“Facial Recognition Technology (Part II): Ensuring Transparency in Government Use”
House Committee on Oversight and Reform
10:00 AM, Tuesday, June 4, 2019
2154 Rayburn House Office Building
Rep. Gerald E. Connolly (D-VA)

Mr. Chairman, thank you for holding today’s hearing to examine how federal agencies are engaging with facial recognition technology. Several federal agencies are already using this technology to carry out national and public safety missions. As we discussed at this committee’s previous hearing on this topic, use of facial recognition technology must be done transparently and it is Congress’ role to provide ongoing oversight and, if needed, create a stator framework to protect Americans’ civil rights. I look forward to hearing from our nation’s law enforcement agencies about the benefits of biometric technology. We must have a robust discussion about the consequences of adopting this technology.

In some cases, the federal government’s adoption of facial recognition technology can lead to innovative solutions, efficient processes, and enhanced security. For example, the Customs and Border Protection (CBP) is using facial recognition technology to improve the flow of international travelers. In 16 U.S. airports, including the Washington Dulles International Airport located in my district, CBP uses facial recognition technology to screen inbound international passengers. This biometric entry and exit system creates a paperless process for passengers and screeners by scanning faces against a database of passport and visa photos, and it allows travelers to get through airport security more efficiently. The primary benefit of this program is increased security. Allowing technology to manage routine and repetitive tasks for the majority of international travelers enables CBP officers to focus their energy on uncommon but potentially dangerous security threats. With the promise of this new technology, however, comes valid concerns about data collection and privacy implications and whether the benefits of this technology outweigh costs to individual civil liberties. The tension between security and individual freedoms are essential questions to our society and prompt us as a committee to carefully oversee agency use of technologies that can be easily abused by an overzealous Administration.

The Transportation Security Administration (TSA) is also using facial recognition technology in airport screening. In September 2018, TSA released its Biometrics Roadmap, which outlines a path to screen the general population of domestic travelers. While I support the adoption of new technology, we must ensure that all new programs are rolled out in a transparent manner and, when it is appropriate, allow individuals to opt out. When implementing facial recognition programs, agencies should establish standards to notify private citizens when facial recognition technology is used and whether it is mandatory. The Washington Post recently reported on TSA’s pilot program to use biometric technology in Atlanta. Of the 25,000 daily passengers routed through this terminal, only about 2 percent of travelers opted out of the option to submit their face to scanning and identification. This low opt out rate raises questions about whether travelers are sufficiently aware of their participation or its implications.

Additionally, we must regulate the extent to which federal agencies share individuals’ personal information with the private sector. TSA’s collaboration with the airline industry could be helpful for promoting the most efficient use of the technology and streamlining security and ticketing lines for airline customers. The federal government, however, puts its citizens at risk when it shares access to a traveler's personal data with the private sector, even temporarily.

Questions over facial recognition technology's accuracy continue to cloud its potential benefits. While the Federal Bureau of Investigation (FBI) praises its increased capabilities to combat crime and terrorism, a 2016 Government Accountability Office (GAO) study criticized the FBI for not properly assessing the technology's performance. GAO noted that the FBI had not assessed the frequency of false positive rates with their software nor conducted sufficient testing to ensure accuracy. The report recommended six actions the FBI should take to improve the transparency, accuracy, and privacy of its facial recognition systems. Unfortunately, three years after the initial report, GAO still lists these actions as part of the DOJ's high-priority open recommendations. The FBI must commit to closing those recommendations and taking steps to make its operations and use of facial recognition technology more transparent.

Technology has and will continue to improve the lives of every American. But with new technology, come new responsibilities to curb possible abuses. Facial recognition technology could revolutionize American air travel. But only if we take careful steps to roll out new technologies carefully, transparently, and thoughtfully. I look forward to working with my colleagues on both sides of the aisle to find a balance between the risks and rewards of facial recognition technology.