U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Opening Statement

Chairman Bill Foster (D-IL)
of the Subcommittee on Investigations and Oversight

Investigations & Oversight Subcommittee Hearing:
Privacy in the Age of Biometrics

June 28, 2022

Good morning, and welcome to our members and our panelists. Thank you for joining us for this hearing on securing privacy in the age of biometric technologies. Biometric technologies have made great strides in recent years, and offer a convenient upgrade to many security measures, from opening your smart phone with a fingerprint to passing through Customs with a face match.

Much of the discussion around biometrics has revolved around the serious deficiencies in the ability of facial recognition technology to accurately match non-white, female, and young faces. These discrepancies have been a legitimate obstacle to fair, equitable implementation. And in the past few years, much work has gone into closing these gaps, particularly at the National Institute of Standards and Technology. Accuracy across demographic groups has improved dramatically. While facial recognition researchers and companies should continue to address remaining racial bias in their algorithms, we on the Science Committee should explore the next frontier of problems that accompany the inevitable expansion of biometric technologies.

The utility of biometric technologies are surely understood by everyone in this (virtual) room. We are constantly opting in to lend our biometric information to make our lives that much easier – unlocking our phone with our masked faces, accessing bank accounts with our voice, and perhaps you've even visited a grocery store that used facial recognition technology for easy check-out. And when you opt in to these uses, there is a baseline expectation that your information will be used as intended. Informed consent and regulations on data storage and sharing are important pieces of the puzzle. Illinois's Biometric Information Privacy Act, for example, is currently the most protective law on the books in the United States. The ACLU successfully settled with facial recognition company, Clearview AI, for violating the rights of Illinois residents, and the company must now offer residents an opt-out mechanism. Today our focus will be on how technological solutions can secure our privacy while allowing us to enjoy the benefits of biometric tools.

Biometric privacy enhancing technologies can and should be implemented along with biometric technologies. So-called B-PETs can be implemented at the point of capture, improving the precision of collection tools to ensure they are not picking up features that are not necessary for use. They can insert obfuscations on the data collected, degrading the quality of the information

or introducing statistical noise so the biometric data is unusable for unintended uses. A technique called template protection can ensure that one system's biometric information is encrypted such that it cannot be read by another system – for example, someone's image obtained from the security system at a doctor's office, for example, cannot be linked to their workplace's identity verification system.

Federal agencies – including NIST, who is represented at this hearing today, as well as DHS's Science and Technology Directorate – are already working to develop and improve privacy-protective technologies for biometric technologies. The America COMPETES Act, which I am helping to conference with the Senate, contains a number of provisions that will future-proof the government's definitions and standards for biometric identification systems and invest in privacy enhancing technologies. I look forward to hearing from our panel about how we can further invest in these protections as biometric technologies become more and more prevalent in our daily lives.

The timing of our discussion today is notable. In overturning Roe v. Wade, the Supreme Court has substantially weakened the Constitutional right to privacy. States attempting to criminalize access to medial care may try to use biometric data to prove where someone has been and what they did there. This makes protecting Americans' biometric data more important than ever.

I now yield to Ranking Member Obernolte for his opening statement.