WRITTEN STATEMENT

OF

JAMES BENJAMIN HUTCHINSON

TESTIMONY ON BEHALF OF THE INTERNATIONAL BIOMETRICS + IDENTITY ASSOCIATION (IBIA)

BEFORE THE

COMMITTEE ON OVERSIGHT & GOVERNMENT REFORM UNITED STATES HOUSE OF REPRESENTATIVES

LAW ENFORCEMENT'S USE OF FACIAL RECOGNITION TECHNOLOGY

PRESENTED

22 MARCH 2017

Introduction

Good morning Chairman Chaffetz, Ranking Member Cummings, Committee Members, and other distinguished guests. Thank you for inviting me to testify today. My name is Benji Hutchinson. I appear before you on behalf of the International Biometrics + Identity Association, more commonly known as IBIA. I am an employee of NEC Corporation of America. NEC Corporation of America is a member company of IBIA. I am appearing here in my personal capacity at the request of IBIA.

I have 13 years of experience in the biometrics, forensics, and identity technology industry. I have supported a wide range of customers throughout my career, largely federal national security agencies but also some law enforcement. I have held top secret security clearances and I currently teach a graduate level course on the ethics, privacy, policy, and law of identity analysis at George Mason University. Also, I chair the IBIA's Advances in Biometric Technology Working Group.

The purpose of my testimony today is to provide the committee with an overview of the identity technology industry, an understanding of biometrics and facial recognition technology, and the industry perspective on privacy.

Overview of IBIA and the Identity Industry

IBIA is the leading international trade group representing the identification technology industry. The association recognizes the vital role identity plays in a globally connected world. The mission of IBIA is to advance the adoption and responsible use of technologies for managing human identity to enhance security, privacy, productivity, and convenience for individuals, organizations, and governments. To effectively carry out this mission, IBIA focuses on three core activities: advocacy, connections, and education. IBIA brings broad industry stakeholders into a single organization to provide essential support for access to decision makers, inform members with industry reports, and establish a platform for debate on public policy and legislation regarding identity technology.

The biometrics and identity industry is a multi-billion dollar international industry with diverse offerings. Identity products include biometric software and hardware solutions for fingerprint, palm, iris, DNA, voice, and of course facial recognition solutions. Physical identity solutions include secure credentials such as passports and common access smart cards. Our industry also offers professional services and subject matter expertise for customers with requirements to positively identify individuals for various reasons.

Member companies of IBIA serve various government agencies at the federal, state, and local levels. Our members also serve private sector clients. The missions and operations that IBIA supports include law enforcement, defense and counter terrorism, border management and travel security, education, finance, gaming, health care, cybersecurity, human resources, elections, physical access, and benefits distribution. We have 27 national and international member companies from across the identity technology industry. IBIA membership consists of large, established companies, mid-size, and new, small companies that have recently entered the market.

Basics of Biometrics

Biometrics are unique physical or behavioral characteristics which can be used to identify individuals. Biometric technologies capture, process and measure these characteristics electronically and compare them against existing records to create a highly accurate identity management capability. As previously mentioned, common physical biometric indicators in use today include fingerprints, faces, irises, voices, and DNA, among many others.

Biometrics have been around for over 100 years in various forms around the world for various use cases. In the U.S., the techniques of measuring fingerprints, latent fingerprints, and palm prints grew in popularity among the law enforcement community in the early 20th century. The modern digital version of biometrics in use today by law enforcement or national security professionals developed about 45 years ago. The technology has progressed rapidly in the past 16 years, largely due to heavy investment in research and development after the tragic terrorist attacks of 9/11.

Basics of Facial Recognition

1. **How does it work?** Facial recognition technology uses the layout of facial features and their distances from one another for identification against a "gallery" of faces with similar characteristics. These characteristics can be extracted and measured from either a still or video images. Using statistics,

facial recognition algorithms can measure the differences between the face being searched and the enrolled faces in a gallery. The smaller the difference, the more likely those faces match. Facial recognition technology is primarily used for anonymously characterizing faces, verification (1:1) searching known faces, and identification (1:N) searching unknown faces. (International Biometrics + Identity Association n.d.)

