AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE CURRENT AND FUTURE APPLICATIONS OF BIOMETRIC TECHNOLOGIES

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON RESEARCH &
SUBCOMMITTEE ON TECHNOLOGY

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

TUESDAY, MAY 21, 2013

Serial No. 113–29

Printed for the use of the Committee on Science, Space, and Technology



Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PRINTING OFFICE
81–193PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

DANA ROHRABACHER, California
RALPH M. HALL, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
FRANK D. LUCAS, Oklahoma
RANDY NEUGEBAUER, Texas
MICHAEL T. McCAUL, Texas
PAUL C. BROUN, Georgia
STEVEN M. PALAZZO, Mississippi
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
LARRY BUCSHON, Indiana
STEVE STOCKMAN, Texas
BILL POSEY, Florida
CYNTHIA LUMMIS, Wyoming
DAVID SCHWEIKERT, Arizona
THOMAS MASSIE, Kentucky
KEVIN CRAMER, North Dakota
JIM BRIDENSTINE, Oklahoma
RANDY WEBER, Texas
CHRIS STEWART, Utah
VACANCY

EDDIE BERNICE JOHNSON, Texas
ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
DONNA F. EDWARDS, Maryland
FREDERICA S. WILSON, Florida
SUZANNE BONAMICI, Oregon
ERIC SWALWELL, California
DAN MAFFEI, New York
ALAN GRAYSON, Florida
JOSEPH KENNEDY III, Massachusetts
SCOTT PETERS, California
DEREK KILMER, Washington
AMI BERA, California
ELIZABETH ESTY, Connecticut
MARC VEASEY, Texas
JULIA BROWNLEY, California
MARK TAKANO, California
ROBIN KELLY, Illinois

SUBCOMMITTEE ON RESEARCH

HON. LARRY BUCSHON, Indiana, *Chair*

STEVEN M. PALAZZO, Mississippi
MO BROOKS, Alabama
STEVE STOCKMAN, Texas
CYNTHIA LUMMIS, Wyoming
JIM BRIDENSTINE, Oklahoma
LAMAR S. SMITH, Texas

DANIEL LIPINSKI, Illinois
ZOE LOFGREN, California
AMI BERA, California
ELIZABETH ESTY, Connecticut
EDDIE BERNICE JOHNSON, Texas

SUBCOMMITTEE ON TECHNOLOGY

HON. THOMAS MASSIE, Kentucky, *Chair*

JIM BRIDENSTINE, Oklahoma
RANDY HULTGREN, Illinois
DAVID SCHWEIKERT, Arizona

LAMAR S. SMITH, Texas

FREDERICA S. WILSON, Florida
SCOTT PETERS, California
DEREK KILMER, Washington
EDDIE BERNICE JOHNSON, Texas

CONTENTS

Tuesday, May 21, 2013

Page

Witness List 2
Hearing Charter 3

Opening Statements

Statement by Representative Larry Bucshon, Chairman, Subcommittee on Research, Committee on Science, Space, and Technology, U.S. House of Representatives 6
Written Statement 7
Statement by Representative Daniel Lipinski, Ranking Member, Subcommittee on Research, Committee on Science, Space, and Technology, U.S. House of Representatives 8
Written Statement 9

Witnesses:

Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology
Oral Statement 11
Written Statement 14
Mr. John Mears, Board Member, International Biometrics and Identification Association
Oral Statement 27
Written Statement 29
Dr. Stephanie Schuckers, Director, Center for Identification Technology Research
Oral Statement 43
Written Statement 45
Discussion 54

Appendix I: Answers to Post-Hearing Questions

Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology 64
Mr. John Mears, Board Member, International Biometrics and Identification Association 66
Dr. Stephanie Schuckers, Director, Center for Identification Technology Research 68

Appendix II: Additional Material for the Record

Submitted statement of Representative Frederica S. Wilson, Ranking Member, Subcommittee on Technology, Committee on Science, Space, and Technology, U.S. House of Representatives 72

THE CURRENT AND FUTURE APPLICATIONS OF BIOMETRIC TECHNOLOGIES

TUESDAY, MAY 21, 2013

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON RESEARCH &
SUBCOMMITTEE TECHNOLOGY
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittees met, pursuant to call, at 10:06 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Larry Bucshon [Chairman of the Subcommittee on Research] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

Subcommittees on Research and Technology Hearing

The Current and Future Applications of Biometric Technologies

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

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

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.

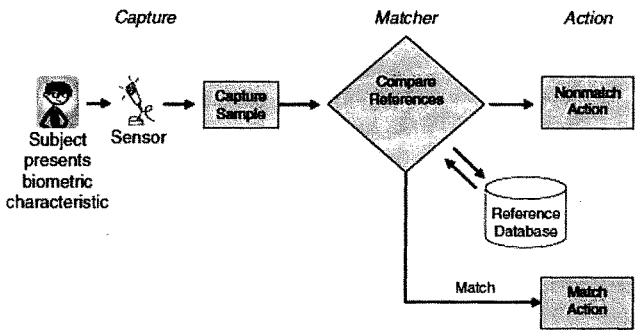


FIGURE S.1 Sample operation of a general biometric system. The two basic operations performed by a general biometric system are the capture and storage of enrollment (reference) biometric samples and the capture of new biometric samples and their comparison with corresponding reference samples (matching). 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.

Chairman BUCSHON. Good morning, everyone. This joint hearing of the Subcommittee on Research and the Subcommittee on Technology will come to order.

Welcome to today's joint hearing entitled "The Current and Future Applications of Biometric Technologies." In front of you are packets containing the written testimony, biographies and Truth in Testimony disclosures for today's witnesses.

Before we get started, since this is a joint hearing involving two Subcommittees, I want to explain how we will operate procedurally so all Members understand how the question-and-answer session period will be handled. As always, we will alternate rounds of questioning between the majority and minority Members. The Chairmen and Ranking Members of the Research and Technology Subcommittees will be recognized first. Then we will recognize Members present at the gavel in order of seniority on the full Committee and those coming in later after the gavel will be recognized in order of arrival. I now recognize myself for five minutes for an opening statement.

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 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 past 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, known as NIST, dates back to the 1960s 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-Berkeley are developing a biometric security that uses brain waves to replace passwords, calling them passthoughts. That is pretty interesting.

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.

[The prepared statement of Mr. Bucshon follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON RESEARCH CHAIRMAN LARRY 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."

Chairman BUCSHON. I now recognize Mr. Lipinski for his opening statement.

Mr. LIPINSKI. Thank you, Chairman Bucshon. I want to thank you and Chairman Massie for holding this joint hearing to examine the use of biometric technologies. I also want to thank our witnesses for being here. I just want to know first, who is James Bond here?

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 hundred 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 ages.

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 noncompliant 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. Let me just say, I don't use the same password. I don't want to suggest that and give anyone ideas.

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 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.

Thank you again for holding this hearing, and I yield back the balance of my time.

[The prepared statement of Mr. Lipinski follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON RESEARCH
RANKING MEMBER DANIEL LIPINSKI

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.

Chairman BUCSHON. For the record, I don't use the same password for all my things either, partially because of this type of stuff. Thank you, Dan, for those comments.

If there are Members who wish to submit additional opening statements, your statements will be added to the record at this point.

Chairman BUCSHON. It is now time to introduce our panel of witnesses. Our first witness is Dr. Charles Romine, the Director of the Information Technology Laboratory at the National Institute of Standards and Technology. ITL is one of six research laboratories within NIST and conducts research addressing measurement challenges and information technology as well as issues of information and software quality, integrity and usability. ITL is also charged with leading the Nation in using existing and emerging IT to help meet national priorities. Dr. Romine holds a B.A. in mathematics and a Ph.D. in applied mathematics from the University of Virginia. Welcome.

Our second witness is Mr. John Mears, a Board Member of the International Biometrics and Identification Association. He is currently the Senior Fellow for IT and Security Solutions at Lockheed Martin. Mr. Mears has worked on program performance segment

strategy and technology plans for biometric identification and verification applications supporting the homeland security, defense and law enforcement communities. He holds both bachelor's and master's degrees in electrical engineering from the University of Florida. Welcome.

Our final witness is Dr. Stephanie Schuckers, the Director of the Center for Identification Technology Research, or CITeR. She is currently Professor in the Department of Electrical Engineering, Computing Engineering at Clarkson University. Her research focuses on processing and interpreting signals which arise from the human body. Dr. Schuckers received her doctorate degree in electrical engineering from the University of Michigan.

As our witnesses should know, spoken testimony is limited to five minutes after which Members of the Committee have five minutes each to ask questions. Your written testimony will be included in the record of the hearing.

I now recognize our first witness, Dr. Romine, for five minutes.

TESIMONY OF DR. CHARLES H. ROMINE, DIRECTOR,
INFORMATION TECHNOLOGY LABORATORY,
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Dr. ROMINE. Chairman Bucshon, Chairman Massie, Ranking Member Lipinski, Ranking Member Wilson and Members of the Subcommittees, I am Chuck Romine, Director of the Information Technology Lab at NIST, and thank you for the opportunity to appear before you today to discuss our role in standards and testing for biometrics.

NIST has nearly five decades of experience in proving human identification systems. NIST responds to government and market requirements for biometric standards by collaborating with Federal agencies, academia and industry to support development of biometric standards, conformance testing architectures and tools, research advanced biometric technologies, and develop metrics for standards and interoperability of electronic identities.

NIST research provides state-of-the-art technology benchmarks and guidance to U.S. government and industry. To achieve this, NIST actively participates in Federal biometric committees and national and international standards-developing organizations.

Biometric technologies can provide a means for recognizing individuals based on one or more physical or behavioral characteristics. These can be used to establish or verify personal identity of enrolled individuals. By statute and Administration policy, NIST encourages and coordinates Federal agency use of voluntary consensus standards and participation in the development of relevant standards and promotes coordination between public and private sectors in the development of standards and conformity assessment activities. NIST collaborates with industry to develop a consensus standard that is used around the world to facilitate interoperable biometric data exchange. The standard is evolving to support law enforcement, homeland security, forensics, and disaster victim identification.

Internationally, NIST leads development of biometric standards that have received widespread acceptance. Use of these standards

is mandatory by large international organizations for identification and verification of travelers at border crossings.

In response to the Homeland Security Presidential Directive 12, NIST developed a standard to improve the identification and authentication of Federal employees and contractors for access to Federal facilities and IT systems. NIST is updating the standards and guidelines for iris and facial images and private-enhancing on-card comparison. NIST leads the development of conformance test suites for implementations of national and international biometric standards.

At the request of DHS, NIST assisted with conformance testing for Transportation Worker Identification Credential specifications resulting in TSA issuing a smart card with the worker's fingerprint for identity verification. To assist in qualifying products to TWIC specifications, three independent testing laboratories have been accredited by NIST and card reader products from about 20 vendors have passed testing.

Understanding capabilities and improving performance of biometric technologies requires a robust testing infrastructure. For more than a decade, NIST has been conducting large biometric technology challenge programs to motivate the global biometric community, to dramatically improve the performance and interoperability of biometric systems, foster standards adoption, and support global deployment, and achieve an order of magnitude or better accuracy gains.

NIST is also working to advance biometrics through the National Strategy for Trusted Identities in Cyberspace, or NSTIC, a White House initiative focused on catalyzing the private sector to create an identity ecosystem. Two NSTIC pilots involve biometrics for authentication, one based on the use of a signature, a second based on smartphone voice and facial recognition.

The NSTC National Biometrics Challenge 2011 report included a few key challenges to the future application of biometrics technologies including research in the privacy and usability of biometrics. For privacy, NIST is collaborating to advance technical methods to safeguard and control the use of biometrics through methods such as liveness detection and biometric template protection.

Usability is a priority for deploying biometric systems within the Federal Government. NIST was identified in a recent National Academies report as one of only two organizations addressing usability in biometric systems. NIST has applied its usability expertise to several studies involving biometric systems. As a result of one study, all of the fingerprint scanners at U.S. ports of entry are now angled to improve the collection process.

In summary, NIST has a diverse portfolio of activities supporting our Nation's biometric needs. With NIST's extensive experience and broad array of expertise, both in its laboratories and in its collaborations with U.S. industry and other government agencies, NIST is actively pursuing the standards and measurement research necessary to deploy interoperable, secure, reliable and usable biometric systems.

Thank you for the opportunity to testify on NIST's activities in biometrics, and I would be happy to answer any questions that you may have.

[The prepared statement of Dr. Romine follows:]

Testimony of

Charles H. Romine
Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the

Subcommittee on Research
Committee on Science
United States House of Representatives

"*The Current and Future Applications of Biometric Technologies*"

May 21, 2013

Chairman Bucshon, Chairman Massie, Ranking Member Lipinski, Ranking Member Wilson and Members of the Subcommittee, I am Chuck Romine, Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in standards and testing for biometrics and identity management.

The Commerce Department's mission is to help make American businesses more innovative at home and more competitive abroad. The development of technically sound measurements, testing and standards are essential for the successful deployment of technologies upon which our society depends. NIST, a non-regulatory agency within the Department works specifically to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST accelerates the development and deployment of information and communication systems that are interoperable, secure, reliable, and usable; advances measurement science through innovations in mathematics, statistics, and computer science; and develops the measurements, testing, and standards infrastructure for emerging information technologies and applications.

