

November 25, 2025

Chief Privacy Officer Roman Jankowski
Department of Homeland Security
2707 Martin Luther King Jr. AVE SE
Washington, DC 20528-065

Dear Chief Privacy Officer Jankowski:

The undersigned organizations, which are dedicated to preserving privacy, civil liberties, and civil rights, write to you regarding the use of facial recognition technology by Immigration Customs and Enforcement (ICE). ICE field officers are reportedly using a smartphone application with facial recognition capabilities, known as Mobile Fortify, to identify people in the field and determine their immigration status.¹ As DHS has acknowledged, facial recognition is “inherently privacy sensitive” and its use (if it should be used at all) requires “safeguards for privacy, civil rights, and civil liberties.”² ICE’s current use of facial recognition technology in the field is dangerous, ripe for abuse, and undermines privacy, civil liberties, and civil rights.

ICE’s use of facial recognition in the field is especially troubling given the technology’s failings. Recent studies have shown facial recognition has higher errors rates for women and people of color.³ The majority of documented wrongful arrests due to misidentification by facial recognition have been of people of color.⁴ The technology is notably even less accurate when the images used are not of ideal quality—such as the images ICE likely obtains in field settings versus a controlled environment. The fact that ICE field agents are mainly using facial recognition on people of color virtually guarantees incidents of misidentification.

ICE’s reckless field practices compound the harm done by its use of facial recognition. ICE does not allow people to opt-out of being scanned, and ICE agents apparently have the discretion to use a facial recognition match as a definitive determination of a person’s immigration status even in the face of contrary evidence.⁵ Using face identification as a definitive determination of immigration status is immensely disturbing, and ICE’s cavalier use of

¹ Joseph Cox, *ICE and CBP Agents Are Scanning Peoples’ Faces on the Street To Verify Citizenship*, 404media (Oct. 29, 2025), <https://www.404media.co/ice-and-cbp-agents-are-scanning-peoples-faces-on-the-street-to-verify-citizenship/>.

² U.S. Dep’t of Homeland Sec., Directive Number 026-11: Use of Face Recognition and Face Capture Technologies (Sept. 11, 2023), <https://perma.cc/BTG6-BTQN>.

³ National Institute of Standards and Technology, *Face Recognition Vendor Test (FRTE) Part 3: Demographic Effects* (Dec. 2019); see also, National Institute of Standards and Technology, *Face Recognition Technology Evaluation (FRTE) Part 8: Summarizing Demographic Differentials* (May 11, 2023), https://pages.nist.gov/frvt/reports/demographics/nistir_8429.pdf.

⁴ Douglas MacMillian, David Ovalle, & Aaron Schaffer, *Arrested by AI: Police ignore standards after facial recognition matches*, Wash. Post (Jan. 13, 2025), <https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/>.

⁵ Cox, *supra* note 1.

facial recognition will undoubtedly lead to wrongful detentions, deportations, or worse.⁶ Indeed, there is already at least one reported incident of ICE mistakenly determining a U.S. citizen “could be deported based on biometric confirmation of his identity.”⁷

The undersigned are not aware of any other law enforcement agency in the U.S. that has a policy allowing facial recognition identification to be used as a definitive or final determination of any kind. Even other subcomponents of the Department of Homeland Security do not consider facial recognition results to be definitive. CBP, which developed Mobile Fortify, does not use facial recognition as a definitive determination of someone’s identity. Where there is an issue with a match, CBP will check other sources, namely federally issued identity documents.⁸ Similarly, TSA uses facial recognition for identity verification and will check federally issued identity documents when there is an issue with a match.⁹

Make no mistake, ICE’s use of facial recognition in the field would be just as disturbing even if the technology was 100% accurate. According to reports, the Mobile Fortify app is connected to troves of data that can be accessed via a “Super Query.”¹⁰ By pointing their phone at an individual for face identification, ICE can query various databases and obtain data related to “individuals, vehicles, airplanes, vessels, addresses, phone numbers and firearms.”¹¹ Such powerful surveillance technology at the hands of ICE field agents threatens privacy, civil liberties, and civil rights and will create a chilling effect on free expression and association. Videos online already show ICE agents aiming their phones at protestors, suggesting that ICE may already be using Mobile Fortify for surveillance of protestors engaged in constitutionally protected speech.¹²

The possibility ICE is using Mobile Fortify app to identify people exercising their First Amendment rights raises serious questions about the risks created by this app. The reality that ICE is using the technology as a definitive determination of immigration status is dangerously reckless and doesn’t align with the most recent, known DHS policy on the use of facial recognition, which states that “[facial recognition] technologies used for identification may not be used as the sole basis for law or civil enforcement related actions.”¹³

⁶ See National Institute of Standards and Technology, *Face Recognition Technology Evaluation (FRTE) Part 2: Identification* (Jan. 22, 2024), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

⁷ Jackie Llanos, *Feds blame U.S. citizen for his arrest under suspended immigration law* (Apr. 21, 2025), <https://floridaphoenix.com/2025/04/21/feds-blame-u-s-citizen-for-his-arrest-under-suspended-immigration-law/>.

