JUST FUTURES LAW

Mobile Fortify: The Facial Recognition App ICE Uses to Surveil Us What We Know

Immigration agents are using a new facial recognition app on their phones called Mobile Fortify to carry out street-level surveillance and real-time "identity checks" on community members. The app, which uses technology from NEC Corporation, is yet another tool that ICE (Immigration and Customs Enforcement) and CBP (Customs and Border Protection) use to justify sweeping arrests and racial profiling. Lawmakers have demanded ICE stop using Mobile Fortify, and Chicago and Illinois have sued the Dept. of Homeland Security (DHS) over its use of the app. This advisory provides a general overview of this facial recognition tool. Here is what we know:

How does the Mobile Fortify facial recognition app work?

Simply by snapping a photo of someone's face or finger in the app, immigration agents can quickly "identify" the person's name and other biographic information. [1] After a photo is taken, the app immediately compares the image against hundreds of millions of CBP or DHS records and looks for a "match." For example, the app apparently scans CBP's database of photos originally used for its Trusted Traveler programs, the Automated Targeting System (ATS), and the Traveler Verification Service. [2] These systems can access a vast quantity of biometric data including:

- Photos from TSA PreCheck, Global Entry, and other fast-track travel identity verification programs
- Photos and identity documents collected from passports, visa applications, airport security screening, airport cameras, and border ports of entry
- Photos from a so-called "Fortify the Border Hotlist" [3]
- Fingerprints and photos from DHS’s biometric database

If an ICE agent takes my photo with the app, what can they find out about me?

- If the app identifies a "match" (which could be inaccurate), the app will show information about the person sourced from various databases. [4] The personal information may include:
  - Name, photo, birth date, gender, nationality
  - Immigration and citizenship information, including: A-number, possible citizenship status, possible visa overstay status, biometric data (fingerprints, photos), and immigration judge decisions, including whether they have a deportation order.
  - Information about family members (it is not clear what this includes)
  - Note: reports state that Mobile Fortify can also pull data from the FBI, Dept. of State, and other federal & state databases, which may mean agents can see license plate numbers, vehicle registration data, phone numbers, addresses and more. [5]

  - If the app does not identify a "match" to an existing facial photo or fingerprint in the government databases, it will not show additional information about the person.

What if the app says I am someone that I am not?

- The app has misidentified people, and the app also pulls from databases that may have inaccurate data.
- ICE officials have stated that they consider an identity "match" in Mobile Fortify to be a "'definitive' determination of a person's [citizenship] status and that an ICE officer may ignore evidence of American citizenship—including a birth certificate" if the app indicates otherwise. In other words, even if you were to provide evidence of citizenship, ICE officials have stated that they will defer to the determination of the app.

What do they do with my data?

ICE uses Mobile Fortify to significantly *expand* its arsenal of biometric surveillance data on people, including noncitizens and citizens.

- If ICE or CBP takes your photo or fingerprint in the app—regardless of whether the app "identifies" you—DHS saves the new image of you in their system for 15 years, along with information about the exact location where the image was taken (geolocation data).
- ICE may be able to catalog your photo and add it to a list of people to target or surveil. For example, there are reports of agents using Mobile Fortify and telling protesters that "their faces would be added to a database." There are also reports of people having their TSA PreCheck privileges revoked shortly after ICE subjected them to face recognition surveillance.

Who are they targeting with the app?

- Federal agents have used the app over 100,000 times. ICE can target anyone with this coercive, punitive surveillance—including noncitizens, US citizens, children, protesters, etc. DHS states that ICE does not allow people to "decline or consent" to the app's surveillance.

Can local police use the app?

- CBP made a version of the app for local law enforcement agencies that coordinate with ICE on immigration enforcement via the 287(g) program. This version of the app reportedly does not give officers detailed information on people. Instead, after snapping a photo, the app directs officers to release the person or contact ICE, thereby creating more potential opportunities for ICE to detain and deport community members. It is not clear which police departments (if any) are using the app, and it is no longer available on Google's app store.

Endnotes

[1] DHS' AI Inventory states that the Mobile Fortify app can also be used to scan photos of identity documents. In addition to facial recognition and fingerprint recognition technology, the app uses character recognition technology to scan text.

[2] Through ATS, the app has the capability to pull data from ICE's deportation database, USCIS (US Citizenship and Immigration Services) databases, FBI NCIC (National Crime Information Center), and the Dept. of State's consular processing system, though it is not clear whether the app has the capability to query and match photos from those systems. The app can also reportedly search data from Nlets, which could include, for example, driver data from states' Dept. of Motor Vehicles.

[3] It is not clear who is targeted on this list. See DHS reference to this list here.

[4] It is not clear whether Mobile Fortify reveals identity information for anyone with a photo or fingerprint "match" in government databases, including US citizens, or only for people with immigration violations or a deportation order. DHS states that the app will show someone's biographic information "If the individual encountered matches a photograph from the Fortify the Border Hotlist" (without defining who is on this list, how people get added to it, etc.). DHS also states that immigration agents may use the app to collect information about people "regardless of citizenship or immigration status." In addition, reports indicate that the app conveyed to federal agents that someone was a US citizen, suggesting that the app may reveal identity information about US citizens and noncitizens.

[5] There are reports that the Mobile Fortify app could soon source data on people not only from government databases, but also from commercial databases, such as those sold to ICE by data brokers like LexisNexis, and from social media surveillance companies. Among other things, commercial surveillance data could potentially allow ICE agents to not only "identify" the individual in front of them using the app, but also to see a map of their friends, family and contacts.