NIST has nearly five decades of experience improving human identification systems. NIST responds to government and market requirements for biometric standards by collaborating with other federal agencies, academia, and industry partners to:

- Support the timely development of biometric standards.
- Develop the required conformance testing architectures and testing tools to test implementations of selected biometric standards.
- Research measurement, evaluation and standards to develop and advance the use of biometric technologies including fingerprint, face, iris, voice, multi-modal techniques, and emerging identity determination technologies from video.
- Develop common models and metrics for identity management, critical standards, and interoperability of electronic identities.

These efforts improve the quality, usability, interoperability and consistency of identity management systems, protect privacy, and assure that U.S. interests are represented in the international arena. In fact, NIST research has provided state of the art technology benchmarks and guidance to U.S. Industry and U.S. Government, who depend upon biometrics recognition.

To achieve this impact, NIST actively participates in the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management and its Standards and Conformity Assessment and Research, Development, Test, and Evaluation Working Groups as well in several USG interagency biometric working groups.

In addition, under the provisions of the National Technology Transfer and Advancement Act (PL 104-113) and OMB Circular A-119, NIST is tasked with the role of encouraging and coordinating federal agency use of voluntary consensus standards and participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST works with a wide variety of standards and specification developing organizations, which have vastly different models by which they develop their technical standards and specifications, but all of which are also characterized by active industry participation. NIST has about 400 NIST staff participating in approximately 120 standards and specification developing organizations. NIST leads national and international consensus standards activities in cryptography,

biometrics, electronic credentialing, secure network protocols, software and systems reliability, and security conformance testing – all essential to accelerate the development and deployment of information and communication systems that are interoperable, reliable, secure and usable.

BIOMETRIC TECHNOLOGY

Biometric technologies can provide a means for uniquely recognizing humans based upon one or more physical or behavioral characteristics and can be used to establish or verify personal identity of individuals previously enrolled. Examples of physical characteristics include face photos, fingerprints, and iris images. An example of behavioral characteristic is an individual's signature. Used with other authentication technologies, such as tokens, biometric technologies can provide higher degrees of security than other technologies employed alone. For decades, biometric technologies were used primarily in law enforcement applications, and they are still a key component of these important applications. Over the past several years, the marketplace for biometrics solutions has widened significantly and today includes public and private sector applications worldwide.

NIST'S BIOMETRIC STANDARDS ACTIVITIES

Voluntary Consensus Standards

Most Standards Developing Organizations (SDOs) are industry-led private sector organizations. Many voluntary consensus standards from those SDOs are appropriate or adaptable for the Government's purposes. According to OMB Circular A119, the use of such standards by U.S. Government Agencies, whenever practicable and appropriate, is intended to achieve the following goals:

- Eliminate the cost to the Government of developing its own standards and decrease the cost of goods procured and the burden of complying with agency regulation.
- Provide incentives and opportunities to establish standards that serve national needs.
- Encourage long-term growth for U.S. enterprises and promote efficiency and economic competition through harmonization of standards.
- Further the policy of reliance upon the private sector to supply Government needs for goods and services.

When properly conducted, standards development can increase productivity and efficiency in Government and industry, expand opportunities for international trade, conserve resources, improve health and safety, and protect the environment.

NIST Information Technology Laboratory (ITL) – An American National Standards Institute (ANSI)-accredited SDO

Under our 1984 accreditation by ANSI, the private-sector U.S. standards federation, NIST continues to develop consensus biometric data interchange standards. Starting in 1986, NIST has developed and approved a succession of data format standards for the interchange of biometric data. The current version of this standard is ANSI/NIST-ITL 1-2011, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*. This standard continues to evolve to support Government applications including law enforcement, homeland security, as well as other identity management applications. This standard, used around the world, facilitates interoperable biometric data exchange across jurisdictional lines and between dissimilar systems developed by different manufacturers. In addition to the exchange of fingerprint, latent, face, and iris biometric data, the 2011 version of the standard includes new modalities (DNA and plantar) as well as a latent print extended feature set (EFS); forensic image markups for face and iris; images of all body parts, new metadata fields such as geoposition of sample collection; biometric data hashing and information assurance; and data handling logs.

NIST researchers are collaborating with biometrics and forensics experts worldwide to further expand the ANSI/NIST-ITL Standard to support forensics and Disaster Victim Identification (DVI). Currently an update is underway to include the introduction of dental data, pattern injury (e.g., bite marks) data, and forensics and investigatory voice data. The update will include new capabilities, such as x-rays and other medical imaging technologies. The additions will promote U.S. and international interoperability for forensics data pertaining to identity, and establish for the first time the exchange of dental information among various systems (such as that used by the Federal Bureau of Investigation (FBI) and INTERPOL and the ones used by medical examiners). NIST has also worked with the biometrics and forensics community to introduce within the ANSI/NIST-ITL Standard a new extended feature set to support the interoperable exchange of latent print feature data between human examiners and with automated fingerprint identification systems (AFIS).

ISO/IEC Joint Technical Committee 1, Subcommittee 37- Biometrics
From the inception of JTC 1/SC 37 in 2002, NIST has led and provided NIST experts to develop international biometric standards in this SDO. JTC 1/SC 37 developed standards have received widespread international and national market acceptance. Large international organizations, such as the International Civil Aviation Organization (ICAO) for Machine Readable Travel Documents (MRTD) and the International Labour Office (ILO) of the United Nations for the verification and identification of seafarers, specify in their requirements the use of some of the international biometric standards developed by JTC 1/SC 37.

The ICAO has moved the world's passports to a new level of travel document security, data integrity and identity management. To facilitate the goal of global interoperability, ICAO selected facial recognition as the globally interoperable biometric (listed as mandatory) for machine-assisted identity confirmation for MRTD. Additionally, ICAO selected, as options, the ability to incorporate the specifications for finger and iris. The ICAO estimate as of December 2012 was that there were 430 million ePassports existing, issued by 108 countries using the JTC 1/SC 37 standards for this application. This program serves as a model for effective collaboration and cooperation between industry through Subcommittees of ISO/IEC JTC 1 and the governments of the world through ICAO. ILO's requirements included the first edition of the finger minutiae and finger image data interchange formats developed by JTC 1/SC 37.

Representative examples of applications in different countries referring to biometric international standards include Spain (for their electronic national identity card and the Spanish e-Passports),, and India (which is deploying one of the world's largest identity assurance systems relying on standards-based biometrics technologies).

Biometric Standard for Mobile Applications
Federal agencies require that their biometric results exchange information with emerging mobile applications, making operations more effective and efficient while improving relevant information sharing associated with a biometric. NIST researchers, with support from DHS and the FBI's Biometric Center of Excellence, developed a protocol for communicating with biometric sensors over wired and wireless networks—using web technologies. The new protocol, called WS-Biometric Devices, allows desktops, laptops, tablets and smartphones to access sensors that capture biometric data such as fingerprints, iris images and face images using web services. The WS-Biometric Devices protocol enables interoperability by adding a device-independent web-services layer in the communication protocol between biometric devices and systems. This work is being developed by a private sector SDO. NIST also is working with industry through the Small Business Innovation Research Program to help bring these plug-and-play biometric devices to market.

Mobile applications typically require a rapid response over limited bandwidth communication channels. To meet performance requirements, so-called "lossy compression" must be applied, but as the name implies, data information is lost as the compression is performed, and this data loss can impact system accuracy as well as interoperability. NIST research measures and analyzes the effects of varying amounts of lossy compression and NIST is working with the biometrics community to establish biometric data transmission profiles that employ well-informed compression best practices.

Homeland Security Presidential Directive (HSPD)-12/ FIPS 201
In response to HSPD-12 (August, 2004), NIST initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, was developed to satisfy the requirements of HSPD-12, approved by the Secretary of Commerce, and issued on February 25, 2005. Since the initial implementation of HSPD-12, federal departments and agencies have issued PIV Cards to over 96% of federal employees and contractors. Moreover, the Administration has made strong authentication an integral part of the Cybersecurity Cross Agency Goal under the GPRA Modernization Act, shown on Performance.gov. Doing so will publicly measure how PIV cards are being used to ensure that only credentialed personnel are on Federal networks.

FIPS 201 incorporates three technical publications specifying several aspects of the required administrative procedures and technical specifications. Of particular relevance is NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, which describes technical acquisition and formatting specifications for the biometric in the PIV system, including the PIV Card itself. This document has recently been updated (Draft NIST Special Publication 800-76-2) to introduce the following biometric technologies for PIV use:

- Iris Image Records— the iris image for biometric authentication has been accepted as an additional modality to PIV credentials while the collection and use of iris recognition is optional.
- On-Card Comparison (OCC) — privacy enhancing capability in which biometric matching is executed on the PIV Card and the enrolled biometric templates cannot be read from the card. OCC also provides a means of performing card activation in lieu of the PIN.
- Facial Image –The facial image provides a cost-efficient authentication mechanism for PIV Card issuance, reissuance and verification data reset processes.
- Chain-of-Trust Records -- The "chain-of-trust" is maintained by a PIV Card Issuer and allows the holder of a PIV Card to obtain a replacement for a compromised, lost, stolen, or damaged PIV Card through biometric authentication and use of the "chain-of-trust" record to personalize the new PIV Card. This capability eliminates the need for complete re-enrollment.

Draft NIST Special Publication 800-76-2 is an important step forward in the use of biometric data for PIV. NIST, as with all of its Special Publications, is engaging the public in the development and review of the document. The final SP 800-76-2 document will reflect the disposition of comments received from the first and second public comment periods and will be published once FIPS 201-2 is approved and published. If this process results in substantive changes to the draft, NIST may repeat the open comment review process to ensure all comments and issues have been adequately resolved.

National Security Presidential Directive/Homeland Security Presidential Directive (NSPD-59/HSPD-24), Biometrics for Identification and Screening to Enhance National Security
The purpose of this directive is to establish a framework to ensure that Federal executive agencies use mutually compatible methods and procedures for the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under U.S. law.

The recommended executive branch biometric standards are contained in the *Registry of United States Government Recommended Biometric Standards*, which is maintained by the NSTC Subcommittee on Biometrics and Identity Management. The recommended standards include ANSI/NIST-ITL 1-2011, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information* and other International Committee for Information Technology Standards (INCITS) and ISO/IEC biometric standards, which have been developed by INCITS M1, and JTC 1 SC 37. Critical identity management applications supported by these standards include: the FBI Electronic Biometric Transmission Specification; the DoD Electronic Biometric Transmission Specification; the DHS Automated Biometric Identification System (IDENT) Exchange Messages Specification; and the Terrorist Watchlist Person Data Exchange Standard (TWPDES).

NIST BIOMETRIC TESTING ACTIVITIES

Conformity assessment to biometric standards enables both providers and consumers to have confidence that biometric products or systems meet specified requirements. For IT, the three most important types of conformity assessment related testing are conformance, performance and interoperability testing. Conformance testing captures the technical description of a specification and measures whether an implementation (product, process, or service) faithfully implements the specification. Conformance testing does not completely ensure the interoperability or performance of conforming products, processes, or services. Therefore, interoperability and performance testing are also important for deployment of IT. Performance testing measures the performance characteristics of an implementation, such as its throughput or responsiveness, under various conditions. Interoperability testing tests one implementation with another to establish that they can work together properly. Testing, and ensuring the competence of bodies that do the testing, is as much of a market driver as the specific standard itself.

CONFORMANCE TESTING

Conformance testing to biometric standards captures the technical description of a specification and measures whether a biometric product's or system's implementation faithfully implements the specification. A Conformance Test Suite (CTS) is test software that is used to ascertain such conformance. NIST actively contributes to both biometric standards and biometric conformance testing methodology standards. These efforts also support users and product developers and the possible establishment of conformity assessment programs to validate conformance to biometric standards.

Conformance Testing for the ANSI/NIST-ITL Standard

Technical work started in 2006 with the release of a CTS designed to test implementations of a Biometric Application Programming Interface developed by the BioAPI Consortium and further work continued in the following years with the development of Conformance Test Architectures (CTAs) and CTSs designed to test implementations of national and international biometric data interchange formats (including the ANSI/NIST-ITL standards) and data structures that can contain biometric data of any modality (e.g., finger, face, and iris). In August 2010, NIST released an Advanced CTA and CTSs designed to test implementations of finger image and finger minutiae biometric data interchange formats specified in four American National Standards, and in 2011 we released a CTS designed to test implementations of the iris image data interchange format developed by ISO/IEC JTC 1/SC 37.

Work on the development of CTA and CTSs for the ANSI/NIST-ITL standards started in 2011 as well. NIST released a CTA/CTS for selected Record Types of ANSI/NIST-ITL 1-2007, and in 2012 we developed, in cooperation with other US Government agencies and industry, a Conformance Testing Methodology (CTM) for ANSI/NIST-ITL 1-2011 (published as NIST SP 500-295) and the associated CTA and CTS. In 2012 and early 2013, NIST released a number of CTSs for biometric international data interchange format standards and selected PIV profiles (including the PIV profile for iris data records specified in NIST SP800-76-2). The ANSI/NIST-ITL 1-2011 CTA/CTS is being updated to also support

data transactions encoded in XML and data specified in the expansion of the standard. CTSs designed to test implementations of international standards encoded in XML are being developed as well. NIST is also working on developing the resources to provide support for testing laboratories and users that wish to offer remote testing of biometric data interchange formats using Web Services.

