients utilizing funds for FRT must make such policies and procedures available to DOJ upon request." at p. 52).

The goal of the ETB is to ensure the Department remains alert to the opportunities and the attendant risks posed by AI and other emerging technologies. It will help guide Department leadership in advancing the Department's use of these technologies in a manner that is lawful and respectful of our nation's values; purposeful and performance-driven; accurate, reliable, and effective; safe, secure, and resilient; and understandable. The ETB will also promote information sharing and coordination across the Department and with interagency partners. The ETB will absorb the FRT Working Group as a subgroup of the ETB.

FRT at the Department

FRT can be used by federal law enforcement in multiple ways, including to help verify identity, associate biographic or other identifying information with facial images of unknown individuals, locate specific individuals within a set of images or videos, and determine how many people are depicted within sets of images or videos. It is an important tool for generating leads to help identify those who may have engaged in unlawful conduct, as well as to help exclude individuals from further investigation.

Currently, the Federal Bureau of Investigation (FBI) and United States Marshals Service (USMS) operate FRT systems. The Department's other law enforcement components, including the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Drug Enforcement Administration (DEA), and the Bureau of Prisons (BOP), do not currently operate FRT systems. USMS is party to a Memorandum of Understanding that allows it access to the Department of Homeland Security's (DHS) Information Network (HSIN), which enables access to the Multi-State Facial Recognition Community of Interest. While HSIN is not an FRT system, it allows authorized users to request indirect facial recognition searches through state and local entities, such as fusion centers. In addition, Department law enforcement components can receive leads from other federal, state, and local agencies that are generated by those agencies' use of FRT.

FBI

The FBI uses facial recognition technology to fulfill its mission to protect the American people in a manner consistent with the constitutional, statutory, regulatory, and policy frameworks that guide all FBI activities, in addition to the Department's Interim FRT Policy and component policies specific to the procurement, tracking, evaluation, and use of FRT. Over the last year, FRT has served as an important tool to assist the FBI in generating investigative leads and, when validated using other investigative techniques, FRT can play a key role in combatting crime and terrorism, as well as locating missing and endangered children, and addressing threats at our nation's border. It is crucial to public security that authorized members of law enforcement and national security agencies have access to advanced biometric technology and services like FRT.

Currently, the FBI is using commercial or third-party services that either are FRT systems or contain an FRT element, as well as its own FRT tools that were created by the Operational Technology Division and the Criminal Justice Information Services (CJIS) Division.

The FBI's Next-Generation Identification (NGI) system contains the Interstate Photo System (IPS). The NGI-IPS offers an automated search and response system targeted toward state and local law enforcement. Authorized law enforcement may submit a probe photo for a search against over 67 million arrest photos and receive a list of ranked candidates as potential investigative leads.

The FBI's Facial Analysis Comparison Evaluation (FACE) Operations Services supports authorized FBI assessments and investigations by enabling FBI personnel to submit requests for FR searches of FBI's NGI-IPS as well as FRT systems maintained by 17 state agencies and 2 other federal agencies with which the FBI has entered MOUs. Except for one state agency FRT system and one federal agency FRT system, FACE Operations Services personnel do not have direct login access—they only transmit requests to the applicable agencies who run the searches and return results, if any, back to FACE Operations Services.

All FRT use cases are reviewed by the FBI's Science and Technology Branch, Office of the General Counsel—including the Privacy and Civil Liberties Officer, and Office of the Chief Information Officer—including the AI Ethics Council. FBI users must obtain supervisory approval and complete training in facial comparison and identification before accessing and using any FRT service. The FBI's policies and procedures emphasize that photo candidates returned are not to be considered positive identifications but treated simply as leads.

