COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Statement of Chairman Bennie G. Thompson (D-MS)

About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies

July 10, 2019

The government's use of biometrics is not entirely new. For example, fingerprints have been used as an identification tool for many decades. Other biometrics include DNA, irises, voice patterns, and palm prints. In recent years, facial recognition has become the new, chosen form of biometric technology. As facial recognition technology has advanced, its use by the government and the private sector has also increased. Currently, DHS is collecting and storing several different kinds of biometric information and is using this information for multiple purposes. CBP and TSA are using biometrics to confirm the identities of travelers, for example. The Secret Service is piloting a surveillance system using facial recognition. I am not opposed to biometric technology, and recognize it can be valuable to homeland security and facilitation. However, its proliferation across DHS raises serious questions about privacy, data security, transparency, and accuracy. The American people deserve answers to those questions before the federal government rushes to deploy biometrics further.

Last month, the Committee held roundtable discussions with both industry and privacy and civil liberty stakeholders about the Department of Homeland Security's increasing use of biometric technology. Stakeholders have significant concerns about the data DHS is collecting and whether the Department is safeguarding our rights appropriately. They have good reason to be concerned. Absent standards, Americans may not know when, where, or why the Department is collecting their biometrics. People also may not know that they have the right to opt out, or how to do so. Worse yet, they may not know that biometric technology is in use, as is the case when face recognition is used to passively surveil a crowd like under the Secret Service's pilot program. Recent reports also indicate ICE has been scanning through millions of Americans' drivers' license photos without their knowledge or consent. These troubling reports are a stark reminder that biometric technologies should only be used for authorized purposes in a fully transparent manner.

Data security is another important concern. Frankly, the Federal government does not have a great track record securing Americans' personal data, and biometric information can be particularly sensitive. Unfortunately, earlier this year, a CBP subcontractor experienced a significant data breach, including traveler images, raising important questions about data security. Americans want to know that if the government collects their biometric data, they are going to keep it secure from hackers and other bad actors. Moreover, the accuracy of certain biometric technology is in question, despite advancement in recent years. Studies by highly regarded academic institutions have found facial recognition systems in particular are not as accurate for women and darker-skinned individuals. Last July, the American Civil Liberties Union (ACLU) conducted a test using Amazon's facial recognition tool called "Rekognition." The ACLU built a database of 25,000 publicly available arrest photos. Using Rekognition, the ACLU searched the database using pictures of every current Member of Congress. The software incorrectly matched 28 Members with individuals who had criminal records. Although the misidentified members included both Democrats and Republicans, men and women, and a wide range of ages, nearly 40 percent of the false matches were people of color. This is unacceptable.

It is not fair to expect certain people in our society to shoulder a disproportionate burden of the technology's shortcomings. Before the government deploys these technologies further, they must be scrutinized and the American public needs to be given a chance to weigh in. Biometrics and facial recognition technology may be a useful homeland security and facilitation tool, but as with any tool it has the potential to be misused – especially if it falls into the wrong hands. Today, the Committee will hear from Federal witnesses on this important topic. I am pleased that we have witnesses from Customs and Border Protection (CBP), the Transportation Security Administration (TSA), the Secret Service, and the National Institute of Standards and Technology (NIST) before us. They represent just a few of the agencies involved in the government's increasing use of biometric technology. I look forward to hearing from them about how they are using biometric technology currently, their plans for the future, and what they are doing to address these concerns. As Congress, it is our job to ensure they protect the rights of the American people before they move forward.

# # #

Media contact: Adam Comis at (202) 225-9978