Conformance Testing for Transportation Worker Identification Credential Specifications
DHS has asked NIST to assist with its Transportation Worker Identification Credential (TWIC) specifications. The TWIC program is authorized under the provisions of the Maritime Transportation Security Act of 2002 (MTSA) (P.L. 107-295) and is a joint initiative of the Transportation Security Administration (TSA) and the U.S. Coast Guard, both under DHS. TWIC is a common identification credential for all personnel requiring unescorted access to secure areas of MTSA-regulated facilities and vessels, and all mariners must hold Coast Guard-issued credentials. TSA issued workers a tamper-resistant "Smart Card" containing the worker's biometric (fingerprint template) to allow for a positive link between the card itself and the individual. The TSA also has a requirement to establish a process to qualify products and to maintain a Qualified Technology List (QTL) of TWIC card readers for use within the TWIC program.

DHS has asked NIST to assist with the establishment of a conformity assessment framework in support of a QTL for credential verification and authentication products, to be managed by TSA. Additionally, NIST is assisting with the establishment of a testing process for qualifying products for conformity to specified standards and TSA specifications. NIST's wealth of experience with the Cryptographic Module Validation Program, smart card technology, and specific experience with the PIV card validation program, makes NIST uniquely qualified to assist TSA in establishing a conformity assessment program and a QTL for the TWIC Program.

In FY 2010, NIST set the framework for the conformity assessment process for TWIC readers and for the QTL for the credential readers that successfully passed the conformity tests and satisfy all TWIC requirements. As of the end of FY 2012, three independent testing laboratories have already been accredited by NIST's National Voluntary Laboratory Accreditation Program (NVLAP) to perform TWIC reader evaluations and are now available to conduct this testing for reader vendors. Card reader products from about 20 vendors have already demonstrated the ability to meet the initial requirements.

NIST is currently developing, in collaboration with our partners, the conformity assessment testing suite for credential readers. NIST will continue to support DHS's efforts by assisting in launching and managing the Conformity Assessment Program and the QTL.

PERFORMANCE AND INTEROPERABILITY TESTING
For more than a decade now, NIST has been organizing and conducting large biometric technology challenge programs and evaluations for a variety of purposes. The Multiple Biometric Grand Challenge, Face Recognition Grand Challenge and Iris Challenge Evaluation programs were conducted to challenge the face and iris recognition communities to break new ground solving research problems on the biometric frontier. The Iris Exchange (IREX) and Minutia Exchange (MINEX) programs have engaged a global community to give quantitative support for biometric data interchange standards development, to measure conformance and interoperability, foster standards adoption, and support global deployment. The Face Recognition Vendor Tests (FRVT) and the Multi-Biometric Evaluation (MBE) have been conducted to assess capabilities of face recognition prototypes for one-to-many identification and one-to-one verification. They have measured accuracy gains over the last decade that are well beyond an order of magnitude. This program has recently been expanded to test gender and age determination for emerging digital signage applications. The Speaker Recognition Evaluations (SRE) program has long challenged that community to improve speaker identification capabilities and to make implementations more robust and

versatile. The Fingerprint Technology Evaluation (FpVTE) program and Proprietary Fingerprint Template Evaluations (PFT) were developed in response to statutory mandates to established performance standards for fingerprint identification and verification.

NIST Fingerprint Minutiae Exchange (MINEX) Testing Program
NIST MINEX is an ongoing evaluation program to test fingerprint template generators and the accuracy of fingerprint matchers using interoperable standard fingerprint minutiae templates. The General Services Administration (GSA) uses the results from this interoperability testing as criteria towards certification and inclusion on the GSA Approved Products List (APL) for FIPS 201 compliant devices.

NIST Face Recognition Vendor Testing (FRVT) Program
NIST FRVT provides independent evaluations of commercially available and prototype face recognition technologies. These evaluations provide the U.S. Government with information to assist in determining where and how facial recognition technology can best be deployed, and FRVT results help identify future research directions for the face recognition community. The latest FRVT (launched July 2012) evaluated large-scale one-to-many face recognition algorithms from still face photos and (for the first time) from video, along with testing automated methods for detecting pose, expression, and gender.

NIST Iris Exchange (IREX) Testing Program
The NIST IREX testing program was initiated at NIST in support of an expanded marketplace of iris-based applications based on standardized interoperable iris imagery. The work is conducted in support of the ISO/IEC 19794-6 standard and the ANSI/NIST-ITL 1-2007 Type 17 standard.

- IREX I – (Jan 2010) Defined, tested, and validated accurate and interoperable Compact Iris Image Records for use on smart card credentials (e.g., PIV)
- IREX III – (April 2012) Evaluated large-scale one-to-many iris identification algorithms.

NIST Speaker and Language Recognition Evaluation (SLRE) Testing Program
NIST SLRE is an ongoing evaluation program to test and advance automated Speaker and Language Recognition capability through systematic evaluations and analysis that focuses research on the identified barriers that prevent the technology from reaching its full potential. The NIST project contributes to standardization efforts through the development of ANSI/NIST-ITL Type 11 standard, and is building a community-based scientific working group to develop best practices for Speaker Recognition as used for Forensic and Investigatory purposes.

- LRE-11 – (Dec 2011) Language Recognition Evaluation focusing research on distinguishing between confusable languages pairs and language dialects
- SRE-12 – (Dec 2012) Speaker Recognition Evaluation focusing research on the presence of environmental noise and capabilities with deeper speaker learning (vast amounts of training data).

Biometrics Laboratory Accreditation Program
DHS requested establishment of the Biometrics Laboratory Accreditation Program (Biometrics LAP) by NIST's NVLAP to accredit laboratories that perform conformance testing, interoperability testing, technology testing, scenario testing, and operational and usability testing for biometrics products (systems and subsystems) as defined in nationally and internationally recognized biometrics products testing standards. NIST Handbook 150-25, Biometrics Testing, presents technical requirements and guidance for the accreditation of laboratories under the NVLAP Biometrics Testing LAP. NIST Handbook 150-25 was developed with the participation of technical experts in the field of biometrics testing and was approved by NVLAP. The handbook is intended for information and use by accredited laboratories, assessors conducting on-site visits, laboratories seeking accreditation, laboratory accreditation systems, users of laboratory services, and others needing information on the requirements for accreditation under this program. There are presently two laboratories accredited under this program.

BIOMETRICS FOR THE NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE (NSTIC)

NIST is also working to advance biometrics through its work supporting implementation of the NSTIC. NSTIC is a White House initiative focused on the creation of an "Identity Ecosystem" where all Americans can choose from a variety of identity solutions that enable more secure, convenient and privacy-enhancing experiences everyplace they go online. Biometrics are one of many types of identity solutions that will play a role in the Identity Ecosystem.

NSTIC prescribes that identity solutions in this ecosystem adhere to four guiding principles. Identity solutions will be privacy-enhancing and voluntary, secure and resilient, interoperable, and cost-effective and easy to use.

Privacy is particularly important in NSTIC, and the Strategy calls for the Identity Ecosystem to offer improved privacy protection to individuals. Although individuals will retain the right to exchange their personal information in return for services they value, these protections will ensure that the default behavior of Identity Ecosystem providers is to:

- Limit the collection and transmission of information to the minimum necessary to fulfill the transaction's purpose and related legal requirements;
- Limit the use of the individual's data that is collected and transmitted to specified purposes;
- Limit the retention of data to the time necessary for providing and administering the services to the individual end-user for which the data was collected, except as otherwise required by law;
- Provide concise, meaningful, timely, and easy-to-understand notice to end-users on how providers collect, use, disseminate, and maintain personal information;
- Minimize data aggregation and linkages across transactions;
- Provide appropriate mechanisms to allow individuals to access, correct, and delete personal information;
- Establish accuracy standards for data used in identity assurance solutions;
- Protect, transfer at the individual's request, and securely destroy information when terminating business operations or overall participation in the Identity Ecosystem;
- Be accountable for how information is actually used and provide mechanisms for compliance, audit, and verification; and
- Provide effective redress mechanisms for, and advocacy on behalf of, individuals who believe their data may have been misused.

With its mission of catalyzing a marketplace of secure, privacy-enhancing identity solutions, the NSTIC National Program Office (NPO) has begun to explore how a number of authentication technologies including biometrics can be applied to meet the NSTIC vision and guiding principles. Last September, the NSTIC NPO awarded grants to five projects that will pilot NSTIC-aligned identity solutions that increase confidence in online transactions, prevent identity theft, and provide individuals with more control over how they share their personal information.

The five pilots were specifically selected for their potential to demonstrate innovative frameworks that can provide a foundation for the Identity Ecosystem, and tackle barriers that have, to date, impeded the Identity Ecosystem from being fully realized. The pilots span multiple sectors including health care, online media, retail, banking, higher education, and state and local government, and will test and demonstrate new solutions, models, or frameworks that do not exist in the marketplace today. Two of these pilots involve biometrics. One, led by the American Association of Motor Vehicle Administrators, will be demonstrating the use of signature as a biometric for authentication. A second, led by Daon, a private

company, will be demonstrating the use of smartphone-based voice and facial recognition biometrics for authentication. Both pilots have a two-year period of performance and in the coming months will hit "go live" milestones.

In addition, in February, 2013, the President issued Executive Order 13636 to assist private industry and promote cyber security for the Nation's critical infrastructure owners and operators. The Executive Order directs NIST to facilitate industry-led development of a framework of best practices and voluntary cybersecurity standards for core critical infrastructure.

NIST BIOMETRIC RESEARCH ACTIVITIES ADDRESSING FUTURE CHALLENGES IN BIOMETRIC TECHNOLOGIES

The "*National Biometrics Challenge 2011*" report, published by NSTC's Subcommittee on Biometrics and Identity Management, included a few key challenges to the future application of biometric technologies, including the evolution of many of the measurement, standards and testing activities described above, as well as privacy of biometrics and usability of biometrics.

Addressing Privacy of Biometrics through Technology
Biometric technologies can be used to enhance privacy and provide a convenient authentication factor for data security. Biometrics also present some new challenges in terms of protecting personally identifiable information (PII). At NIST, we are working with the international research and standards communities to advance technical methods to safeguard and control the use of biometrics. For instance, a theft of biometric information could facilitate criminal access to accounts protected with biometrics (or multi-factor authentication). The challenge to government and industry is to create solutions that allow for the use of biometrics, while mitigating security and privacy risks (e.g., identity theft or linking user accounts) through methods such as "liveness detection" and biometric template protection.

"Liveness detection" is a method that industry is developing to counter the presentation of fake biometrics (or spoofs) at a sensor, i.e., if a biometric sample is being captured from a living subject present at the point of capture. The potential for this sort of attack is mitigated in cases in which biometrics are being collected under the supervision of an officer or other personnel. Standards, best practices, and independently evaluated techniques can enable the private sector to use a wider array of multi-factor authentication technologies to protect online transactions. A future revision of FIPS 140-2 will address this topic. In addition, NIST has successfully initiated an international standards project on anti-spoofing/liveness detection within JTC 1 SC 37 (Biometrics). This is the first standards project in this field, with the goal of strengthening the security and privacy of biometrics as an authentication factor for unattended applications. NIST is leading an international "team" of co-editors and has completed the fourth official working draft.

Another issue is that of biometric template protection (also known as cancelable or revocable biometrics). Passwords are stored and validated without being revealed through modern cryptographic means, but the same techniques cannot be used for probabilistic data, such as biometrics. Biometric template protection techniques are being developed to create biometric templates (or samples) which can be used to recognize a person but do not resemble the person's original biometric. For instance, if a template is compromised through a data breach, then the affected template can be cancelled, and a new biometric template can be issued.

NIST has collaborated with the research community through a grant to advance performance metrics for evaluating these new techniques and has held a seat (as the sole U.S. representative) on the Advisory Board of an EU research project known as the TrUsted Revocable Biometric IdeNtitiEs (TURBINE) Project .

Usability of Biometrics

The usability and ease of use of biometric systems is an overarching need and goal for deployed biometric systems within the Federal government. NIST has applied its expertise in usability and biometrics to several studies involving biometric systems in border security and airport environments, including:

- NISTIR 7540 (Sept. 2008) "Assessing Face Acquisition" – in response to a request from the Office of Biometric Identity Management (OBIM) (formerly the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program), the biometrics usability team at NIST examined the then-current OBIM face image collection process to identify any usability and human factors that may improve the existing face image capture process. The report presented results of the study that examined five usability and human factors enhancements to the then-current OBIM collection process.
- NISTIR 7504 (June 2008) "Usability Testing of Height and Angles of Ten-Print Fingerprint Capture" – this study, supported by DHS, was performed in preparation for the 10-print fingerprint capture pilot testing phase of the process through which DHS and the OBIM program transitioned from a two-print fingerprint capture process to a 10-print slap capture process. A concern was identified that the existing counters that housed the fingerprint scanners were too tall to support the capture process. The NIST Biometrics Usability team examined the impact on fingerprint capture performance based on angling of the fingerprint scanners at the existing counter heights. The study was designed to provide guidance on the "best" angle to position a fingerprint scanner given the counter heights common in U.S. ports of entry. As a result of this effort, all of the fingerprint scanners at U.S. ports of entry are now angled correctly for the collection process.

NIST's usability and biometrics research was cited in the 2010 National Academies of Science (NAS) Report, *Biometric Recognition: Challenges and Opportunities*, in which NIST is identified as one of only two organizations addressing usability in biometric systems. The NAS Report notes that "[t]he adoption of biometric systems depends on the ease with which people can use them," and calls for "...more standardized user interfaces coupled with broader human factors testing."

