COMMITTEE ON SCIENCE SPACE & TECHNOLOGY
REPUBLICANS

Opening Statement of Ranking Member Jay Obernolte as Prepared for Delivery

Investigations and Oversight Subcommittee Hearing – Privacy in Biometrics

June 29, 2022

Good morning. Thank you, Chairman Foster, for convening this hearing. And thanks to our witnesses for appearing before us today.

The purpose of this hearing is to discuss the benefits and risks of biometric technologies and to explore research opportunities in privacy-enhancing technologies for biometric applications. I hope today's hearing will be a productive discussion that will help us learn ways to improve biometric technologies for the future.

Once confined to the world of science fiction, biometric technologies have become integrated into our daily lives. From unlocking an iPhone with a fingerprint or face scan, to asking Alexa or Siri what the weather is, to boarding an airplane, biometric technology is everywhere, and it is rare to go a day in 2022 without interacting with some form of biometric technology.

The benefits are clear: when used well biometrics give us easier authentication, more secure logins, and personally customized interactions with technology.

Given the prevalence of biometrics, I am particularly glad to have Dr. Charles Romaine from the National Institute of Standards and Technology (NIST) here with us today to tell us more about the important work NIST is doing in this space. NIST has been conducting biometrics research and development for over 60 years, and in the 1960s, NIST helped the Federal Bureau of Investigations (FBI) with work on fingerprint technologies to support law enforcement and forensics.

Today, NIST conducts research projects as well as testing and evaluation of several biometric modalities including fingerprints, face, iris, voice, and DNA.

Additionally, NIST is also engaged in biometric standards development at the national and international level. Standards and their guidance are important to enable the exchange of biometric data between agencies and their systems; provide guidance on how biometric systems are tested and performance is measured; define methods for assessing the quality of biometrics; and to ensure government systems work well together.

NIST's role in researching biometrics technologies and establishing standards and guidance will not only drive advances in how we use biometrics, but also give us a better understanding of the potential security and privacy risks associated with them.

Biometrics are no different than many advanced technologies in that their misuse can harm individuals – in this case by compromising their privacy or the security of their information. Biometrics are a tool, and like any tool, they can be used to benefit individuals, or to harm them.

As policymakers, we need to be acutely aware of the risks associated with this technology, especially covert collection and the issue of individual consent to have one's information stored and used.

However, we must also balance that awareness against the potential benefits that biometrics bring to society. Were we to adopt a draconian approach that effectively prevents the development and use of biometrics, we would lose these valuable benefits—and not just the airport and smartphone convenience I mentioned earlier.

Biometric technologies have extraordinarily helpful applications. For example, Ukraine's defense ministry is using Clearview AI's facial recognition technology to recognize Russian assailants and identify dead combatants. Marinus Analytics' tool Traffic Jam uses facial recognition and AI to detect patterns in sex-trafficking ads to help law enforcement identify victims.

If government takes an overly heavy-handed approach to regulating biometrics technologies, we'll lose out on life-saving applications like these.

I have seen this approach firsthand. I was a Member of the California State Legislature during the early days of facial recognition, before its risks and benefits were well understood, and we considered a lot of misguided proposals that would have effectively banned the use of facial recognition technology. It is much easier to push for legislation to outlaw a technology entirely than it is to conduct due diligence and try to intelligently balance its benefits against its risks.

That's why NIST's work is so valuable. Better understanding of the technology and carefully developed standards and guidelines will help us develop biometrics in a way that provides safeguards without stifling innovation.

I'm looking forward to learning more about that work today.

Thank you, Chairman Foster, for convening this hearing. And thanks again to our witnesses for appearing before us today. I look forward to our discussion.

I yield back the balance of my time.