TESTIMONY OF

Dr. Stephanie A. C. Schuckers
Director, Center for Identification Technology Research
Professor of Electrical and Computer Engineering, Clarkson University

BEFORE THE

United States House of Representatives
Committee on Science, Space and Technology
Subcommittee on Research and Subcommittee on Technology

The Current and Future Applications of Biometric Technologies
PRESENTED
10 am, May 21, 2013

Chairman Bucshon, Chairman Massie, Ranking Member Wilson, Ranking Member Lipinski, Members of the Committees. Thank you very much for the opportunity to testify to you today.

My name is Stephanie Schuckers. I am a Professor in Electrical and Computer Engineering at Clarkson University and Director of the Center for Identification Technology Research (CITER), a National Science Foundation Industry/University Cooperative Research Center. I have been working in biometrics since 1997 and in biomedical applications since 1992. I am currently serving as the Vice President of Finances for the IEEE Biometrics Council. It is my pleasure to give some comments on the current state and the future of biometric technology, particularly as it relates to research.

In our society with the ubiquity of electronic mediums, there is a need to establish a trusted relationship between individuals and between individuals and organizations in order to support electronic commerce (including mobile transactions), worker and employer interactions, delivery of benefits from governments, movement of individuals across international borders, social connections, and delivery of quality healthcare. There are many ways to establish a trusted relationship. These include:

- What you have? (birth certificates, drivers licenses, credit cards, passports, key)
- What you know? (passwords, PINs, mother's maiden name, address, email, phone number, Social Security Number)
- Who you are? (personal traits, biometrics)

Biometrics is defined as "automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics" [1][2]. Secure trusted transactions in the past have primarily relied solely on what you have and what you know. The addition of biometrics adds

another dimension of security that was previously only available in limited cases. This new layer not only promotes security but also reduces the burden on individuals to provide additional information.

There has been a decade of dramatic expansion of biometrics for government and commercial applications. These large programs, supported by academic and industrial research and development, have demonstrated the usefulness of biometrics as one component in the processes needed to establish identity as part of a trusted relationship. For example, every day during the morning rush hour, over 12,000 people enter the Pentagon building. The Pentagon Force Protection Agency uses biometrics integrated with other identity credential methods to control the access into Pentagon facilities [3] [4] [5]. In another example, the trusted traveler program, Nexus, which is used by over 650,000 people at 19 border locations [6][7], reduces the hurdles of border crossings. A higher level of scrutiny initially allows less examination at repeated crossings, in part, because a biometric is provided. In the Next Generation Identification (NGI) system of the FBI, fingerprint search reliability is over 99% with response times under five minutes, when compared against a repository of over a 100 million persons, according to The National Biometrics Challenge report in 2011 [7].

One emerging area is the use of biometrics as part of authentication to support transactions over the internet. E-commerce totals over $180 billion dollars in sales in the US alone, with projections of over 7% growth per year [8][9]. Mobile payment systems are developing that will contribute to the rise in electronic payments. Presently replacement of a lost password requires the need to reveal additional information. Combining password authentication with a biometric reduces the amount of private information that would need to be revealed repeatedly in order to re-establish the trusted relationship. Depending upon the transaction, multiple levels of trust can be created by combinations of different forms of authentication.

Creating and enabling trusted relationships makes it more difficult for those who seek to undermine and destroy that trust through cybercrime, terrorism, and identity theft. Over 5 million individuals are estimated to be victims of identity theft per year. A recent Federal Bureau of Investigation report stated that "identity theft has emerged as a dominant and pervasive financial crime that exposes individuals and businesses to significant losses and undermines the credibility and operation of the entire U.S. financial system." [10] Similarly, in our counterterrorism efforts, knowledge of the individual is a critical aspect to sorting out the minority of individuals who seek to do us harm. Biometrics is one critical tool in a large toolbox of ways to identify them.

Center for Identification Technology Research (CITeR)

The Center for Identification Technology Research (CITeR) is a National Science Foundation Industry/University Cooperative Research Center focusing on biometrics [11]. CITeR was founded in 2001 by West Virginia University (WVU). CITeR, currently led by Clarkson University, also includes University of Arizona, The University at Buffalo, and several partner schools including Michigan State University.