IMPACTS OF NIST BIOMETRIC STANDARDS, TESTING, AND RESEARCH ACTIVITIES

NIST research has provided U.S. Government agencies (whose missions' involve biometrics collection and matching) with state-of-the-art technology benchmarks and guidance. This research has helped enhance identity systems and operations including the FBI Integrated Automated Fingerprint Identification System (IAFIS) and its new Next Generation Identification (NGI) System, the DHS Automated Biometric Identification System (IDENT)/OBIM, the DoD Automated Biometric Identification System, the Department of State Biometric Visa (BioVisa) Program, and the Intelligence Community (IC) systems.

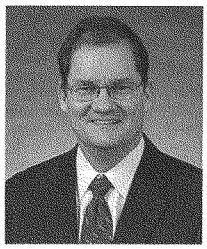
For example, the ANSI/NIST-ITL Biometrics Interchange Standard has facilitated interoperable biometric data exchange between agencies, providing a key enabling capability for the Government to implement NSPD-59/HSPD-24. NIST biometric technology evaluations in fingerprint, face, and iris have provided the Government with timely analysis of market capabilities to guide biometric technology procurements and deployments. The FBI has co-sponsored the challenge problems and evaluations and leveraged this market analysis in its acquisition of NGI system increments. NIST research assisted DHS in its transition to ten prints within OBIM where NIST conducted usability studies for slap capture of ten prints, evaluated required slap segmentation technologies, developed supporting data exchange records, and measured the interoperability between slap and rolled fingerprints. NIST is currently working with DHS to provide standards guidance, best practices, and analysis in support of designing a biometric-enabled U.S. exit process and system.

NIST has a diverse portfolio of activities supporting our Nation's biometric and identity management efforts. With NIST's extensive experience and broad array of expertise both in its laboratories and in successful collaborations with the private sector and other government agencies, NIST is actively pursuing

the standards and measurement research necessary to deploy interoperable, secure, reliable, and usable identity management systems. The NIST biometrics program of work continues to support the advancement of biometrics technologies while enabling the protection of individual privacy and other legal rights under U.S. law.

Thank you for the opportunity to testify on NIST's activities in biometrics and identity management. I would be happy to answer any questions that you may have.

Charles H. Romine



Charles Romine is Director of the Information Technology Laboratory (ITL). ITL is one of six research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of $120 million, more than 350 employees, and about 160 guest researchers from industry, universities, and foreign laboratories.

Romine oversees a research program designed to promote U.S. innovation and industrial competitiveness by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for Federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology

Education:

Ph.D. in Applied Mathematics from the University of Virginia

B.A. in Mathematics from the University of Virginia.

Chairman BUCSHON. Thank you for your testimony.

I now recognize our next witness, Mr. Mears, for five minutes.

TESIMONY OF MR. JOHN MEARS,
BOARD MEMBER, INTERNATIONAL BIOMETRICS
AND IDENTIFICATION ASSOCIATION

Mr. MEARS. Thank you. Chairman Bucshon, Chairman Massie, Ranking Member Lipinski, Members of the Committee, good morning, and thank you for inviting the International Biometrics and Identification Association to this hearing. The IBIA is a nonprofit trade group that advocates and promotes the responsible use of technologies for managing human identity.

As the Committee is well aware, biometrics is not new, unproven or radical. People have developed means throughout recorded history to uniquely identify themselves starting with the first handprint signatures of authors of cave paintings on walls 31,000 years ago. In fact, I think it is an injustice that the first caveman wasn't given prior art credit by the Patent Office for what has evolved into modern hand geometry and palm print biometrics. And as a serious aside, I would note that in the last week, the FBI has added a national palm print capability to its Next-Generation Identification system.

My written testimony addresses the Committee's questions in detail. In my oral comments this morning, I want to highlight some key points about biometric identification that do not always receive the attention they should. From an industry perspective, biometric technology is real and working today. There are successful U.S. government programs that prove this; for identification, IAFIS, NGI, U.S. VISIT, DOD ABIS; for verification, HSPD–12 PIV, DOD CAC, TWIC.

Biometrics have evolved from custom development to integration of commercial components. An example is the 1999 first implementation of IAFIS versus the 2013 version of Next Generation Identification, which in large part uses COTS algorithms, commercial off-the-shelf algorithms. Biometric systems have improved sharply in accuracy. I can cite IAFIS at 92 percent versus NGI at 99.6 percent accuracy.

Biometrics provide greater security and privacy than alternate means of identification including IDs and passwords which are vulnerable and becoming obsolete, as the Chairman observed; and biographics, which are subject to error, spoofing and identity theft. New applications will develop in the private sector in health care and finance, and perhaps significantly, mobility and smart consumer devices will probably in large part drive the acceptance and the need for the security and convenience that biometrics provide.

The common thread from 31,000 years ago is that it matters who I am. No matter the period of history, identifying ourselves is an important function, so much a part of our lives that we sometimes take it for granted. In practice, we identify ourselves by our biometrics, our biographics and our behaviors as illustrated in figure 1 in my written testimony. A biometric is a measurable biological or anatomical and physiological or behavioral characteristic that can be used for automated recognition. The figure shows a sampling of biometric types, and we are all familiar with the most com-

mon of these since they include things like fingerprints, faces, irises, our voices and DNA.

There are in fact a number of others that are shown in the figure including some that are emerging in future applications. The most useful of these exhibit permanence. They can be easily observed, measured and automated, and the best ones are very discriminating to the individual and are hard to spoof or reproduce.

Biographics are descriptors that are assigned by others or that we attribute to ourselves but can change over time as we live our lives. These include things like our names, our addresses, our public records, our Social Security numbers. Biographics are useful for identification but are generally less accurate because they do change over time and can be publicly discovered and spoofed, for instance, in the case of identity theft, and public records sometimes contain errors that are problematic, for instance, name misspellings versus watch lists or errors in credit reports, which actually has happened to me.

Behaviors are descriptors of our actions over periods of time. Group behavior can be observed, for example, in postings on social networking sites, through online transactions, phone records, emails and affiliations. Individual behavior includes such things as handwriting composition style, keystroke dynamics, walking gait and online behavior. Many of these individual behaviors can be difficult to capture and analyze at present but are potentially very useful, particularly for logical and cyber security. In practice, many techniques for authentication and identification use a combination of descriptors of identity. However, if you have to single out one technique, biometrics are the most convenient, reliable and secure means available today.

Biometrics are, by their definition, personal for all of us. It matters who we are, both to ourselves and to the people with whom we have personal and transactional relationships. With the advancement of sensors and computing capability to digitally represent and process biometrics, our lives can be made more secure and more convenient on an individual level as well as for our society. Biometrics are proven and effective when managed properly.

Thank you for your time and consideration today. I look forward to your questions.

[The prepared statement of Mr. Mears follows:]

WRITTEN TESTIMONY OF
John C. Mears
Director, International Biometrics and Identification Association
Lockheed Martin Senior Fellow
Chief Technologist, IS&GS Civil Information Technology and Security Solutions

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, Ranking Member Lipinski, Chairman Massie, Ranking Member Wilson, Members of the Committees, good morning and thank you for inviting the International Biometrics and Identification Association to this hearing. The IBIA is a non-profit trade group that advocates and promotes the responsible use of technologies for managing human identity. My name is John Mears, and I am a Board member of the IBIA, in addition to being a Lockheed Martin Senior Fellow and Chief Technologist for Lockheed Martin's IS&GS Civil Information Technology and Security Solutions line of business.

INTRODUCTION

The IBIA's key focus is on the use of technology in determining identity. Biometrics, which is one of the technologies playing an increasingly important role in identity management, has begun to permeate our everyday lives. The associated technology is commonly embedded and operating well today within solutions that protect our national borders and ports; identify criminals and terrorists; and secure critical facilities, computers, and networks. Increasingly, we see applications in healthcare, the financial industry, and perhaps most significantly, in personal consumer devices.

As the Committee is well aware, biometrics is not new or radical. People have used biometrics throughout recorded history to uniquely identify themselves, starting with the first handprint "signatures" of authors of paintings on cave walls 31,000 years ago. In fact, I think it is an injustice that that first caveman wasn't given prior-art credit by the patent office for what has evolved into modern hand geometry and palm print biometrics! (Note that in the last week, the FBI has added a national palm print capability to its Next Generation Identification system – NGI.)

The common thread from 31,000 years ago to today is that *it matters who I am.* In my personal relationships, and in my business transactions, *it matters who I am,* both to myself, and to the people with whom I have relationships or conduct transactions. However, in those first villages, people knew everyone intimately – by their appearance, by their voices, by their behavior, by their work products – and by their handprint signatures. It was easy to transact business based on a confident understanding of identity.

The difference today is our large and growing population, and the distributed nature of our relationships. Our relationships and transactions aren't limited to a village of a few dozen people as they were 31,000 years ago. According to the US Census Bureau, the world population today is in excess of 7 billion, and the US population is in excess of 315 million. Our economy is global, and it isn't unusual for us to do business with people almost anywhere on the planet. As powerful as the human brain is, how many of us haven't had problems remembering names and faces? It is a natural part of our evolution as a species that we apply our technology to this important question: *with whom am I dealing?* Further, *How do I keep my personal information secure, so that only I can access it?*

What makes modern biometric use highly effective are technology developments that enable precise measurement coupled with computational power. This allows measurements to be transformed into mathematical representations that can be rapidly and objectively converted to unique and secure identifiers that are quickly used to determine a person's identity. Computers allow this to be done quickly, and across numbers of people in excess of what any individual could be expected to remember.

To-date however, (pending "the singularity"), computers are not sentient, and we have to "teach" them. Compounding this challenge, our view of what constitutes human identity is evolving and becoming more nuanced than our understanding even 5 years ago. In addition, the stakes are becoming higher, whether for law enforcement, counter-terrorism, defense, intelligence, homeland security, healthcare, finance, or e-Commerce.

KEY POINTS TO CONSIDER

Before we dive into the formal definitions, and answer the Committee's detailed questions, we believe it is important to offer some key executive summary points regarding biometrics:

- Unique qualities of biometrics technology to consider
  - It's focused on the "who" – the individual
  - It's easy to use, simple to understand
  - It's inclusive and egalitarian
  - It improves security, lowers risks, and is more convenient
  - It's a contemporary solution for a complex and rapidly changing digital world
  - Given that PIN numbers and passwords are becoming less effective and ultimately obsolete, is there a better alternative than biometrics?
- Substantiating statements extracted from details to follow
  - Biometric technology is real and working today.
  - There are successful programs that prove this:
    - For identification: IAFIS, NGI, US VISIT, DoD ABIS
    - For verification: HSPD-12 PIV, DoD CAC, TWIC
  - Biometrics work better than biographics and other techniques, and are less prone to errors, spoofing, and fraud.
  - Biometrics have evolved from custom development to integration of commercial (COTS) components:
    - Example: IAFIS (1999) vs. NGI (2013)
  - Biometric systems have improved sharply in performance:
    - Example: IAFIS (92% accuracy) vs. NGI (99.6% accuracy)
  - Biometrics are expanding from Government-only projects to probable pervasive use in personal devices and applications due to consumer demand for personal experiences, data and cyber security, and privacy.
  - It is natural for us to take advantage of technology to make our lives easier and better. Identification is a human function that surely benefits from what technology – specifically advances in computing and sensing – can offer.

HUMAN IDENTIFICATION DEFINED

The practice of human identification involves making choices among the characteristics that constitute identity, and then optimizing the statistical certainty until it approaches 1. To this end, what are the choices? How is "human identification" defined?

Figure 1: Elements of Human Identification:

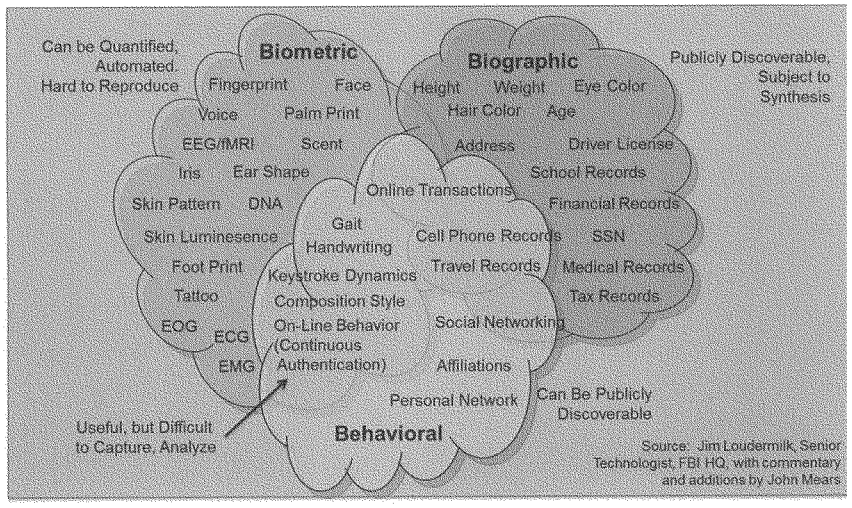


Figure 1 illustrates the three major elements that can define human identity: biometrics, biographics, and behaviors.

The National Science and Technology Council's subcommittee on Biometrics and Identity Management describes biometrics as a characteristic defined as "a measurable biological (anatomical and physiological) or behavioral characteristic that can be used for automated recognition." We are all somewhat familiar with the most common of these, since they include things like fingerprints, faces, irises, our voices, and our DNA. There are many other more esoteric biometrics, including some not listed here (like the type and number of beneficial bacteria in our intestinal tracts). However, as the definition implies, the most useful of these exhibits permanence, and can be easily observed, measured, and automated. The best ones are very discriminating, to the individual, and are hard to spoof or reproduce.

