ELECTRONIC FRONTIER FOUNDATION

TSA Modernization Act

Face prints, fingerprints, and retina scans—all of these sensitive biometric markers and more could be captured from travelers by the government at checkpoints throughout domestic airports.

The TSA Modernization Act (S. 1872), sponsored by Senator John Thune (R-SD), would authorize the U.S. Transportation Security Administration and U.S. Customs and Border Protection to deploy "biometric technology to identify passengers" throughout our nation's airports, including at "checkpoints, screening lanes, [and] bag drop and boarding areas."

TSA and CBP's alarming vision of pervasive biometric surveillance at airports cuts against the right to privacy, the "right to travel,", and the right to anonymous association with others that are hallmarks of our democratic country. The invasive data collection proposed by this bill would invade the privacy of countless innocent Americans and foreigners, and the dangers of collecting sensitive biometric data on these travelers far outweigh any potential benefits.

Mission Creep

Congress initially authorized a biometric data collection exit program for foreign visitors, supposedly to help track visa compliance. However, CBP is currently subjecting all travelers, including U.S. citizens, to face recognition screening on certain outgoing international flights. This bill would expand that authority to allow CBP and TSA to collect *any* biometrics they want from *all* travelers—international *and* domestic—wherever they are in the airport.

The data collected from these programs—your fingerprint, the image of your face, and the scan of your iris—will be stored in FBI and DHS databases and can be searched again and again for immigration, law enforcement, and intelligence checks, including checks against latent prints associated with unsolved crimes. In addition to the significant accuracy problems with face recognition software, especially for non-white and female travelers, these databases, such as arrest warrant databases, are often riddled with errors and inaccuracies.

Security Risks

Face recognition is a unique threat to our privacy, because our faces are easy to capture and hard to change. Face images may be captured covertly, from a distance, at high speed, and on a large scale. When the government gathers sensitive biometric information, it creates a honeypot of information that could be misused by identity thieves or even government employees abusing their access privileges.

As we saw with the 2015 Office of Personnel Management data breach and the 2017 Equifax breach, no government agency or private company is capable of fully protecting your private and sensitive information. But losing your social security or credit card numbers to fraud is nothing compared to losing your biometrics. While you can change those numbers, you can't easily change your face.

Congress should uphold individual privacy by rejecting the TSA Modernization Act or any similar biometric surveillance expansion program.

Want more information?

Please contact Legislative Analyst India McKinney at **india@eff.org**.