CITeR functions as a **cooperative** of academic, industrial, and government organizations. Over twenty affiliates, define, fund, and oversee work to meet common mission needs. Affiliates include the Federal Bureau of Investigation (FBI), Department of Defense (DOD), Department of Homeland Security (DHS), systems integrators, technology providers, and small businesses. Projects are defined by faculty through ***interfacing*** with affiliates and ***integrating*** research needs. Projects are chosen by affiliate vote and reviewed at meetings held twice a year. Through this process of concept development, the speed of innovation is increased as ideas are ***shared*** at the definition stage, rather than at the traditional publication stage. Additionally, these close connections between academia and industry promote translation of research to industry, further stimulating innovation and leading to the creation of jobs. In addition to commercial uses of biometrics to support authentication, translation of research leads to products being more rapidly put in the hands of operational users, such as police, border agents, and forces.

The focus of CITeR is human measurement and identification, with core foundations of trust, security, reliability, and privacy. The research strives to build a comprehensive theoretical, analytical, and empirical framework within which the performance of tools can be modeled, predicted, and tested. Research being conducted in CITeR include the foundations of biometric science, statistical modeling, security, privacy, novel biometrics, computational models, unconstrained biometric recognition, and multi-biometric fusion [11].

Outcomes from CITeR include shared datasets, software tools, academic papers, and students graduating with Bachelor's, Master's and PhD's with expertise in biometrics formed through CITeR-funded projects. CITeR seeks to increase the participation of students from under-represented groups in Science, Technology, Engineering, and Mathematics (STEM) disciplines by engaging them early in the pipeline. Biometrics naturally fascinates students given its unique nexus of security, engineering, and biology.

Based on my interactions within CITeR, my own research endeavors, and my knowledge of the larger biometric community, in the following paragraphs I summarize some of the research challenges I see in biometrics for current and future applications.

While these topics are outlined below, more detail can be found in reports such as the The National Biometrics Challenge from 2011 by the *National Science and Technology Council (NSTC)* Subcommittee on Biometrics and Identity Management [7], *National Science Foundation* Workshop on Fundamentals Research Challenges in Biometrics hosted in 2010, Biometric Recognition: Challenges and Opportunities by the National Research Council [21], other reports [1,10,11,12], and professional organizations such as the *IEEE Biometrics Council*.

Identity Management

Identity management (IdM), as defined by the 2008 Identity Management Task Force Report, is "the combination of technical systems, rules and procedures that define ownership, utilization and safeguarding of personal identity information. The primary goal of the IdM process is to assign attributes to a digital identity and to connect that identity to an individual." [12] Biometrics, as a component of identity management, is an automated methodology for connecting the stored personal information to the identity of an individual through physiologic or behavioral measurements. Research in IdM and biometrics is focused on aspects such as understanding 'identity', defining application specific requirements, providing a means for anonymity, dealing with duplicated identities, and providing methods for combining multiple attributes into a single identity, e.g. multifactor authentication. Standards and interoperability are critical facets for IdM as well as for biometric systems to interact within and across applications. In particular, National Strategy for Trusted Identities in Cyberspace (NSTIC) efforts is creating an identity ecosystem which supports multi-factor authentication [10]. NSTIC, with support from academia and industry, furthers our nation's efforts to reduce identity threat and cybercrime.

Recommendation: Support the NSTIC framework and further research into the intersection of identity management and biometrics.

Security and Privacy

Biometric systems measure and store information from individuals. As with other personal information such as demographic information, biometric data must be protected and remain confidential. Ongoing research and development efforts target protection of biometric data, examples of which are outlined below. Continuing to advance the state of the art in this area will further the ability to use biometrics and reduce the need for the release of other personal information to confirm identity when other authentication methods such as passwords are lost or forgotten. Despite standards for password and other security mechanisms [13], "one out of five Web users still decides to leave the digital equivalent of a key

under the doormat: they choose a simple, easily guessed password like "abc123," "iloveyou" or even "password" to protect their data," according to the The New York Times [14]. Investment is needed to develop systems that use layers of security while making these systems convenient for the user. Combinations of security mechanisms as well as enhancing the protections of the biometrics and other security mechanisms are critical to keeping personal information safe, while ensuring the free flow of data for the right people at the right time. Some examples of privacy enhancements include the following.

- *Template protection* is supported by technologies such as biometric cryptosystems by which biometric matching (e.g., comparisons of a measured fingerprint with a stored reference fingerprint template) is performed in the encrypted domain such that biometric information is not disclosed at any point in the matching process.
- *Cancelable biometrics* is a transformation of biometric information that allows the stored biometric tempate of an individual to be cancelled and replaced if that information becomes compromised.
- *Liveness detection* is the protection from the vulnerability when someone's biometric is stolen and an artificial biometric is created. For example it was reported that a South Korean woman used a special tape on her fingers to fool the fingering recognition system at Japan airport [15]. Additionally, BBC News reported a Brazilian doctor used 'fake fingers' made of silicone to sign in absent colleagues [16].