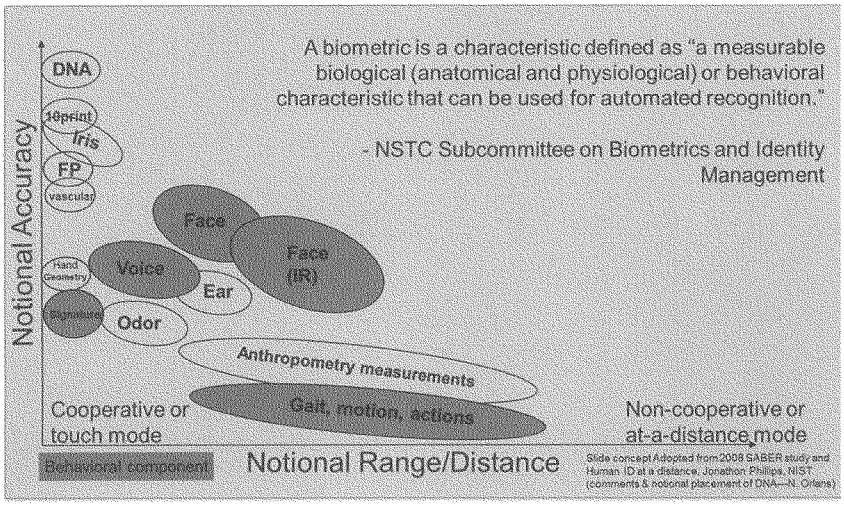
Biographics are descriptors that are assigned by others, or that we attribute to ourselves, but may change over time as we live our lives. These include things like our names, our addresses, our public records, our Social Security numbers. Biographics are useful for identification, but are generally less accurate because they do change over time, can be publicly discovered and spoofed (e.g. identity theft), and public records sometimes contain errors that are problematic (e.g. name misspellings vs. watch lists, and errors in credit reports).

Behaviors are descriptors of our actions over small or large periods of time. They can be classed in two ways: behavior in a group setting; and, individual behavior. Group behavior can be observed, for example, in postings on social networking sites, through on-line transactions, phone records, emails, and affiliations. Many of these group behaviors can be publicly observed, and can be spoofed, as we observed in the Manti Te'o case. Individual behavior includes such things as handwriting, composition style, keystroke dynamics, walking gate, and on-line behavior (useful for an emerging insider threat mitigation technology called "continuous authentication"). Many of these individual behaviors can be difficult to capture and analyze (at present), but are potentially very useful, particularly for logical and cyber security.

In practice, many techniques for authentication (identifying an individual with an asserted identity) and identification (trying to identify an unknown subject against a large number of candidates) use a combination of descriptors of identity. The security industry has evolved to evaluate threats vs. economic cost so that factors are chosen to optimize probability of correct identification vs. application vs. facilitation of commerce. See the appendix for a more detailed discussion of this principle for one example.

Biometrics can increase confidence in identification processes. However, not all biometrics provide the same level of assurance, and many factors impact effectiveness. Figure 2 illustrates this point for a selection of biometric types. The graph shows notional accuracy on the Y (vertical) axis, and notional sensing range or distance of sensing on the X (horizontal) axis. Some biometrics require physical contact for sensing purposes, and some can be accomplished at a distance. Some are best pursued with cooperative subjects, and others do not require cooperation, particularly those done at a distance. Notionally, the most accurate biometrics require touch, or are presently done at short range, like DNA, ten print fingerprints, or iris. Less accurate, although useful at a distance, are biometrics like walking gait, anthropometry, and other remotely observable behaviors.

Figure 2: Characteristics of biometric modalities for different applications:



HOW ARE BIOMETRIC TECHNOLOGIES EVOLVING?

Biometric technology development is accelerating as computing power increases, sensor technologies develop and evolve, and the associated biosciences make rapid advances. Confidence has increased with successful experiences on large programs, and more devices and algorithms from our industry have become commercial offerings, reducing risk and obviating the need for previously large custom development projects. Concerns about privacy, protection of data, and the desire for more personal experiences are driving consumer adoption, which could be the most compelling evolutionary driver that the industry will see. This, in turn, will influence and accelerate the evolution of biometrics in the more traditional domains of usage.

Large successful biometric programs which inform the evolution of our industry include identification programs such as IAFIS, NGI, DoD ABIS, and US Visit, and biometric smart card (verification) programs such as HSPD-12 PIV, DoD CAC, and TWIC. Other countries are pushing forward with ambitious biometric identification programs such as India's Aadhaar program from their UIDAI organization.

Sensor devices are becoming cheaper, smaller, faster, and more accurate, with improved capture quality and tolerance/detection of operator error. Sensors are becoming available at the component level, greatly facilitating incorporation into mobile devices, including smart card readers, laptops, tablet PCs, and smart phones. In addition, general purpose "sensors" like still cameras, video cameras, LADARs, and multi-spectral devices are seeing applications as stand-off biometric sensors for such things as iris and face recognition.

Algorithms for individual biometric modalities have increased greatly in accuracy in recent years, driven in part by algorithm improvements, and part by general advances in computer technology. For example, the FBI's venerable IAFIS system, first deployed in 1999, and running to this day, has a quoted accuracy of 92%, and was largely custom-developed. The FBI's powerful new NGI system uses commercially available algorithms, and achieves an accuracy of 99.6% against the same fingerprint gallery.

Advances in biosciences are being incorporated into evolving biometric sensors so that some of the more "traditionally hard" biometrics come closer to the practicality of fingerprint, face, and iris recognition. For example, microfluidic technology, along with advances in chemistry and microelectronics, have made rapid DNA identification cheap enough, easy enough, and fast enough (90 minutes) to be considered for forward deployment with the military, or installation in police booking stations. DNA-wrapped carbon nanotubes on arrays of field effect transistors show promise as scent sensors, both for human scent as a biometric, as well as other security applications such as explosives, drugs, and contraband detection.

We must acknowledge the contribution of the collaboration between industry, government, and the standards bodies in evolving biometrics. We have the famous Electronic Biometric Transmission Standard (EBTS) message type shepherded by NIST, and I note with interest the adoption of the National Information Exchange Model (NIEM), which has a biometric domain parallel to the EBTS standard. Standards evolve more slowly, but they have a stabilizing effect on the industry (and the consumers of the technology).

As biometric technologies become more accessible, and use cases become more compelling, we are seeing the evolution of renewed interest by healthcare, the finance industry, and organizations working to improve cyber security. In healthcare, there are multiple motivations, from patient identification, to caregiver identification, to narcotics security, billing integrity, and reduction of insurance fraud (to include Medicare and Medicaid). In the financial industry, biometrics are important for employee identification, as well as customer identification, particularly where large transactions are concerned, although there is an overriding desire to simply use biometrics to improve customer service. To this last point, it is consumer convenience, desires for privacy, and the need to protect personal data that may be the most important driver of the evolution of biometrics from this point forward.

HOW DOES INDUSTRY MANAGE THE DIVERSE FIELD OF BIOMETRICS?

Our industry manages the diverse field of biometrics along four different dimensions: tactical; strategic; standards-driven; and disruptive.

Tactically, we are driven by current customer needs and near-term Government procurements. This is often informed by experience on existing engagements and contracts, driving incremental progress and revenue.

Strategically, we look at market trends, competitive assessments, primary and secondary research, strengths, weaknesses, and gaps. We then develop action plans against a projected 5 year market trajectory, looking to fill gaps by R&D, licensing, partnering, or acquiring.

Our development plans are tempered by our participation in conferences, consortia, and standards meetings, so that we evolve offerings that comply with standards, interoperate, and ultimately drive market development for our whole industry.

Occasionally, usually through breakthroughs in R&D, and less often through business model disruption, we discover a previously untapped market segment or niche. Perhaps one recent example of this is the offering of "Identification as a Service" or IDaaS, which is a disruptive new way to provide such services in the very efficient and rapidly evolving cloud computing market.

WHAT RECOMMENDATIONS DOES IBIA HAVE FOR FEDERAL POLICY MAKERS IN THE AREA OF BIOMETRIC TECHNOLOGIES?

Our enumerated recommendations and qualifying comments are listed below:

1. Enhance familiarity with biometrics and associated technology
2. Reach out to understand what has already been done in the US and around the world
    a. What has worked
    b. What hasn't worked
    c. Lessons-learned
3. Use industry organizations (like the IBIA) as a source of information
4. Understand that biometrics can enhance privacy and security
    a. With transparency, good policy, good underlying cybersecurity, and independent audits, then privacy – and public confidence – will be enhanced
    b. IDs and passwords are increasingly hacked, and are no longer sufficient to ensure security and privacy. Fraud and identity theft siphon Government and individual funds. Biometrics present an attractive and effective authentication factor to take security to another level.
    c. Applications of biometrics do not always require a central database – your device or smart card can contain your biometrics within, and be available for local matching

5. When you are assessing feasibility of projects, reach out to industry for the latest cost estimates on available commercial technology
    a. We should all work together to see that cost estimates have a defensible basis, are as accurate as possible, and are based on the latest data (given how quickly technology evolves).
    b. The industry is evolving very rapidly, so commercial function off-the-shelf is increasing while cost is decreasing – just like other aspects of technology evolution.
    c. Much more can be accomplished now through configuring of COTS tools and equipment, without need of costly and time consuming custom development
6. Recognize that different biometrics have different ideal applications – they aren't all the same
    a. Some are dependent on touch
    b. Some are suitable for stand-off purposes
    c. All are statistical in nature
    d. Some are more accurate than others
    e. Using them in combination (something called "fusion"), or with other factors, increases confidence in identity

WHAT DO YOU ENVISION AS THE FUTURE APPLICATIONS OF BIOMETRIC TECHNOLOGIES?

We see the future of biometric technologies in two ways; first, by market segment; and second, by technology to be applied. Looking beyond the current applications in law enforcement, homeland security, intelligence, and defense, we see strong growth against a small current base in several emerging segments.

Future Applications by Market Segment

In commercial and consumer products we see the most potential for dramatic change in the market. People are accumulating more and more personal data and application power in their portable smart devices. This drives a need for more security, and a drive toward personalization. Both of these trends, along with biometric technology rapidly being developed by the smart phone industry, are driving toward biometrically secured smart phone data, and continuous authentication for protection against theft. Generational turn-over will accelerate acceptance as it becomes too compelling and easy to use to reject. As smart, portable devices permeate our lives, so too will biometrics for convenience and preservation of privacy.

In the finance industry, we'll see the acceptance of biometrics for authorization of financial transactions, primarily for convenience and customer service, and secondarily to prevent fraud.

In healthcare, there are a number of applications, from patient identity, to caregiver identity, to billing integrity, narcotic security, and to counter insurance or Medicare/Medicaid fraud.

Cybersecurity is of increasing concern, and many times *who we're dealing with* makes all the difference in defending against cyber threats. For higher-security applications, biometrics can and will be used for access to computers and networks, and behavior monitoring will provide something called "continuous authentication" so that insider threats may be detected and stopped. Migration to cloud computing will enhance our ability to secure our systems by providing a common and secure infrastructure for many applications while simplifying log-on – up to and including presentation of biometrics for the more secure applications.

Future Applications by Technology Type

There are a number of exciting technologies emerging now or on the 5 year horizon:

- Rapid DNA identification. Imagine a time when you can check a person in custody at a police booking station for DNA identification as easily as you can do a mug shot or take their fingerprints. If you can only hold them for 2 hours, wouldn't it be nice to know if they are the serial killer for whom you are looking? Technology is coming to market now from our industry that will allow an untrained policeman to test DNA on a suspect and get an answer within 90 minutes, eliminating the backlog in DNA testing that has resulted in so many criminals going free.
- Simultaneous face and iris capture. Digital cameras are being offered with such high resolution, that soon, with the appropriate lighting both face and iris biometrics can be captured and fused, resulting in very high identity assurance.
- Scent as a biometric. Mentioned earlier, advances in nanotechnology and molecular biology are allowing us to think that scent will soon become a practical biometric. In addition the same technology can be used to detect explosives, drugs, contraband, and industrial process threats so that our world can be made more secure, and man's best friend can go back to being man's best friend.
- Fingerprints can be captured forensically without dusting, fuming, or long and destructive dye treatments. Fingerprints on people can be captured without need of touching a sensor.
- Analytics can be applied to pictures and video to help extract useful identifying biometrics for real-time threat detection and forensic analysis.
- Voice, or speaker identification, will become a more routine biometric, facilitating financial and security transactions, as well as routinely aiding police investigations and sharing of data, much like fingerprints are shared for police use today.
- Portable people identification capability, perhaps embedded in glasses (like Google Glasses) or on a helmet (DoD application for soldiers).
- New biometrics will be explored, driven by biomedical developments (see Figure 1). For example, it has been shown that in small populations (e.g. squads of soldiers), cardio-pulmonary patterns are biometrics.

Our industry is dedicated to making these advancements helpful, secure, and cost effective both for individuals, and our society as a whole.

WHAT WILL THE PRIVATE SECTOR'S ROLE BE IN REACHING THOSE GOALS?

