

COMMITTEE ON
**SCIENCE, SPACE, AND
TECHNOLOGY**
CHAIRMAN LAMAR SMITH



For Immediate Release
May 21, 2013

Media Contacts: Kim Smith Hicks, Zachary Kurz
(202) 225-6371

**Statement of Research Subcommittee Chairman Larry Bucshon (R-Ind.)
Hearing on “The Current and Future Applications of Biometric Technologies”**

Chairman Bucshon: Good morning, I would like to welcome everyone to this morning’s hearing on the current and future applications of biometric technologies. I look forward to our witnesses’ testimony on how this technology is developing and the ways biometrics might better the lives of my constituents and every American.

Many of us have been introduced to biometric technologies through by way of movies and TV shows - James Bond-style spy thrillers and the ever-present mega-vault secured with iris and palm scanners. While these examples portray a high-tech, futuristic technology that has little application to the average person, the reality is that biometric technologies have been utilized over the last two decades in many industries and fields. Whether being used to enhance security by controlling physical access to facilities or preventing fraud by controlling electronic access to computer networks, these practical applications affect everyone on an individual and collective scale. This includes safeguarding our international borders and protecting financial transactions, which is essential as technology rapidly advances and our world becomes more dependent on cyber infrastructure.

Just last week, the Department of Homeland Security released a solicitation seeking information on commercially available live scan fingerprint systems for possible use by federal, state, and local law enforcement agencies. Additionally, they are researching ways for quicker identification by developing tablet-based technologies that can capture biometrics at the scene of a crime.

Biometric research done by the National Institute of Standards and Technology, also known as NIST, dates back to the 1960’s – starting with fingerprint identification technology the FBI used to support law enforcement.

Today, NIST continues their research in developing uses and enhancing different types of biometric technologies, including fingerprinting, face and iris scanning, voice recognition and DNA testing. Biometric technologies are often touted as a democratic approach to identity management, because no language, gender, age, race, financial status, or literacy rate impedes their use. Because of this, many see biometrics playing a major role in fixing the so-called “identity gap” many developing countries face. For example, India has implemented a robust biometric identification program with the hopes of reducing fraud and corruption, ensuring credible elections, and improving national security.

Additionally, biometric supporters point to the consumer’s convenience of using biometric technologies. Many ask, why must we continue to carry key fobs, remember passwords, and enter personal identification numbers when we can use uniquely personal physical patterns in place of additional items? Researchers at the University of California-Berkley are developing a biometric security that uses brain waves to replace passwords—calling them “passthoughts.”

But with praise also comes concern. Such as, how can we ensure biometric data is secure and being used appropriately?

My colleagues and I are looking forward to learning about the positive impacts biometric technologies might have in increasing convenience in our everyday lives and improving our personal and national security, while having an open discussion about policy implications and addressing the concerns that some might have. We have an excellent panel of witnesses ranging across industry, academia, and government to lead our discussion.

I would like to extend my appreciation to each of our witnesses for taking the time and effort to appear before us today. We look forward to your testimony.

###