The FBI is committed to responsible use of FRT that ensures appropriate respect for individuals' privacy and civil liberties and is compliant with all applicable law and policy. A variety of laws and policies prohibit the FBI from conducting investigative activity based solely on the exercise of constitutionally protected rights or the demographic characteristics of a person. The Attorney General's Guidelines for the FBI's Domestic Operations (AGG-DOM) and the FBI's Domestic Investigations and Operations Guide (DIOG) regulate the collection and use of all photos by the FBI, including FRT use. The FBI's use of FRT during an investigation must have a valid purpose consistent with the AGG-DOM and must comply with the U.S. Constitution and all applicable statutes, Executive Orders, and Department of Justice (DOJ) regulations and policies. Additionally, DOJ and FBI policy prohibits the use of FRT results as a means of positive identification or as the sole basis for an arrest. Instead, FRT results generate investigative leads that require further investigation to substantiate or invalidate those leads.

We strongly believe that FRT and other AI-enabled tools can greatly enhance the FBI's lawful investigative capabilities when used in a way that respects the constitutional rights of citizens. The FBI has and will continue to apply safeguards against the possibility for misuse, including approval and use requirements in their DIOG, limiting use of these systems to tip and investigative lead purposes only, incorporating human review of any results, and subjecting use to rigorous oversight, including review by the FBI's AI Ethics Council—all in compliance with the Department's Interim FRT policy.

USMS

The USMS uses FRT during its fugitive, missing child, and substantive criminal investigations and protective security missions. FRT is used solely to generate leads for the USMS within active fugitive investigations or other authorized criminal investigations and not for positive identification. Potential matches must be verified by USMS personnel via other investigative efforts and may not serve as the basis for taking any enforcement action (such as conducting an arrest or executing a search warrant) against an individual or premise or be directly relied upon in an application or affidavit to obtain court orders or warrants to further the investigation. In fugitive and missing child matters, where a person of interest has already been identified by the USMS as a criminal target (e.g., pursuant to the outstanding arrest warrant) or missing child (e.g., as identified by a state/local agency with the missing person matter), the FRT tool may be used to gather more information regarding the individual in question, such as identifying locations to conduct physical surveillance or social media platforms where the individual may be active and indicate their whereabouts. In protective operations, an individual who is a threat to a USMS protectee may be known or unknown at the time of the FRT search.

For several years, USMS has held a contract with Clearview AI, an "off the shelf" platform that includes a database of facial images sourced from public-only web sources, including news media, arrest photo websites, and public social media. Clearview's database only contains images from the internet that can be obtained without entering login information. More recently, USMS has executed an MOU that allows it to access DHS's HSIN and request indirect facial recognition searches through state and local entities, such as fusion centers. Because of the structure of USMS Task Force operations, which involve specially deputized Task Force Officers (TFOs), TFOs may have access to parent agency owned FRT systems or other systems. In circumstances where there is a demonstrated law enforcement need for the information, these systems may be accessed by TFOs following verification of their state/local law enforcement credentials.

Similar TFO access may occur within Task Forces operated by FBI, DEA, and ATF. In these cases, as a rule, the Department and its law enforcement components do not have direct access to other law enforcement agencies' FRT systems, and use of such systems would be for lead generation purposes.

FRT Testing and Research

The FBI works closely with the National Institute of Standards and Technology (NIST) on assessing FRT algorithms. The FBI employs robust auditing and established requirements to assess accuracy and to identify and mitigate potential deficiencies in these algorithms related to gender, race, and age. To ensure accuracy of facial recognition algorithms, the FBI has an interagency agreement with NIST to conduct independent third-party validation of the FBI's operational use of various FR technologies. On February 22, 2024, NIST released its latest Face Recognition Technology Evaluation (FRTE) reports. NIST found that accuracy of the current FBI algorithm for its NGI-IPS exceeded 99.88 percent when comparing a probe photo mugshot to a gallery of mugshots. When searching webcam images (i.e., a relatively unconstrained data set) against mugshots, the current FBI NGI IPS algorithm's accuracy exceeded 99.25 percent.