We see value in bringing our real-world experience, across a number of customers and countries, to the pragmatic development of standards and practices, participating with NIST and Government entities in the US and around the world. We expect to continue our innovative research and development work internally, but increasingly work through business alliances and relationships with academia, both directly and through organizations such as CITeR. We will continue to offer new products, services, and business models to the marketplace, where the best will survive over time, thus strengthening our industry.

We expect to play a key role in supporting privacy and associated policy. Related to this, we also expect to have parallel development efforts on counter-spoofing, liveness detection, and cyber security related to biometrics.

We also expect to play an important role in education and awareness. We have a self-interest to educate the market, so that the market will accept – and buy – our products. However, we also need to step up to the responsibility to help our policy and law-makers, since we believe the best policies and laws come from good understanding of the related domains. Not least of our responsibilities is to our next generations. We expect to remain strong supporters of STEM education, not only because it is the right thing to do, but also because it is in our self-interests. We can only continue to innovate and run our businesses if we can get qualified people in sufficient quantity, and in the case of my company, qualified, clearable US Citizens. Only a handful of Universities offer degrees in biometrics at present, and West Viriginia University, founder of CITeR, is one of them. As a result, my company offers scholarships at WVU to worthy biometrics students. However, there are many ways companies can support STEM education. At IBIA, we all know we have to do our parts.

CONCLUSION

First let me say that the IBIA is delighted that you reached out to us for information on our industry. It is one of our recommendations to your policy question that you reach out to industry, particularly for questions of fact or feasibility. We are happy to support formal sessions like this hearing, or even informal discussions with staff. Please do feel free to call on us when you think we can be of assistance.

Biometrics are, by their definition, personal for each of us. It matters *who we are*, both to ourselves, and to the people with whom we have personal and transactional relationships. With the advancement of sensors and computing capability to digitally represent and process biometrics, our lives can be made more secure and convenient on an individual level, as well as for our society. Education and good policy will ensure that security and convenience will always be preserved, even as technology advances. Consumer acceptance and adoption will likely become the predominant driver of widespread biometrics use and advancements, so it is in the interests of our industry to ensure biometrics enhance privacy, security, convenience, and a personal experience

that represents *who we are*. Thank you for your time and consideration today. I look forward to your questions.

APPENDIX

Reference to NIST FIPS PUB 201-2

This principle of matching threat to applications vs. techniques is well-known, and has even been reduced to standard practices, as illustrated in NIST FIPS PUB 201-2, Table 6-2 (reproduced below).

Table 6-2. Authentication for Physical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism
LITTLE or NO confidence	VIS, CHUID
SOME confidence	PKI-CAK, SYM-CAK
HIGH confidence	BIO
VERY HIGH confidence	BIO-A, OCC-AUTH, PKI-AUTH

The context is smart identity card-based authentication, although the principle of trading off risk vs. security need is generally applicable to many applications for which biometrics may be appropriate. In this case, simply observing the card ID number and visually inspecting the card (which includes a face photograph), gives little to no confidence that the credential and/or identity asserted are valid. Verifying with security certificates or card authentication keys gives some confidence that the card is valid. Adding the requirement for presentation of a biometric yields high confidence in both the card and the asserted identity. Having an attended (observed by another human) biometric with on card match and authentication certificate verification yields very high confidence that the card is valid and the asserted identity of the human is valid against the stored biometrics.

John C. Mears
LM Senior Fellow
Chief Technologist and Strategist
Information Technology and Security Solutions
Information Systems & Global Services – Civil
Lockheed Martin Corporation



Mr. Mears is the Chief Technologist and Strategist for Information Technology and Security Solutions (IT&SS) within the Lockheed Martin IS&GS Civil division. In this position, he is responsible for technology advocacy, strategy development, operational technology insertion and growth, new business assistance, and external representation of Lockheed Martin technology and business interests for the area.

Previously at Lockheed Martin, Mr. Mears was Director of Biometrics and Identity Management. He was responsible for program performance, segment strategy, and technology plans for biometric identification and verification applications supporting the homeland security, defense and law enforcement communities. Major program responsibilities for Mr. Mears included the Transportation Worker's Identification Credential (TWIC) program for the TSA, and the FBI's Card Scanning Service IV (CSS IV) program. Research initiatives included Lockheed Martin's rapid DNA identification program, advanced latent print image processing, the carbon nanotube FET smell sensor, and 3D face LADAR, among others.

Mr. Mears began his career with the IBM Corporation in Gaithersburg, Md. Among other assignments, he was lead satellite tracking station engineer for the U.S. Global Positioning System. In addition, he spent two years on assignment in the U.K. establishing commercial product development activities within the Hursley Lab near Winchester in Hampshire.

He is a member of three Boards of Directors, including the International Biometrics and Identification Association (non-profit), the Smart Card Alliance (non-profit), and IriTech Corporation (LM marketing alliance partner).

Mr. Mears holds both Bachelors and Masters Degrees in Electrical Engineering from the University of Florida, and he has more than 30 years of experience in advanced technology solutions, market development, and product management. Mr. Mears was appointed to be a Lockheed Martin Senior Fellow in 2013.

###

Chairman BUCSHON. Thank you.

I now recognize our final witness, Dr. Schuckers, for five minutes.

TESIMONY OF DR. STEPHANIE SCHUCKERS,

DIRECTOR, CENTER FOR IDENTIFICATION TECHNOLOGY RESEARCH

Dr. SCHUCKERS. Thank you very much for the opportunity to testify to you today.

There is a need to establish a trusted relationship between individuals and between individuals and organizations in order to support e-commerce, worker and employer interactions, delivery of benefits, movement of individuals, social connections and health care, and as the other testimonies pointed out, there are many ways to establish a trusted relationship, and they include what you have like credit cards and passports; what you know, passwords, PINs, mother's maiden name; and who you are, biometrics, the topic today.

Transactions in the past have primarily rested on what you have and what you know. The addition of biometrics adds another dimension of security. Emerging is the use of biometrics as part of authentication to support transactions over the Internet, including mobile payments. With weaknesses in passwords alone, combining authentication with a biometric reduces the amount of private information that would need to be revealed repeatedly in order to reestablish a trusted relationship. Depending on the transaction, levels of trust can be created by combinations of different forms of authentication. This is supported by the National Strategy for Trusted Identities in Cyberspace, NSTIC, and is included in my recommendations in my written testimony.

Creating and enabling those trusted relationships makes it more difficult for those who seek to destroy that trust through cyber crime, terrorism and identity theft. Similarly, in our counterterrorism efforts, knowledge of the individual is a critical aspect in sorting out those minority of individuals who seek to do us harm where biometrics is a critical tool in a large toolbox of ways to identify those individuals.

To support these efforts, I highlight two recommendations in my written testimony. The first recommendation: invest in fundamental research for enhancement of privacy within biometric systems and develop policies which encourage the inclusion of privacy-preserving techniques. As with other personal information, biometric information must be protected and remain confidential. One example of methods in the research community and in some of the commercial sectors is something called template protection. This is where biometric matching is performed in an encrypted domain such that biometric information is not disclosed at any point. Another is liveness detection. This protects vulnerability when an attacker creates and uses an artificial biometric—James Bond. Continuous attention is required in order to stay one step ahead of those who seek to defeat those security mechanisms. Privacy and security are often spoken in terms of tradeoffs, giving up privacy in order to achieve security. The research goal is to actually change

the paradigm where we can look to maximize both privacy and security with some of these methods.

Recommendation two: invest in fundamental research challenges in biometrics through the cooperation of government, industry and academia. Investment in fundamental research is needed to provide the foundation for biometrics in the future. It includes such things as studying uniqueness and the permanence of biometrics traits that have been mentioned in some of the other comments.

Other related recommendations in my written testimony have to do with enhancing data sharing to support research and increasing our cybersecurity workforce, including those who have expertise in biometric systems.

As a unique structure for pursuing research, I would like to highlight the Center for Identification Technology Research, CITeR, of which I am the Director. CITeR is a National Science Foundation industry-university cooperative research center, and it focuses on biometrics. CITeR functions as a cooperative of industry such as system integrators, technology providers, small businesses, and government organizations such as the FBI, DHS and DOD. Projects are defined by faculty through interfacing with that community and integrating their research needs. Outcomes include creating workforce trained in the industry and government needs but also promoting innovation through translation of research to commercial products and creating jobs.

In summary, research, close collaboration between industry, government, academia and investment in education will continue to make the United States the best in the world. In biometrics, this investment can reap benefits for improving our security in cyberspace, protecting our national security and stimulating our economy as a leader in the technology of the future. Thank you very much.

[The prepared statement of Dr. Schuckers follows:]

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.

Dr. Stephanie Schuckers is a Professor in the Department of Electrical and Computer Engineering at Clarkson University and serves as the Director of the Center of Identification Technology Research (CITeR), a National Science Foundation Industry/University Cooperative Research Center. Professor Schuckers research focuses on processing and interpreting signals which arise from the human body. She is currently the Vice President for Finances for the IEEE Biometrics Council and served as a consultant for the Army Science Board. She has started her own business, and has over 25 journal publications as well as over 40 other academic publications.

Chairman BUCSHON. Thank you, and I thank the witnesses for their testimony, reminding Members that Committee rules limit questioning to five minutes. The Chair at this point will open the round of questioning. I recognize myself for five minutes.

Just an overriding question for all three of the panelists, why isn't biometric technology being more quickly integrated into our everyday lives? Is there financial barrier, a security barrier, a privacy barrier? And if so, where do you think the bottleneck comes from? Does it come from research and development or application or deployment, or where? Dr. Romine?

Dr. ROMINE. Yes, I would like to take that. I think there are a number of possible reasons, and one of the reasons for establishing the National Strategy for Trusted Identities in Cyberspace is to try to catalyze greater adoption of identify management technologies broadly speaking. At NSTIC, some of the grant activity goes to trying to explore the use of biometrics as part of that ecosystem. I think a lot of it also is sort the maturity of the technology. So I think one of the roles that NIST has to play with industry is trying to advance the state-of-the-art in a way that we get greater confidence.

Mr. MEARS. One of the observations that industry would make is that we sometimes see quantum advancements in technology as a result of what we call a "killer app." That is, there is a compelling application that is popular with masses of people, perhaps consumers, that drives adoption of a particular technology. We think that in the realm of mobility, the proliferation of smart devices, the drive for convenience and personalization of these devices and the need to hold those devices securely will drive adoption of biometrics into consumer devices, which will drive volume and in fact drive acceptance generationally over time that we think will allow us to permeate—allow it to permeate other industries and applications.

Dr. SCHUCKERS. I guess I would agree with the other two. I think it is looking to get that perfect storm. As many of us have, we have a fingerprint reader on our laptops. It doesn't do anything besides get us into the laptop. I think that is where the mobile devices come in. As we use our mobile devices as a form of payment, now there is a value associated with those mobile devices, and that is that killer app that we are talking about. And then it comes to the convenience of it. It is frustrating, as we talked about, to have to remember long, secure passwords, or we use simple passwords that we use in multiple places. By making the convenience of a simple swipe or a face on your mobile phone, that is where the demand comes because you want your phone protected because it pays for things. An enabling thing is NSTIC, National Strategy for Trusted Identities in Cyberspace. That provides that interoperability and standards such that when you do that authentication, it goes somewhere, and it gives you that process such that you have that secure transaction.

Chairman BUCSHON. Thank you. I am going to make an editorial comment and then I will have some other questions. I was in health care before this, and I did a lot of my training and practice trauma-related-type things, and I can tell you, at medical centers, the number of people who come in unidentified is fairly significant, and biometric technology used in that application would be ex-

tremely helpful to identify people for family notification or other reasons.

That said, is there one area that maybe all of you can comment on that you think that this could really revolutionize how we live our everyday lives? Is there a game-changing area that you think potentially that we should focus on first maybe or, you know, a few that would really make a revolutionary change in the way we live our everyday lives. For example, in my view, you know, online purchasing security or some other thing, and what ones maybe we are close to being able to apply broadly that would change people's lives. Dr. Romine?

Dr. ROMINE. Well, I think you have probably hit on one, which is that acceptance is going to be driven by providing added value to the customer, and the customer in this case is going to have to be sort of the American citizen perhaps rather than government-only applications. For that, the usability of these systems is absolutely crucial. There has to be both value added and a good customer experience that adds to the efficiency of the transaction, the effectiveness of the transaction, and satisfaction for the user.

Chairman BUCSHON. I am running out of time, so if you could be brief. Mr. Mears?

Mr. MEARS. Okay. I will just add on what I said before. So the rumors in the industry are the Apple 5S iPhone is scheduled to come out this summer with a fingerprint reader, and we think this is going to be an enabling technology. It allows that platform to do a number of different applications, and we think it will launch from there once the platform is enabled by biometrics.

Chairman BUCSHON. Dr. Schuckers?

Dr. SCHUCKERS. I agree with what the other two Members have said that are testifying today. I think the killer app is the mobile payment system, and I think the driver is the customer who wants their phone to recognize them when they are holding it, essentially.

Chairman BUCSHON. Thank you. I now recognize Mr. Lipinski for his questions.

Mr. LIPINSKI. Thank you, Mr. Chairman. What you are talking about here, I don't know if I should start going down this road but I am going to quickly do it.

Why have we not gotten there yet? I think most people feel like they would pay something extra. If I didn't have to remember all my passwords, I would pay something extra for that if I could use a fingerprint, if I could, you know, go purchase something, plug it in the USB port, use my fingerprint. How come it hasn't happened yet up to this point, if you can be—if anyone has a very brief answer to why to this so we can move on. Mr. Mears?

