<u>Opening Statement</u>
Ranking Member Daniel Lipinski

Committee on Science, Space, and Technology
Subcommittee on Research
The Current and Future Applications of Biometric Technologies

May 21, 2013

Good morning. I want to thank Chairman Bucshon and Chairman Massie for holding this joint hearing to examine the use of biometric technologies. I'd also like to thank our witnesses for being here today. I'm looking forward to your testimony.

Right now, biometric technologies are used mostly by federal, state, and local governments to identify criminals and to ensure our national security. Most people equate biometrics with fingerprints. This is because fingerprints have been used for more than a 100 years and automated recognition systems have been commercially available since the 1970s. In fact, the FBI has 110 million fingerprint records, the Department of Defense has 9.5 million, and the Department of Homeland Security has 156 million fingerprints in their database.

But the landscape for biometric technologies is changing and other technologies are being rapidly deployed in other countries. For example, India is in the process of collecting biometric information for every single resident. They have already enrolled more than 300 million people and they are not just collecting fingerprints, but also iris scans. Efforts such as these could help combat fraud and waste, but also raise significant civil liberties concerns.

Advances in facial recognition are being driven largely by companies such as Facebook and Google who are using facial recognition algorithms to "tag" people on social media.

All of these technologies have their own advantages and disadvantages. For example, a suspect won't leave their iris scan behind at the scene of a crime as they would a fingerprint, but it appears that the characteristics of the iris remain more stable over a person's lifetime.

The bottom line is there is enormous potential for these technologies, but there are also a number of research gaps. There are many questions and gaps of a scientific or technical nature. For example, as I mentioned earlier, it appears that the characteristics of the iris are fairly stable over time, but biometric technologies rely on the distinctiveness of an individual and there is a need to build up our fundamental understanding of how biometric traits vary not only between people, but as an individual person ages.

But there are also many research questions related to the social and cultural aspects of biometrics. As I am sure we will hear today, a biometric system is only as good as the quality of data it collects. Even when a person is a willing provider of their biometric data, there is variation in the quality of that information let alone when a person is non-compliant or they are actively trying to deceive the technology. Understanding how a person interacts with a biometric sensor and what impact social or cultural beliefs have on that interaction is key to obtaining quality data. For example, a person may be reluctant to touch a sensor out of a “fear of germs” or their religious beliefs may not permit them to show their face in public.

As my colleagues are well aware, I have been passionate about the need to secure cyberspace. I often comment on the fact that most people use a few passwords for all of their online activities from banking to streaming movies. We all know that using the same password is not what we should do, but we do it anyway because it is just easier. Unfortunately, that password can be forgotten, guessed or stolen.

Biometric technologies hold the potential to significantly increase cybersecurity because it is much more difficult to steal someone’s fingerprint or a scan of their iris and you generally don’t forget your finger at home, but these technologies are not widely deployed in the private sector.

The National Institute of Standards and Technology is trying to address this through the National Strategy for Trusted Identities in Cyberspace, but there is still a lot of work to be done. Part of this is because most biometric systems cost too much for commercial applications and there is no compelling business case for such an investment.

Also, I, like most Americans have some concerns about how the use of biometric technologies affects my privacy. I hope to ask the witnesses some questions about the security and privacy of biometric technologies later this morning.

I am especially interested in learning more about the sharing of biometric data and the potential for secondary uses of these technologies.

Mr. Chairman, I believe the potential of biometric technologies to enhance our security is great and worth pursuing, but I also believe we need to make certain that there are appropriate safeguards in place so these technologies are not abused.