Rigorous testing and research also assess algorithm performance, including demographic differentials. In addition to NIST's January 2024 FRTE reports, the FBI has considered other research partner results, such as the 2023 United Kingdom National Physical Lab Report on FRT performance called, "Facial Recognition Technology in Law Enforcement Equitability Study" (March 2023), and other federally funded academic research and other efforts performed internally by government experts, such as "Impact of Blur and Resolution on Demographic Disparities in 1-to-Many Facial Identification" (January 2023), published by experts from University of Notre Dame and the Florida Institute of Technology.

In 2018, a team of scientists from NIST and three universities tested the accuracy of professional face identifiers in a study that constitutes the most comprehensive examination to date of face identification performance. Using a large, varied group of trained, professional face examiners and comparing the accuracy of state-of-the-art FRT algorithms against the human experts, the study determined that although the best machines performed in the range of the best-performing human experts, neither gets the best results alone; maximum accuracy was achieved only with collaboration between human and machine.

Findings from this research inform the FBI's practices in both automation (i.e., algorithm selection) and human review. For example, we have learned that algorithm accuracy may be reduced by poor quality facial images. This limitation has informed the FBI's position that FRT should only be used to generate potential candidates as investigative leads, all of which require manual adjudication by an individual trained to perform FR comparison and analysis based on their role.

Civil Rights Concerns

The mission of the Department is to uphold the rule of law, keep our country safe, and protect civil rights. Our use of any technology must foster public trust and confidence while upholding the Constitution and American values. Although FRT is an important and reliable technology, as with any law enforcement tool, misuse risks exacerbating shortcomings in certain policing approaches, including shortcomings that impact equity and fairness. As outlined in "Current Capabilities, Future Prospects, and Governance," the January 2024 Report of the National Academies of Sciences (Report), co-sponsored by the FBI and DHS, misuse of FRT occurs due to such factors as:

- FRT's low cost and ease of deployment
- Its potential for use by inexperienced and inadequately trained operators,
- Its potential for surveillance and covert use,
- The widespread availability of personal information that can be associated with a face image, and
- The observed differences in false negative (FN) and false positive (FP) match rates across phenotypes and demographic groups.

As discussed in the Report, use of FRT can have implications for equity and fairness:

- Some systems deployed in the U.S. are trained using datasets that are imbalanced and disproportionately rely on data from White individuals. As a result, these systems have higher FP match rates for racial minorities.
- Such systems can also provide law enforcement with a powerful new surveillance tool that can serve to reinforce patterns of or perceived need for elevated scrutiny, especially in marginalized communities, which may be compounded through law enforcement's use of reference galleries based on arrest photos.

At the same time, FRT and similar biometric tools have become essential to promoting public safety, including for identifying and locating missing children, fighting human trafficking, identifying missing and deceased individuals, and identifying perpetrators of crime. When employed correctly, FRT affirmatively strengthens our public safety system. FRT also strengthens our capacity to secure access to sensitive locations through identity verification.

For the Department, the key is ensuring that we have the right tools and expertise to leverage technologies like FRT and realize their benefits, while also ensuring that we have effective safeguards in place to mitigate potential harm. We understand and accept

our responsibility to lead when it comes to our own use and governance of FRT and similar biometric technologies.

CONCLUSION

The Department's Interim FRT Policy centers the Department's commitment to the rule of law and the protection of privacy, civil rights, and civil liberties. It is expressly designed to ensure fidelity to the principle that "the Department's use of FRT must comply with all applicable provisions of the U.S. Constitution, including the Fourth Amendment's protection against unreasonable searches and seizures and the First Amendment's freedom of association and speech, as well as other laws, regulations, Attorney General Guidelines, and Departmental and component policies." The Interim FRT Policy, which will be updated upon completion of the interagency best practices report required under the Policing EO , is designed to enable Department personnel to use FRT effectively, with care and subject to controls, while simultaneously protecting the privacy, civil rights, and civil liberties of the American people.