2. **What is a facial recognition algorithm?** Facial recognition algorithms are computer instructions that generally perform three functions: image processing, feature extraction, and matching. Image processing could include enhancing the quality of an image against a predetermined standard. Feature extraction is the process of locating points of interest or features in a digital face image that are relevant for matching. These features are then extracted, and a mathematical representation of the image is generated. Matching is the process of comparing multiple facial representations. The result of the matching process is a similarity score, which is then compared with the threshold value to determine a match or no-match decision by a human. (American Association of Motor Vehicle Administrators, Driver Standing Committee & Law Enforcement Standing Committee, Facial Recognition Working Group 2015)
3. **How accurate is the technology?** The accuracy of automated facial recognition technology has steadily improved over the past 15 years. For high performing facial algorithms, error rates can be as low as 1%. This means algorithms can match faces accurately around 99% of the time. However, it is important to note that matching accuracy is highly dependent on the quality of a face image, the quality and composition of the face images in a gallery, and the proprietary algorithm used to search and match. In 2014, the National Institute for Standards and Technology (NIST) found that the error rates continued to decline and algorithms had improved at identifying individuals from still photo images of poor quality or captured under low light (National Institute of Standards and Technology 2014) and (Government Accountability Office 2015). More recently in 2017 in a study on facial images from video, NIST found that with small galleries of 480 faces, the proportion of searches that do not yield the correct identity at rank 1 ranges from below 1% to above 40%. (National Institute of Standards and Technology n.d., 8). A final word on accuracy, the algorithmic facial

recognition process out performs human operators in terms of speed and accuracy when initially searching through large amounts of data. The final match decision, particularly for law enforcement applications, from search results is made by a human through their visual examination of ranked candidates returned by the automated search. Training of human examiners for this process is critical. Professionally trained humans are responsible for deciding to take action on a face match. In these applications, you can think of automated facial recognition as an "investigative tool" that returns several match candidates of interest that are then further investigated by a trained professional examiner. Similarly, in border security applications such as real time surveillance, the algorithms can be tuned to match only top candidates who surpass a certain score threshold, which would trigger a real time response. Even in these circumstances, trained professional examiners are responsible for taking action on any matches.

4. **How effective is facial recognition technology at dealing with race, ethnicity, gender, and certain age groups?** Race, sex, and age are not generally considered or factored into the mathematics of a facial recognition algorithm. These aspects are largely biographic and contextual data descriptors. Algorithms are developed to be as accurate as possible using mathematical feature sets such as the number of pixels between the eyes. It is important to note that it is in the best interest of our industry to develop highly accurate algorithms that do not consider such aspects at the algorithm level. However, when dealing with homogenous data sets of faces, there have been instances where the technology's effectiveness has varied with ethnicity, race, gender, and certain extreme age groups. Faces change over time. A baby does not have the same face at age 18 nor does that person have the same facial structure at age 70. Once a match is made, the human examiner must look at images analytically, not holistically. This approach helps to diffuse the possibility of human error because examiners look for analytical attributes that distinguish a face (e.g. moles, nose, nostrils). Facial recognition is a photographic comparison technique similar to other types of comparison in the field of forensic science.
5. **Would vendors allow customers access to source code for tuning?** As a general practice, the majority of facial recognition vendors would never allow customer access to the facial recognition algorithm source code as this

is considered proprietary information. If this occurred, it would be a rare exception. Vendors would never allow access to source code for tweaking or tuning an algorithm. This practice would open up technology companies to liability, void warranties, and undermine technology performance and credibility. Such a practice could ultimately destroy our business. Nevertheless, biometric software applications do allow users to tune search parameters. For example, operators can configure a system to return match results with candidates above or below a certain score threshold. Such parameters are common among all biometrics modalities and systems including fingerprint systems.

6. **How is the technology tested by industry?** Each vendor tests their algorithms with their own internal methodologies based on best practices developed by academia and industry research and development; and then outlined by the American National Standards Institute (ANSI), the International Standards Organization (ISO), and the National Institute of Standards and Technology (NIST). In addition, many members of IBIA submit facial algorithms to NIST for testing that is consistent, truly transparent to all, and according to a common methodology. The testing methodologies used by NIST to assess the efficacy of facial recognition algorithms are extensive and sophisticated.

