U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEES ON RESEARCH AND TECHNOLOGY

The Current and Future Applications of Biometric Technologies

Tuesday May 21, 2013
10:00am-12:00pm
2318 Rayburn House Office Building

Purpose

On Tuesday, May 21, 2013, the Subcommittees on Research and Technology will examine the current development and state of biometric technologies, and the challenges of adopting biometric technology. The hearing will also focus on the practical applications of biometric technologies, future uses of the technologies, and how their use impacts public policies.

Witnesses

- **Dr. Charles H. Romine**, Director, Information Technology Laboratory, National Institute of Standards and Technology
- **Mr. John Mears**, Board Member, International Biometrics and Identification Association
- **Dr. Stephanie Schuckers**, Director, Center for Identification Technology Research

Background

The term biometrics is an umbrella descriptor for the various methods of identifying individuals using unique aspects of the body—the most common being fingerprints. There are a number of unique biometric indicators such as handprints, vein dimensions, iris and retina detection, body odor, voice, and gait detection. Currently biometric identification technologies are most commonly used to secure facilities, protect computer network access, counter fraud, border protection, and fighting crime. Biometric security utilizes 'what you are' to authenticate individuals, as opposed to 'what you know' such as a password.

Basics of Biometric Technology

Biometric technologies work to confirm the identity of an individual by comparing patterns of physical or behavioral characteristics in real-time against a database of the pattern(s). The device that captures the biometric marker creates an electronic digital template, which is encrypted and stored and then serves as comparison for authenticating future personal identification inputs. These templates are generated from algorithms, which aim to prevent the reconstruction, decryption, and reverse-engineering of an individual's identity.

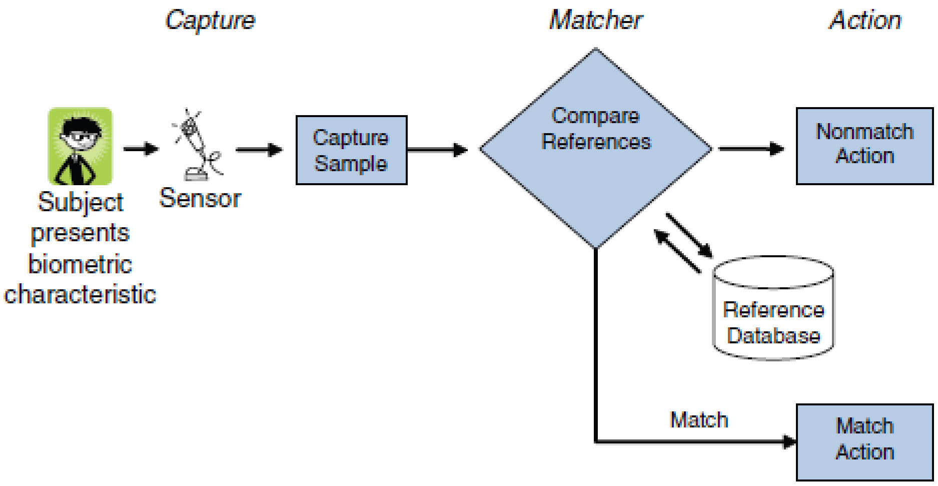

FIGURE S.1 Sample operation of a general biometric system. The two basic operations performed by a general biometric system are the capture and storage of enrollment (reference) biometric samples and the capture of new biometric samples and their comparison with corresponding reference samples (matching). This figure depicts the operation of a generic biometric system although some systems will differ in their particulars. The primary components for the purposes of this discussion are "capture," where the sensor collects biometric data from the subject to be recognized; the "reference database," where previously enrolled subjects' biometric data are held; the "matcher," which compares presented data to reference data in order to make a recognition decision; and "action," where the system recognition decision is revealed and actions are undertaken based on that decision.[1]

State of the Technology

Many biometric technologies are already mainstream, publicly-available technologies. For example, Facebook employs facial-recognition software that eases name tagging of uploaded photos, Apple's Siri uses voice recognition to operate smartphone and tablet functions, theme parks use fingerprints to identity season pass holders, and some hospitals and school districts use biometrics to identify and manage patients or students.

Biometric Legislation

Currently there are very few laws that directly govern the use of biometric systems or the storage of biometric templates; however, there are several privacy laws that reference approved biometric methods for a variety of industries. Several bills have been introduced and referred to committees in the 113th Congress that would incorporate the use of biometric technologies in identify individuals, such as Medicare beneficiaries, agricultural workers, and visa holders.[2] Below is a list of existing laws that include some provisions specific to biometric policy.

[1] WHITHER BIOMETRICS COMMITTEE, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 2, National Research Council of the National Academies (2010).

[2] *See* H.R. 418, 113th Cong. (2013); H.R. 242, 113th Cong. (2013); H.R. 300, 113th Cong. (2013).

Health Insurance Portability and Accountability Act 1996 (HIPPA)

HIPPA mainly addresses the way personal health information is managed and administered, but a number of provisions address data security. Title II of HIPAA, the Administrative Simplification provisions, required the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. Biometric technologies were among the technologies that complied with the regulations for secure access to electronic medical records. Other technologies include: Secure Password, Biometric, PIN, Token and Telephone Call Back.

The Sarbanes-Oxley Act of 2002

The Sarbanes–Oxley Act of 2002, passed in response to a number of major corporate and accounting scandals, established enhanced financial standards for all U.S. public company boards, management, and public accounting firms. Biometrics offers the ability to control access to financial data, to ensure compliance with the act when properly implemented, and to provide best practices for firms that are affected by the law.

Gramm-Leach-Bliley Financial Modernization Act of 1999

The Gramm-Leach-Bliley Act requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. Protecting the privacy of consumer information held by financial institutions is at the heart of the Gramm-Leach-Bliley Act's privacy provisions. Biometric technology utilizing multi-factor authentication can form the basis for compliance with this Act.

Issues for Examination

The Subcommittees will examine the potential benefits biometric technologies can provide the American people, while also considering the potential policy implications of biometric implementation. Specifically, the hearing will explore the current state of biometric technologies and future applications that may transform the lives of Americans—while determining the challenges of implementing biometric technologies.