United States Senate

September 11, 2025

Todd Lyons
Acting Director
U.S. Immigration and Customs Enforcement
500 12th Street, SW
Washington, DC 20536

Dear Acting Director Lyons,

U.S. Immigration and Customs Enforcement (ICE) is reportedly using a new biometric mobile phone application to surveil individuals in the United States, including U.S. citizens. This app reportedly allows federal agents to identify and retrieve vast amounts of information on a person, just by pointing a phone at their face. ICE is reportedly repurposing data held across federal and state databases related to "individuals, vehicles, airplanes, vessels, addresses, phone numbers and firearms"[1] and may even be planning to buy data from commercial data brokers for this app. Biometric scanning technology — such as facial recognition — is often biased and inaccurate, especially for communities of color, but even when accurate, this type of on-demand surveillance threatens the privacy and free speech rights of everyone in the United States, especially when weaponized against protesters and anyone who speaks out against the federal government's policies. ICE should immediately cease using this app and explain its policies and practices surrounding the use of biometric technology.

Although U.S. immigration authorities have previously used biometric scanning technology at the border and ports of entry,[2] ICE now appears to have deployed the technology on American streets. ICE has reportedly developed an app known as Mobile Fortify, about which it has released little information, including its purposes or limitations.[3] The app reportedly allows agents to point a smartphone at an individual's face or fingerprints and identify the individual based on a biometric match against several federal databases, including the Customs and Border Protection (CBP)'s Traveler Verification Service and the Seizure and Apprehension Workflow databases.[4] The app also appears to permit agents to conduct a so-called "Super Query" on people they encounter. This in-app functionality would apparently permit any agent to simultaneously query databases related to "individuals, vehicles, airplanes, vessels, addresses,

[1] 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/.

[2] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Traveler Verification Service*, (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

[3] Cox, *supra* note 1.

[4] *Id.*

phone numbers and firearms"[5] on any person they encounter in public, simply through pointing a phone at them. Super Queries reportedly pull data from the Federal Bureau of Investigation's National Crime Information Center database, the U.S. Citizenship and Immigration Services' Customer Identification Verification database, the Nlets system, and the CBP's TECS and Seized Assets and Case Tracking System databases.[6] ICE also appears to be considering linking data from commercial data brokers, such as LexisNexis, to the app.[7] Previous reporting has indicated that ICE purchases data such as an "individual's location, work history, family relationships, and many other data points" in its contract with LexisNexis.[8] The idea that federal agents can access such detailed, sensitive information on an individual, merely by pointing their phone at them, is chilling.

ICE's increased use of facial recognition tools inside the United States is particularly concerning given the known limitations of this technology. Most notably, despite recent advancements, facial recognition tools remain unreliable especially for communities of color,[9] which already suffer from increased surveillance and over-policing. Especially given ICE's recent expansion of its 287(g) program — which authorizes participating state and local law enforcement the authority to conduct immigration enforcement activities and has been proven to foster environments that increase racial profiling[10] — facial recognition tools are likely to be disproportionately weaponized against communities of color. A 2024 test by the National Institute of Standards and Technology found that facial recognition tools are less accurate when images are low quality, blurry, obscured, or taken from the side or in poor light — exactly the kind of images an ICE agent would likely capture when using a smartphone in the field.[11] In fact, in April 2025, ICE wrongfully detained a U.S. citizen for 30 hours in a county jail based on an incorrect "biometric confirmation of his identity."[12] This is unacceptable. With ICE expanding its use of facial recognition tools, mistakes such as this will almost certainly proliferate.

Moreover, even if ICE's facial recognition tools were perfectly accurate, these technologies would still pose serious threats to individual privacy and free speech. With this new tool, ICE agents can aggressively expand its biometric collection activities across the United

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

[6] *Id.*

[7] *Id.*

[8] Sam Biddle, *ICE Searched LexisNexis Database Over 1 Million Times in Just Seven Months,* The Intercept (June 9, 2022), https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances/.

[9] 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.

[10] American Immigration Council, *The 287(g) Program: An Overview, (July 8, 2021),* https://www.americanimmigrationcouncil.org/fact-sheet/287g-program-immigration/.

[11] 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.

[12] Jason Tapper, *Facial Recognition Is Getting a Lot More Invasive Under Trump*, Slate (June 6, 2025), https://slate.com/technology/2025/06/ice-facial-recognition-camera-surveillance-mistake-deported.html.

States. In fact, a recent video shows ICE agents pointing their phones at protesters, raising significant questions about whether the agency is already using facial recognition tools to surveil protesters.[13] In the absence of meaningful regulation of the government's use of facial recognition tools, the public is likely to be increasingly subject to ongoing, real-time surveillance. This Big Brotherism means that individuals may be less able to move, assemble, or appear in public without the federal government identifying and tracking them. As studies have shown, when individuals believe they are being surveilled, they are less likely to engage in First Amendment protected activities, such as protests or rallies — undermining the very core of our democracy.[14] Coupled with the Administration's recent actions — including the expansion of the 287(g) program,[15] expansion of fast-track removal process and third-country removals,[16] and ICE's increasingly aggressive enforcement tactics[17] — the use of these biometric tools raises significant concerns about possible misuse.