Continuous attention is required in order to stay one step ahead of those who seek to defeat security mechanisms. Privacy and security are often spoken in terms of tradeoffs, i.e., giving up privacy in order to achieve security. The research goal in this area is to change the paradigm to achieve both privacy and security. Investment and policies that encourage inclusion of privacy enhancing technology will keep us ahead of attackers and at the forefront of biometric technology around the world.

Recommendation: Invest in fundamental research for enhancement of security and privacy within biometric systems and develop policies which encourage inclusion of privacy-preserving techniques for applications which use biometrics.

Underlying Science of Biometrics

Biometrics relies upon two fundamental properties: uniqueness and permanence. Because *uniqueness* is difficult to measure, the science of biometrics focuses on studying individuality of the biometric, i.e. the likelihood biometric samples from two different individuals will match when they should not. We study this through empirical observations and the development of statistical models [17]. *Permanence* is associated with the ability to recognize the same individual over repeated measurements in time. Factors such as aging and environmental variability can produce events when an individual is not recognized

when they should be. Through studies performed by academic, government and industrial organizations, the science of biometrics is emerging, particularly for core biometric attributes, such as fingerprints, iris, face, voice, and DNA. Government investment in biometrics is coordinated by the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management. CITeR has studied the science of biometrics throughout much of its existence. However, much of the funded research has focused on near-term implementation challenges. Investment in fundamental research is needed to provide the foundation for biometrics in the future.

Recommendation: Invest in the fundamental research challenges in biometrics through cooperation of government, industry and academia.

Research Infrastructure/Data Sharing

Research in biometrics depends on access to data sets from multiple individuals, perhaps even millions of individuals. Research is appropriately constrained by human subject protections. A continuing challenge in this area is the expense of collecting data as well as the limited ability to share data amongst organizations. This challenge is not unique to our field but is present in many other areas of research including public health, psychology, sociology, business, etc. At CITeR, we have completed more than twenty studies with over a million biometric samples collected from thousands of individuals to support our research endeavors [11]. We have data sharing mechanisms in place approved by our Boards for the Protection of Human Subjects; however, funding typically is focused on paying for the collection of the data. There is little funding available for the protected sharing of appropriate data, both in terms of the infrastructure and personnel costs for deriving the benefits of the data analysis while ensuring that human subject protections are maintained. Additionally, investment is needed to study methods that improve the sharing of data while protecting the underlying privacy of the biometric information.

Recommendation: Invest in mechanisms which encourage and support data sharing amongst organizations and invest in research which enables data sharing while maintaining human subject protection.

Education and Workforce Training

Biometrics is a crosscutting and interdisciplinary area that requires knowledge of electrical engineering, computer science, biology, statistics, information technology, policy, and industrial design. Individuals are needed who have crosscutting depth in all of these areas in order to understand and to develop end-to-end biometric systems. The educational foundations of biometrics are being developed through the efforts of universities who are providing undergraduate and graduate programs (e.g. WVU's undergraduate program in Biometric Systems [18]) as well as the IEEE Certified Biometrics Professional

[19]. These efforts need to continue and grow. Given that identity is one key aspect of our cybersecurity challenges, growth in the number of individuals trained in biometrics is a critical component for the cybersecurity workforce. Long term, this goes to the larger effort of increasing the number of students graduating the Science, Technology, Engineering, and Mathematics (STEM) fields.

Recommendation: Increase cybersecurity workforce including those who have expertise in biometric systems.

Future of Biometrics and their applications

There are many potential uses for biometrics. Mobile devices, e.g. smart phones, have become more ubiquitous and in the future they are likely to incorporate biometrics to identify the user beyond a passcode or a gesture password. This recognition may occur via traditional biometrics such as fingerprint, voice or face recognition or through the use of more natural uses of biometrics whereby the phone automatically recognizes its owners and authorized users. As we are better able to make the connection between a device and an individual, that trust will enable confidence and support such applications as using our devices for payment at point of sale locations, such as the grocery store. For example, today, customers can walk into a Starbucks store, and scan their smart phones to pay for their orders [20].

Emerging biometric systems like rapid-DNA have the potential to solve difficult problems like assessing familial relationships for immigration to reduce hassle for those individuals, as well as have the potential to be part of solutions for problems such as human and child trafficking and refugees. Biometrics have the potential to help with challenges associated with an aging population. Technologies can assist in lengthening the time individuals can stay in their home while ensuring that their health and safety is maintained. Likewise, biometrics can facilitate the management of patients in large hospitals to ensure that treatment and medications reach the correct individuals.

