COMMITTEE ON HOMELAND SECURITY

H.R. XXXX, the "Realigning Mobile Phone Biometrics for American Privacy Protection Act"

Introduced by
***Rep. Bennie G. Thompson**, Ranking Member, Committee on Homeland Security*

Originally cosponsored by
***Rep. Lou Correa**, Ranking Member, Subcommittee on Border Security & Enforcement*
***Rep. Shri Thanedar**, Ranking Member, Subcommittee on Oversight, Investigations & Accountability*
***Rep. Yvette Clarke**, Chair, Congressional Black Caucus*
***Rep. Grace Meng**, Chair, Congressional Asian Pacific American Caucus*
***Rep. Adriano Espaillat**, Chair, Congressional Hispanic Caucus*

Immigration and Customs Enforcement (ICE) has deployed an unproven biometric mobile phone application to identify a person by capturing their face or fingerprint through a phone camera. The application, Mobile Fortify, utilizes Customs and Border Protection (CBP) systems, such as the Traveler Verification Service, to identify a person and their citizenship or immigration status. Congress has long had concerns with the Federal government's use of facial recognition technology—including bias, inaccuracy, and the erosion of privacy and civil rights and civil liberties—and has regularly conducted oversight of how DHS utilizes such technology. The Mobile Fortify application has been deployed to the field while still in beta testing, which raises further concerns about its accuracy. Additionally, until December 2025, CBP had made a different facial recognition application, Mobile Identify, available to state and local law enforcement that work with ICE on immigration enforcement, raising substantial concerns about civil rights and civil liberties.

H.R. XXXX, the *Realigning Mobile Phone Biometrics for American Privacy Protection Act* would reign in DHS's use of Mobile Fortify and Mobile Identify to better protect privacy, civil rights, and civil liberties by requiring a Department-wide standards and guidelines:

- prohibiting the use of these mobile phone applications except for identification at ports of entry,
- prohibiting DHS from sharing these applications with non-DHS law enforcement agencies,
- requiring these applications be removed from DHS information technology outside ports of entry,
- making DHS render these applications inoperable on any non-DHS information technology,
- requiring the destruction of any image, photograph, or fingerprint of a U.S. citizen captured on these applications before the standards and guidelines under this bill are implemented, and
- requiring that within 12 hours of being taken through the use of these applications, any image, photograph, or fingerprint of a U.S. citizen be destroyed.