ICE's expanded use of biometric technology systems threatens a sweeping and lasting impact on the public's civil rights and liberties. To help us better understand ICE's use of this technology and its implications, please respond in writing to the following questions by October 2, 2025:

1. Please provide a detailed description of ICE's development and deployment of the Mobile Fortify mobile phone application.
    a. Please provide ICE's original intent and justification for developing the Mobile Fortify app.
    b. Who did ICE contract with to develop and deploy the Mobile Fortify app? Please provide the contract under which ICE obtained and uses the app.
    c. When did ICE first begin deploying the Mobile Fortify app on phones carried by ICE officers?
    d. Does ICE allow its officers to use the Mobile Fortify app for interior enforcement? If so, when did ICE first allow its officers to use the Mobile Fortify app in the field?
    e. How many ICE officers have access to a work phone with the Mobile Fortify app on it?

[13] Cox, *supra* note 1.

[14] Jennifer Lynch, *Clearview AI—Yet Another Example of Why We Need A Ban on Law Enforcement Use of Face Recognition Now*, Electronic Frontier Foundation (Jan. 31, 2020), https://www.eff.org/deeplinks/2020/01/clearview-ai-yet-another-example-why-we-need-ban-law-enforcement-use-face.

[15] U.S. Immigration and Customs Enforcement, Delegation of Immigration Authority Section 287(g) Immigration and Nationality Act: 287(g) Participating Agencies, (Aug. 19, 2025), https://www.ice.gov/identify-and-arrest/287g.

[16] Ashley Wu and Albert Sun, *How Trump Has Targeted New Groups for Deportation*, New York Times (May 30, 2025), https://www.nytimes.com/interactive/2025/05/21/us/trump-immigration-policy.html.

[17] *Trump says immigration authorities can arrest people at churches and schools*, The Guardian (Jan. 21, 2025), https://www.theguardian.com/us-news/2025/jan/21/trump-ice-churches-schools-hospitals-sensitive-areas.

f. Do any state or local law enforcement participating in the 287(g) program have access to a work phone with the Mobile Fortify app on it?

g. Before deploying the Mobile Fortify app, did ICE conduct any testing of its accuracy? If so, did that testing include using images that were low quality, blurry, obscured, or taken from the side or in poor light? If so, please provide those test results. If not, why not?

h. Is ICE conducting any ongoing testing or review of the app's accuracy when used by officers in the field? If so, please provide those results. If not, why not?

i. Has ICE conducted any legal review on the authority permitting the deployment and use of Mobile Fortify?

j. Has ICE conducted a privacy threshold analysis or privacy impact assessment for the deployment and use of Mobile Fortify, as required by the E-Government Act?

2. What are ICE's current policies, practices, and procedures governing use of the Mobile Fortify app? Please provide any written ICE materials reflecting them.

a. Under what circumstances are ICE officers permitted to use the Mobile Fortify app to attempt to identify an individual?

b. Are ICE officers permitted to use the Mobile Fortify app to attempt to identify an individual at a protest? If so, does ICE have any policies, practices, or procedures governing that use? If so, please provide any written ICE materials reflecting them. If not, why not?

c. Does ICE track its officers' use of the Mobile Fortify app to attempt to identify an individual, including frequency, location, date, and reason?

i. If so, how many times have ICE officers used the Mobile Fortify app to attempt to make an identification and how often has that attempt succeeded?

ii. Does ICE track identifications later established to be incorrect? If so, please provide figures for those incorrect identifications.

iii. Does ICE track how many of those attempted identifications, successful identifications, and incorrect identifications occurred at protests? If so, please provide those figures.

d. Have ICE officers used the Mobile Fortify app to collect information on individuals under the age of 18? If so, please provide detailed information on the locations, dates, and reason for the collection of information on minors.

e. Which databases does ICE use to compare images and other biometric information collected through the Mobile Fortify app, and what databases does the Mobile Fortify app pull information from for Super Queries?

i. What is the legal basis permitting the repurposing of data from each of those databases for use in Mobile Fortify?

ii. Are U.S. citizens included in those databases?

iii. If so, does ICE have any policies, practices, or procedures around the use of the Mobile Fortify app to identify U.S. citizens?

iv. Does ICE plan to expand Mobile Fortify to include information from data brokers, such as LexisNexis? If so, please describe the nature of the partnership and whether ICE officers will be able to use Mobile Fortify to query data on U.S. citizens from data brokers.

3. Please describe all the ways in which ICE uses identifications obtained through the Mobile Fortify app.
    a. For what purposes does ICE use identifications obtained through the Mobile Fortify app?
    b. Does ICE disclose to other federal entities or third parties information collected through the Mobile Fortify app or any identifications obtained through it?
        i. If so, which federal entities or third parties? Please describe the nature of any sharing agreement between ICE and these entities and third parties.
        ii. Does ICE impose any restrictions on those federal entities or third parties' use, retention, or disclosure of information or identifications obtained through the Mobile Fortify app?
    c. How long does ICE retain information collected through the Mobile Fortify app?
    d. How does ICE safeguard information collected through the Mobile Fortify app?
4. Will ICE commit to ending the use of the Mobile Fortify app? If not, why not?
5. Please describe in detail any additional facial recognition or other biometric identifications tools ICE uses.

Thank you for your attention to this important matter.

Sincerely,

Edward J. Markey
Edward J. Markey
United States Senator

Ron Wyden
Ron Wyden
United States Senator

Cory A. Booker
United States Senator

Tina Smith
Tina Smith
United States Senator

Elizabeth Warren
Elizabeth Warren
United States Senator

Chris Van Hollen
Chris Van Hollen
United States Senator

Bernard Sanders

Bernard Sanders
United States Senator

Jeffrey A. Merkley

Jeffrey A. Merkley
United States Senator

Adam B. Schiff

Adam B. Schiff
United States Senator