⁸ *Final Rule with request for comment: Collection of Biometric Data from Aliens Upon Entry to and Departure From the United States*, 90 Fed. Reg. 48604, 48612 (Oct. 27, 2025), <https://www.govinfo.gov/content/pkg/FR-2025-10-27/pdf/2025-19655.pdf>.

⁹ The Privacy and Civil Liberties Oversight Board, *Use of Facial Recognition Technology by the Transportation Security Administration Staff Report*, 1 (May 9, 2025), <https://documents.pclob.gov/prod/Documents/OversightReport/90964138-44eb-483d-990e-057ce4c31db7/Use%20of%20FRT%20by%20TSA%2C%20PCLOB%20Report%20%285-12-25%29%2C%20Completed%20508%2C%20May%2019%2C%202025.pdf>.

¹⁰ Joseph Cox, *Inside ICE’s Supercharged Facial Recognition App of 200 Million Images*, 404media (July 17, 2025), <https://www.404media.co/inside-ices-supercharged-facial-recognition-app-of-200-million-images/>.

¹¹ *Id.*

¹² Joseph Cox, *ICE Is Using a New Facial Recognition App to Identify People, Leaked Emails Show*, 404 Media (June 26, 2025), <https://www.404media.co/ice-is-using-a-new-facial-recognition-app-to-identify-people-leaked-emails-show/>.

¹³ U.S. Dep’t of Homeland Sec., *supra* note 2.

Furthermore, ICE has failed to conduct a privacy impact assessment (PIA) specifically for Mobile Fortify. According to an available Privacy Threshold Analysis (PTA) of the Mobile Fortify app, a PIA is required, but CBP and ICE privacy officers determined that “existing privacy documentation is sufficient” to cover the use of Mobile Fortify.¹⁴ One of the relevant PIAs cited in the PTA assesses the Enforcement Integrated Database (EID). Ignoring whether the PIA is sufficient assessment of the privacy risks of the EID, it is a mistake to claim it is sufficient for Mobile Fortify. The EID PIA addresses the collection of biometrics on “investigation subjects and/or individuals subject to removal from the United States.”¹⁵ In other words, specific people known to ICE and for whom ICE uses biometrics to confirm their identity. In contrast, the Mobile Fortify app is being used on anyone ICE field agents happen to encounter and decide to run face verification on. The PTA for the Mobile Fortify app explicitly contemplates “collect[ing] information in identifiable form about individuals regardless of citizenship or immigration status” and retaining that data, including photos of U.S. citizens and Legal Permanent Residents, for 15 years.¹⁶ The PIA for EID does not address these types of uses of facial recognition in the field.

Given the dangers of facial recognition and ICE’s reckless use of it via the Mobile Fortify app, ICE should immediately stop its use of facial recognition in the field. The DHS Privacy Office should immediately release any privacy or other analysis the Office has performed related to ICE’s use of facial recognition in the field via the Mobile Fortify app. Additionally, the DHS Privacy Office must confirm whether Directive 026-11 is still DHS’s policy regarding the agency’s use of facial recognition technology, and if not, provide the current policy that governs its use.

If you have any questions, please contact Jeramie D. Scott, EPIC Senior Counsel, at jscott@epic.org.

¹⁴ Privacy Threshold Analysis: Mobile Fortify Application for ICE Enforcement and Removal Operations (May 12, 2025), <https://www.documentcloud.org/documents/26209262-mobile-fortify-pta/15>.

¹⁵ Dept. of Homeland Security, *Privacy Impact Assessment Update for the Enforcement Integrated Database (EID) – EAGLE, EDDIE, and DAVID* (May 14, 2019), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-eid-may2019.pdf>.

¹⁶ Privacy Threshold Analysis: Mobile Fortify Application for ICE Enforcement and Removal Operations, *supra* note 14.

Sincerely,

ACLU

Advocacy for Principled Action in Government

Amnesty International USA

Asian Americans Advancing Justice | AAJC

Center for Democracy & Technology

Center on Race, Inequality & the Law at NYU School of Law

Disability Rights Education and Defense Fund (DREDF)

Electronic Frontier Foundation (EFF)

Electronic Privacy Information Center (EPIC)

Equality California

Free Information Group

Free Press

Government Information Watch

Japanese American Citizens League

The Leadership Conference on Civil and Human Rights

The Legal Aid Society

Muslim Advocates

NACDL

New America's Open Technology Institute

Project on Government Oversight

Restore The Fourth

Secure Justice

Southern Poverty Law Center

Surveillance Technology Oversight Project

UnidosUS