In summary, research, close collaboration between industry, government and academia, and investment in education will continue to make the United States the world leader in biometrics. In biometrics, this investment can reap benefits by improving our trust in cyberspace, by protecting our national security, and by stimulating technological developments that will drive the economy in the future.

Recommendation: Ensure America is in the forefront of technology in the years to come; Encourage close collaboration between industry, university, and academia to promote innovation; Build jobs through investment in STEM education and research.

References

[1] "The National Biometrics Challenge 2006," 2006. [Online]. Available: http://www.biometrics.gov/Documents/biochallengedoc.pdf.

[2] "Biometrics.gov - Introduction to Biometrics." [Online]. Available: http://www.biometrics.gov/.

[3] J. Cofer, "Leveraging Cutting Edge Security Technology to Protect Those Who Protect Our Nation," *Security Industry Association, 2011 Government Summit*. [Online]. Available: http://www.siaonline.org/WorkArea/showcontent.aspx?id=8582.

[4] "Pentagon Visitors Access to Building." [Online]. Available: http://www.pfpa.mil/access.html.

[5] "Biometric Access Control in the Department of Defense," *Biometrics Consortium Conference*, 23-Sep-2010. [Online]. Available: http://biometrics.org/bc2010/presentations/DOT/coleman-Biometric-Access-Control-in-the-Department-of-Defense.pdf.

[6] "NEXUS Program," *U.S. Customs and Border Protection - Travel*. [Online]. Available: http://www.cbp.gov/xp/cgov/travel/trusted_traveler/nexus_prog/.

[7] "The National Biometrics Challenge 2011," 2011. [Online]. Available: http://www.theiacp.org/Portals/0/pdfs/LEIM/2012Presentations/COM-TheNationalBiometricsChallenge.pdf.

[8] "ComScore: U.S. E-Commerce Sales Up 15% in 2012," *Wall Street Journal Online*. [Online]. Available: http://online.wsj.com/article/BT-CO-20130207-714496.html.

[9] "US Online Retail Forecast: 2011 To 2016," *Forrester Research*. [Online]. Available: http://www.forrester.com/US+Online+Retail+Forecast+2011+To+2016/fulltext/-/E-RES60672?docid=60672/.

[10] "Making Online Transactions Safer, Faster, and More Private," *National Strategy for Trusted Identities in Cyberspace*. [Online]. Available: http://www.nist.gov/nstic/.

[11] "CITeR: Center for Identification Technology Research." [Online]. Available: http://www.clarkson.edu/citer/ http://www.clarkson.edu/citer/research/collections/index.html CITeR Portfolio, http://www.clarkson.edu/citer/pdf/citer_portfolios090512_final.pdf CITeR Impact 2010, http://www.clarkson.edu/citer/pdf/62087.pdf

[12] "Identity Management Task Force Report 2008." [Online]. Available: http://www.biometrics.gov/Documents/IdMReport_22SEP08_Final.pdf.

[13] K. Scarfone and M. Souppaya, "NIST SP 800-118: Guide to Enterprise Password Management (DRAFT)." [Online]. Available: http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf.

[14] "Simple Passwords Remain Popular, Despite Risk of Hacking," *The New York Times Online*. [Online]. Available: http://www.nytimes.com/2010/01/21/technology/21password.html.

[15] "AFP: SKorean fools finger printing system at Japan airport: reports." [Online]. Available: http://www.google.com/hostednews/afp/article/ALeqM5jwMl9y-RtlCG0LXfKIF5yX0uxgzg. [Accessed: 17-May-2013].

[16] "Doctor 'used silicone fingers' to sign in for colleagues," *BBC News*, 12-Mar-2013. [Online]. Available: http://www.bbc.co.uk/news/world-latin-america-21756709.

[17] Y. Zhu, S. C. Dass, and A. K. Jain, "Statistical Models for Assessing the Individuality of Fingerprints," *Ieee Trans. Inf. Forensics Secur.*, vol. 2, no. 3, pp. 391–401, 2007.

[18] "WVU Lane Department: Undergraduate Program." [Online]. Available: http://www.lcsee.cemr.wvu.edu/ugrad/degrees.php.

[19] "IEEE Certified Biometrics Professional Program." [Online]. Available: http://www.ieeebiometricscertification.org/.

[20] "Square Wallet from Starbucks Coffee," *Starbucks Coffee Company*. [Online]. Available: http://www.starbucks.com/coffeehouse/mobile-apps/square-wallet.

[21] Biometric Recognition: Challenges and Opportunities, National Academies Press, 2010.