Mr. MEARS. One of the things I would observe is that many applications are kind of stovepiped, that is the applications that you access on a daily basis, and they don't share application data from one to the next, and so there is no real uniform way of communicating between those. So it leads to this stovepipe approach that doesn't lend itself to what we look for what we call unitary logon, the convenience of having one logon with security including biometrics that gives you access to multiple different types of applications. In government services, the migration to the cloud, cloud computing, actually helps security and helps that convenience be-

cause it puts those apps within a cloud community that has a security structure that is amenable to unitary logon, and so you are going to see advancements as a result of that. But I think in short, that is the reason.

Mr. LIPINSKI. Okay. When Apple comes out with this fingerprint reader on the new iPhone, how does that get past that issue?

Mr. MEARS. Well, certainly for the apps that we all know and love on our mobile phones, it can be an enabler that will be accessed for those apps. My comment was more to the large IT systems that reside elsewhere, perhaps in government service, but for the app side, it will definitely drive convenience.

Mr. LIPINSKI. Okay. I am going to move on. Dr. Schuckers, do you want to add something quickly?

Dr. SCHUCKERS. Well, I was just going to say that NSTIC is also creating this independent, private identity broker, and through that brokerage, you can be—that can be your interface to all of those places where you need to provide that password, and so that is an enabler essentially to get at what you want. So the phone can provide it but really you also need that broker who can to say to this application, yes, that this is the right person to get access without giving all the information away, right? They—you authenticate with them like a PayPal but an expanded sort of PayPal.

Mr. LIPINSKI. How far are we away from that?

Dr. ROMINE. Well, the NSTIC program is relatively new. The grants that have gone out are in their first year of full gear-up, but I would say we are optimistic that the program, which is slated to be essentially a five-year program, will actually catalyze a lot of what Dr. Schuckers was talking about with regard to establishing that ecosystem that is interoperable with the pillars of privacy, transparency, usability and so on as a driver.

Mr. LIPINSKI. Thank you. Another question, Dr. Schuckers. You talked about in your testimony that biometrics provide uniqueness and permanence. You also state that much of the funding for biometrics is focused on near-term implementation challenges, and more research is needed to provide a foundation for biometrics. Can you describe the foundational research that is needed, and which biometric traits are more stable over time, which are more unique? How do you find that balance?

Dr. SCHUCKERS. Thank you. So we think of biometrics as all being equal. You know, you hear people say, look, this is a biometric, X is a biometric, and really, biometrics isn't that way because it has these two fundamental properties, which you highlighted: uniqueness and permanence. And so uniqueness has to do with your ability to distinguish an individual in a thousand individuals, a million individuals, and so if we talk about the uniqueness aspects, we think of DNA as kind of one echelon. Then the next echelon would be finger where 10 fingerprints is better able to distinguish people than one fingerprint. Look at iris. An iris would be equivalent to a fingerprint—two irises, to multiple fingerprints. And then we have other levels of things like voice recognition and face recognition and all of the emerging biometrics, and so this is where the research is to understand what the capability is and how it fits into the application. If you are doing a one-on-one transaction on your phone, for the most part your phone only sees you

on a regular basis and you want to protect—you might not need one-in-a-billion kind of accuracy. You may be satisfied with one in a thousand because you get more convenience.

The other aspect is the permanence, and the permanence has to do with, does the biometric vary over time. We all know our face varies over time. So that is the other kind of studies. Essentially, the biometrics are changing. We want diversity in the biometric market to look at different applications of biometrics but we need to understand what its capabilities are so we can weigh them, depending on the application.

Mr. LIPINSKI. Thank you.

Chairman BUCSHON. Thank you. I now recognize Mr. Massie for his line of questioning.

Mr. MASSIE. So my first question deals with the possibility of mission creep here. When Social Security numbers were created, they were ostensibly to tract retirement benefits but now you need a Social Security number and you need to provide it to purchase even health insurance, and there has been recent interest in using biometrics, I think, to curb immigration violations. But at some point it seems as if we might need to provide proof of self to check out a library book or to rent a house or even just to attend a sporting event or log on to the Internet. How is industry ameliorating these concerns, these privacy concerns, right now? Mr. Mears?

Mr. MEARS. Yes, I will address that. One of the things that we believe is that for every application, there must be a privacy policy. If there is something related to personally identifiable information that is going to facilitate that application, it has to be transparent, published, it has got to specify what data is taken, when, under what circumstances, with whom will it be shared, how long will it be retained, and in fact, there have to be sufficient hooks in the application such that you can verify the application conforms to the policy, and in the best case, an independent ability to audit the policies implemented for that particular application. That is what we believe constitutes good privacy, and we would like to see that across every application that requires the provision of personally identifiable information, and certainly the government does that now. We would like to see that in industry as well.

Mr. MASSIE. So my concern becomes when you take a new technology and it intersects a new piece of legislation. So for instance, in the House we just passed the Cyber Intelligence Sharing and Protection Act where companies, private companies, are now absolved of any liability in private contracts with their consumers if they share that information with the government. And so it seems to me as if this biometric information once it is ones and zeros would be part of that sharable set of data. Dr. Schuckers, do you have any comment on that?

Dr. SCHUCKERS. Yes, I do agree that we need to treat a biometric just like we treat the other information about ourselves, and I think that we are grappling with this explosion of data about ourselves. It is not just biometric data, it is all the biographical data we are talking about, but it is also our movements, our shopping habits, where we have been. There is this explosion of data and there is an explosion of data in the commercial sector. The government has limitations on what they can do with data and particular

biometric data. Where is the equivalent on the commercial side? And so I think that we are wrestling with this as a society. Biometric is one piece of information but it is in the context of a lot of other information that is collected about us. And I do think that we need to, along the lines of the things you said, give the ownership of the data to the person such that they know what data is stored about them and where it is stored and give them access to be able to pull data and to give them control, and that is where NSTIC can come into place, control of their own data as best we can.

Mr. MASSIE. I appreciate those comments. Speaking of control over your own data, outside of criminal investigations, we have all heard of DNA being used, are there any industrial applications for DNA as an identifier?

Dr. SCHUCKERS. DNA—well——

Mr. MASSIE. It is kind of, as you mentioned, it is the upper echelon data that doesn't change about a person over their lifespan. It is a little more intrusive to perhaps collect than a facial recognition when you walk by a camera, but give us an example of a DNA application outside of the criminal aspect.

Dr. SCHUCKERS. I do think there is the positive claim aspects of it so if a person wants to emigrate, suppose they have a familial relationship, this is an example of making a positive claim of a relationship. The DNA can confirm that claim in a way that is less hassle than trying to produce documents, than interviews, and the other aspects of it. So that is not commercial, that is still government, so I was trying to struggle a little bit. I think you were asking——

Mr. MASSIE. No, that is actually the sort of answer I was looking for, so it is a great answer. Thank you very much. I yield back my time.

Chairman BUCSHON. And I will recognize Ms. Wilson for 5 minutes.

Ms. WILSON. Thank you, Mr. Chair.

Dr. Schuckers, in your testimony, you mentioned a case where a woman from South Korea used a special tape on her fingers to spoof or fool a fingerprint recognition system at a Japanese airport. I can also imagine a scenario where someone else uses a photo or video to convince a camera that they are indeed the person associated with an access card. As I understand it, research into these vulnerabilities is termed "liveness detection." Can you please describe how the research community is attempting to detect false or fake biometric traits, and how can we ensure someone is who they claim to be when a biometric system is unattended?

Dr. SCHUCKERS. Great. Thank you. This is some research that I am doing in my laboratory and also being done at the Center for Identification Technology Research. So essentially we talked about what you know and what you have and that biometrics is what you are, this kind of other dimension. But as with all these other security mechanisms, it has vulnerabilities, and this is the—one of the vulnerabilities we need to be aware of. What we have to understand is if we are utilizing biometrics in an application, there is a purpose for recognizing someone's identity in that application, and so does the biometric go towards improving the security that we

need with the caveats that we talk about. So we need to not throw the baby out with the bathwater, essentially. I believe that the biometric information can be very useful for some applications because it is complimentary to the other ways we identify people.

That being said, we know it is a vulnerability, therefore, we need to do research in that vulnerability. That is one of the things we do in our laboratory. I have a fake finger here if anybody wants to see it afterwards. We are interested in not faking but what we are interested in is building those technologies that make it difficult for people to fake the biometric. The word "liveness" is about recognizing that that biometric was measured at that time. So even if your face is not secret, knowing that I just took a picture of your face and that you are physically there at that time, that tells you that it is not a fake biometric. So that is the kind of research we need to do is to build those.

You asked about what technologies are in place. There are software methods that can recognize when someone is faking a biometric. There are hardware methods, things that use light to recognize a finger, for example, as a real finger, and so those are the things that we need to continue to research and put in place.

Ms. WILSON. Dr. Romine, what is NIST doing? What are their efforts in liveness detection?

Dr. ROMINE. Well, I am pleased to say that one of the efforts that NIST undertook was to provide a grant to Dr. Schuckers to do research in this area.

Ms. WILSON. That is great.

Dr. SCHUCKERS. Thank you very much.

Dr. ROMINE. We are also engaging—NIST is not currently conducting internally in our intramural program liveness detection research, although we understand, as Dr. Schuckers mentioned, this is a vulnerability that we need to pay attention to. We are engaging the international community in the standards arena around trying to develop standards for this kind of liveness detection, or anti-spoofing. So that is the extent of our current activities, but we were pleased to be able to provide support to a top scientist.

Ms. WILSON. Thank you. Dr. Romine, as you know, almost everyone has a smartphone. They have gone from devices used to call friends and family to being used to purchase coffee at Starbucks or deposit checks, which raises privacy and security concerns. In your testimony, you discuss several challenges including compression and limited bandwidth communication channels that need to be addressed before biometrics can be fully implemented on mobile devices. Can you please speak to what you are doing at NIST to help address the use of mobile devices and privacy and security concerns?

Dr. ROMINE. Certainly. The use of biometrics is a very context-dependent thing, and the idea of accepting a certain vulnerability with the benefit that you accrue for using the biometric is sort of an individual choice. But one of the things that I would say that is very important is the idea of ensuring encryption is done whenever biometric data or indeed any personally identifiable information is transmitted through mobile devices. I think without using that kind of encryption or some other privacy-preserving technology, I think the vulnerability is considerably larger.

Ms. WILSON. I will give back the balance of my time, which is zero.

Chairman BUCSHON. I now recognize Mr. Schweikert for his questioning, five minutes.

Mr. SCHWEIKERT. Thank you, Mr. Chairman.

Have you ever wanted to start to engage in a conversation with something like this but you are fearful you have watched too much sci-fi in the past? But let us actually jump down the line here. First off, fingerprint scanning technology is, what, two generations ago? I mean, we may be still working on some of the protocols and the security and mechanics but, I mean, we were playing around with that in the early 1990s, if I reMember one of my classes. So where are we at technology today? How good is facial, body, human recognition getting through a camera, and why don't we start down the right and work our way over. Where are we at right now? What is cutting edge today?

Dr. SCHUCKERS. Thank you. So I think a lot of the things that we have brought up already are important, even fingerprint, the issues are the scaling, you know, when you are looking at using fingerprints in large-scale applications, those are some of the challenges. Certainly, the security and privacy side of a fingerprint——

Mr. SCHWEIKERT. But can you cite some of the challenge of the box we are in of what is the most cutting-edge thing you hear that is on the horizon right now?

Dr. SCHUCKERS. I think the one area that could be interesting is the mobile device knows you, right? So you want to say cutting edge, so this isn't available now, but you can see it in the near-term future if we do investment and research but you don't necessarily have to do something very deliberate for the mobile device to know who you are. So I think that could be an area that we could invest in and it makes it easy for people to authenticate.

Mr. SCHWEIKERT. Mr. Mears?

Mr. MEARS. So if you are looking for cutting-edge technology, and I would refer you to figure one of my written testimony, there are a number of biometrics that are emerging, many of them out of biomedical research. I will give you an example of the evolving biometrics. One of them is scent, for example. We have all known for years that dogs track us based on our scent, which is genetically determined with a dietary overlay.

Mr. SCHWEIKERT. That explains a lot of things at home.

Mr. MEARS. Well, wouldn't it be great if you could reduce that to a digital format and be able to reacquire that same scent in multiple sensors. Dogs can't communicate to each other once they communicate a scent. That is an example. Another one is standoff technologies in general, being able to acquire biometrics at a great distance for face, for iris, for fingerprints, for example, but have not normally been done at a distance.

Mr. SCHWEIKERT. Well, you are actually hitting to one. Back in December, I reMember coming across an article that was saying that experiments to enable to read iris at a distance. True?

Mr. MEARS. Yes, sir. Some of the commercial technology has been on the order of 2 meters standoff that is commonly available in our industry.

Mr. SCHWEIKERT. So literally I can be at a grocery store register and it would be able to——

Mr. MEARS. Potentially, and that is commercially available today. There is research at Carnegie-Mellon, for example, that is several tens of meters research, and I am seeing in the laboratory more than that, and I can't say more than that. But those are types of technologies for standoff iris.

Mr. SCHWEIKERT. Doctor, what is cutting edge out there? What is on the horizon?

Dr. ROMINE. Well, I would revisit Dr. Schuckers' sort of hierarchy of different biometrics, and as you point out, fingerprints are widely understood, I think, or largely understood, DNA even more so. All of the biometrics technologies that range from fingerprints, iris, face recognition, even gait, how someone walks, how someone types, signatures, all of these things are improving as the technology improves, the capabilities of technology and computation improve.

Mr. SCHWEIKERT. Now, in the private-sector world, am I heading towards a time where I walk into my grocery store and I am going to pay with cash because I don't want it on the database that I have a small Haagen-Dazs problem, and yet somehow my Haagen-Dazs problem gets attached to my file because I paid with cash but it picked up my gait, it picked up my facial recognition, it picked up my iris, and where are we going now in that type of data using biometrics to attach to our personal data files that ultimately end up tagging the fact I have high cholesterol and my insurance rate. Where are we right now in that interlinking?

Dr. ROMINE. So I think this is the challenging intersection between what the technology makes possible and what the policy apparatus makes permissible, and I think from NIST's perspective, at least, we focus entirely on the technology side, measuring the capability of the technology, providing testing infrastructure so that the community can improve its technology. The policy apparatus is going to get increasingly challenging, I think.

Mr. SCHWEIKERT. Mr. Chairman, I yield back, but, you know, there does become sort of that future cascade effect, particularly with health care and many of the other things out there, these attachments. So thank you, Mr. Chairman.

Chairman BUCSHON. I would agree with that, especially the DNA analysis obviously is not an area that you can escape that. You might detect that somebody is going to get Huntington's chorea, for example, or some other thing that might identify them as being not insurable or other issues. So we have got challenges but it is a very exciting field.

At this point I would like to thank the witnesses for their valuable testimony and the Members for their questions. The Members of the Committee may have additional questions for you, and we ask that you just respond to those in writing. The record will remain open for two weeks for additional comments and written questions from Members.

The witnesses are excused and the hearing is adjourned. Thank you very much.

[Whereupon, at 11:03 a.m., the Subcommittees were adjourned.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Dr. Charles H. Romine

QUESTIONS FOR THE RECORD
THE HONORABLE LARRY BUCSHON (R-IN)
U.S. House Committee on Science, Space, and Technology

The Current and Future Applications of Biometric Technologies

Tuesday, May 21, 2013

1. My understanding is that some of the insights that biometric technologies can provide only come to light as the field advances. That is, we do not know what we do not know. Do you think that much of the potential promise of biometrics lie in areas of research that have yet to be explored? As policy makers, how can we measure success of research investments against unknown potential benefits?

   Answer: The progress in biometric technologies is being documented and the benefits from further biometrics research can be reasonably anticipated. In 2011, the National Science and Technology Council (NSTC) authored the National Biometrics Challenge 2011. This study examined the many advances made as government, academia, and the private sector have collaboratively responded to the priorities identified in the NSTC National Biometrics Challenge 2006[1]. It also delineates some of the challenges that have yet to be fully addressed and offers some new goals that might previously have seemed beyond reasonable hope of being attained but that today appear achievable in light of new technologies and research advances[2].

2. We are facing a very difficult budget environment right now. We have to responsibly prioritize our research and development investments. As Congress looks to reauthorize our federal research agencies, should we increase prioritization of biometric technology initiatives, knowing that this will require decreases in other research areas? Is the technology at the point that the private sector should and could be the primary source of innovation and research and development?

   Answer: Federal agencies, partnering with private industry and academia, followed the research, testing, development and evaluation path laid out in the National Science and

[1] Examples:
- All national biometric systems have improved their capability to process very large workloads and accommodate increased database sizes while also improving accuracy and response times.
- The use of commodity hardware and SOAs has led to more flexible system architectures, which have facilitated technology improvement and the introduction of new capabilities. Using dedicated hardware to process biometric information is no longer widely practiced.

[2] Examples:
- Algorithmic improvements in face recognition have been dramatic. While face recognition is being incorporated into the large identification systems, its potential is still not fully realized due, at least in part, to challenges in addressing the many variables in collection and matching (e.g., pose, illumination, expression and aging).
- The development of Rapid DNA systems has significantly advanced molecular biometrics. DNA processing systems capable of providing usable results for non-ideal and degraded samples, as well as systems for new classes of bio-molecular targets such as scent volatiles and microbial colonies, need to be developed.

Technology Council (NSTC) National Biometrics Challenge 2006. This enabled significant advances in operational capabilities. The research needs identified in the NSTC's National Biometrics Challenge 2011 are the collectively identified government and industry priorities for the next several years. Agency efforts are focusing on these priorities and federal agencies with major biometric activities are continuing to coordinate their efforts. As before, partnership between the U.S. Government, the private sector and academia is absolutely necessary for our biometric and identity system challenges to be met and further efficiencies to be achieved.

Responses by Mr. John Mears

QUESTIONS FOR THE RECORD
THE HONORABLE LARRY BUCSHON (R-IN)
U.S. House Committee on Science, Space, and Technology

The Current and Future Applications of Biometric Technologies
Tuesday, May 21, 2013

1. *My understanding is that some of the insights that biometric technologies can provide only come to light as the field advances. That is, we do not know what we do not know. (a) Do you think that much of the potential promise of biometrics lie in areas of research that have yet to be explored? (b) As policy makers, how can we measure success of research investments against unknown potential benefits?*

1(a). At the IBIA, we believe that the potential promise of biometrics includes enhanced collective and individual security, along with personal convenience and collective facilitation of commerce. We believe that these benefits will be realized when more extensive deployments of existing biometrics (for instance, in mobile personal applications) are implemented. This is not to say that additional research isn't important – it is very important to IBIA and is very important to the future of our industry. However, we have observed that commercial and Government adoption of existing biometrics capability often lags the state of the art, which, ironically, slows the funding of less mature technology and fundamental research. This is certainly the case in industry, but also, we believe, in Government-sponsored endeavors. If the public good is more completely served by biometrics, then there will be a natural tendency to support more work in the area.

1(b). In industry, we require a projected benefits statement (often in the form of a "business case"), as a part of the justification for any research. When the research is new or disruptive, it is often hard to formulate such a justification, although it is possible. In the case of the artificial nose (for scent biometrics), we researched the market for trained security dogs of various kinds as a proxy for the market potential for the eNOSE (electronic Nano-Olfactory Sensing Equipment). For rapid DNA identification, we looked at the FBI's National Crime Statistics to project the need for DNA identification testing at police booking stations. As the technology is developed and deployed, it is possible to measure unit acceptance of the associated biometrics devices and systems against the original business case projections. We recognize that the Government may use a different calculus to make such decisions, but this is how we do it in our industry.

2. We are facing a very difficult budget environment right now. We have to responsibly prioritize our research and development investments. (a) As Congress looks to reauthorize our federal research agencies, should we increase prioritization of biometric technology initiatives,

knowing that this will require decreases in other research areas? (b) Is the technology at the point that the private sector should and could be the primary source of innovation and research and development?

2(a). It is difficult from a distance to state that biometrics research is more important than any other research opportunities. For instance, if a cure for pancreatic cancer could be had in the next year with research money that would have otherwise been allocated to biometrics, the IBIA membership would probably vote for the pancreatic cancer research. This being said, research on biometrics is important to our industry, and we are certainly well-practiced in making difficult decisions on research priorities. Conceptually, we create a spreadsheet of research opportunities with associated descriptions, potential benefits, and costs, and then we stack rank them by objective criteria (typically assessed benefits). Then we calculate cumulative project costs starting with the top project on down, until we reach the point where the cumulative costs of the projects equal the available budget. Then we "draw the line" and the projects above the line are funded, and the ones below are deferred. This process is best done by subject matter experts who can accurately normalize cost estimates and potential benefits of a given project vs. any others. Because we believe strongly in this process, we are willing to provide IBIA subject matter experts to Congress to advise on prioritization of (biometrics or other associated) research, should you require such help.

2(b). The answer to this question generally splits along the lines of the intended uses of biometrics. Biometrics used for authentication (1:1 matching of subject to biometric) will gain more and more traction in mobile devices and consumer/commercial applications (including physical and logical access control), and are therefore more relevant to the private sector (although we know the Government is a part of this market). Biometrics used for identification (1:N searches of larger databases for an unknown subject) are more relevant to Government applications such as law enforcement, homeland security, defense, and intelligence. These applications are inherently Governmental, and should benefit from research support by the Government. The mix between private sector funding and Governmental funding will change over time as more Governments around the world adopt biometrics and a viable world-wide Government market develops which warrants more private investment.

Responses by Dr. Stephanie Schuckers

QUESTIONS FOR THE RECORD
THE HONORABLE LARRY BUCSHON (R-IN)
U.S. House Committee on Science, Space, and Technology

The Current and Future Applications of Biometric Technologies

Tuesday, May 21, 2013

1. *My understanding is that some of the insights that biometric technologies can provide only come to light as the field advances. That is, we do not know what we do not know. Do you think that much of the potential promise of biometrics lie in areas of research that have yet to be explored? As policy makers, how can we measure success of research investments against unknown potential benefits?*

We have had some tremendous successes in recent years: use of fingerprints for verifying identity of those crossing our borders; use of biometrics in Afghanistan and Iraq for separating those who intend to do us harm from civilian population; and solving crimes through the use of fingerprints. Establishment of identity is a key need in a functioning society. Biometrics provides the means to associate an individual with their claim of identity that is complimentary to traditional ways (something you have like a passport or something you know like social security number). The need for biometrics to support government and commercial applications will only increase in an advanced society. While fingerprints are considered one of the most mature technologies, there is a need for diversity in biometric modalities to support different applications as one biometric may not be the best to solve all applications. For example, a biometric system which does not require touching a sensor (e.g. standoff iris) may be useful in applications which have a high number of individuals which must be screened (e.g. airports) for sanitary and environmental reasons. Furthermore, diversity of biometric technologies makes it more difficult for adversaries to succeed in identity theft and cybercrime. Beyond fingerprints, more research is needed to study the fundamentals for a diverse array of biometrics in order to bring them to maturity. Success of research can be measured against characteristics such as uniqueness, permanence, privacy, usability, among others. Continued improvement in these characteristics of biometric technology will support use of biometrics in government and commercial applications to benefit society in the future.

2. *We are facing a very difficult budget environment right now. We have to responsibly prioritize our research and development investments. As Congress looks to reauthorize our federal research agencies, should we increase prioritization of biometric technology initiatives, knowing that this will require decreases in other research areas? Is the technology at the point that the private sector should and could be the primary source of innovation and research and development?*

The commercial sector is a key player in the development and maturity of technology. However, establishing the fundamentals of biometric science should be performed in an open manner, where results are published for the community. This type of research is most typically performed by government, academic, and research organizations. Fundamental research questions in biometrics which still remain include study of uniqueness and permanence, an understanding

which is critical for the success of biometrics. Additionally, as highlighted in my testimony, more advancement is needed in techniques that enhance the security and privacy of biometrics such that these privacy-preserving techniques can become commercially realizable. Investment in research will reap the benefits in the long run of simultaneously achieving security and privacy. Examples of other fundamental areas of research include usability, biometrics with reduced constraints, scalability, interoperability, biometric modeling, and continuous authentication. Commercial investment is not sufficient to study the fundamental scientific questions in biometrics that must be answered in order to mature a diversity of biometric technologies which are critical to current and future government and commercial applications. Successes over the last decade demonstrate the usefulness of biometrics as a valuable tool in the fight against terrorism and cyber crime and point to the need for investment in research and development to continue our position of leadership in the world for biometric technology.

Appendix II

Additional Material for the Record

SUBMITTED STATEMENT OF REPRESENTATIVE FREDERICA S. WILSON,
RANKING MEMBER, SUBCOMMITTEE ON TECHNOLOGY,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
U.S. HOUSE OF REPRESENTATIVES

Thank you, Mr. Chairman for holding this hearing on biometrics and thank you to our witnesses for being here this morning.

Biometric technologies can offer a number of benefits. They can increase security here at home by identifying terrorists or they can provide those in the developing world with an "official identity" that will allow them to open a bank account, buy a home, or receive public services. But there are also a number of privacy concerns surrounding biometrics, especially in the context of facial recognition.

Facial recognition raises special concern because the nature of the technology allows it to be used without a person's knowledge or consent. To be honest this offers an advantage from a security standpoint, but it also raises a number of concerns.

There is a fear that remote surveillance will happen on a much broader scale, not just in the airport, but that individuals will be "tracked" as they run their day to day errands.

This technology still has its limits. Facial recognition failed to identify the two Boston bombers even though both had Massachusetts driver's licenses and one was in an FBI database. But surveillance cameras did help to ID the bombers. And the use of surveillance sensors, both on the street and on-line, is increasing dramatically. As biometrics technology improves how it is used will expand dramatically. We have already begun to see the increased use of this technology by corporations such as Google, Apple, Facebook, and others. In the future this technology will not just be used to verify who you are, but who you are with, your family and friends, where you shop and what you buy. These coming biometric applications present serious privacy concerns that have not been well addressed.

The simple fact is that for many of us our face and name are already publically available online and taking that information to re-identify us in our offline activities is not that big of a step.

You may recall a 2011 study where researchers at Carnegie Mellon University were able to deduce portions of a person's social security number from just an online photo.

The use of facial recognition technology beyond public safety—and even how this technology is used in the context of public safety—need to be carefully considered. I look forward to hearing from our witnesses about the current and future uses of biometric technologies and how we can reap the benefits of biometrics while also ensuring our privacy.

Thank you, Mr. Chairman and I yield back the balance of my time.