The Value of Biometrics and Facial Recognition

Biometrics and facial recognition are effective tools to promote lower crime rates, enhance public safety, and prevent terrorism. During the wars of Iraq and Afghanistan, biometric and identity technologies matured rapidly and saved thousands of American lives on the battlefield. U.S. military forces employed (and still use today) these technologies in tactical and strategic forensic investigations, to pursue perpetrators of improvised explosive devices, and to defeat terrorist networks. Often times, enemy combatants did not wear military uniforms and they disappeared into crowds. Biometrics were critical tools in countering this threat. In the law enforcement arena, these tools have also been used countless times as an investigative tool to solve or prevent crimes. Here is just one example:

“John Robert Jones was convicted in 1974 of murdering a fellow soldier at Fort Dix, New Jersey. After three years in prison, Jones escaped and was on the run for more than 37 years under an assumed identity. He was listed as one of the Army's top 15 most wanted fugitives. The U.S. Marshall's Office submitted a photograph of Jones for comparison in the Florida DMV's FR system. A match with an image on a driver's license that Jones had fraudulently acquired in 1981 was returned. Jones was subsequently apprehended, and his fingerprints confirmed he was indeed the wanted fugitive (American Association of Motor Vehicle Administrators, Driver Standing Committee & Law Enforcement Standing Committee, Facial Recognition Working Group 2015)."

Facial recognition is the enabling technology for deterring secure document issuance fraud. It is used by the majority of States and by the Department of State to ensure that an individual is issued only one unique document, driver's license, passport or a visa.

Facial Recognition is One of Many Biometrics Tools

These technologies are investigative tools for law enforcement agencies. They are based on statistics and are not absolute. None of the technologies represented by the IBIA will ever yield a 100% match by themselves. When an image is searched against a database of images, these technologies generate candidate lists, which represent investigative leads. Human operators must always review the results and take action on possible matches. Our customers often refer to our technology as investigative tools for generating leads. Face recognition is no different from other technologies used by law enforcement, such as voice, fingerprint or iris biometrics. Training is very important. We do support the continual education of how to effectively and responsibly use these tools. We also support the continued development of best practices and more standards on facial comparison.

IBIA Position on Ethics and Privacy

The members of IBIA believe that identification technologies should be used solely for legal, ethical, and non-discriminatory purposes. We are committed to the highest standards of systems integrity and database security in order to deter identity theft, protect personal privacy, and ensure equal rights under the law in all identification solutions.

The industry believes in and supports transparency and openness as it pertains to the capabilities of biometrics and identity technologies. We support and encourage best practices to ensure privacy and ethical use of the technology. We believe the technology should be fielded with appropriate privacy policies in place that cover how the data are used, who has access, data sharing, data security, and data redress. Of course this functionality should be subject to applicable laws and policies of the U.S. federal government or the appropriate state.

IBIA Contribution to the Privacy Debate

According to IBIA's Privacy Best Practice Recommendations for Commercial Biometric Use, our primary privacy policy is that biometric data should be treated as personally identifiable information (PII) and, as such, all biometric data should be protected.

Over the years, IBIA has participated in, and will continue to participate in, discussions surrounding privacy and the responsible, ethical use of biometric technology. Specific examples of recent and past IBIA efforts to engage in the privacy debate are listed below:

a. **NTIA General Framework for Privacy** - IBIA Participated in the Department of Commerce, National Telecommunications and Information Administration (NTIA), Multi-Stakeholder Process to develop and publish a general framework for the commercial use of facial recognition titled the "Privacy Best Practice Recommendations for Commercial Facial Recognition Use."

b. **Annual 'connect:ID' Conference** – We co-sponsor this annual event that brings together government, academia, industry, privacy and policy experts all for the express purpose of discussing not only the latest trends in the technology, but also best ways to test, deploy, and enhance the technology in support of our customers and their missions. We also host specific panels on the ethical use of automated identity data as a social good.

c. **Active Member of the Future of Privacy Forum** – IBIA is an active member of the Future of Privacy Forum and has been for 2 years. We have a strong, collaborative relationship. Together, we work to co-develop papers on privacy issues, biometrics and identity technology, and education efforts.

d. **Participation in Public Discourse and Debate** – We accepted the Committee's invitation to participate in today's panel because we felt it was important to appear and provide an industry perspective.

We welcome the opportunity to have a constructive dialogue and collaborate with members of this panel and the broader identity technology community. As in any national or public debate, we may have disagreements with the logic and findings of particular groups, however, we remain committed to a continued dialogue. We encourage members of this public debate to not over emphasize or overstate the potential negative impacts of biometrics technology. As with any new technology or tool, misperceptions and misunderstandings are common. IBIA believes the benefits of identity technology far outweigh the negatives. Part of IBIA's charter is to continually educate the public on this technology.

In Closing

We thank the Committee for the opportunity to testify today. IBIA looks forward to continuing this dialogue with the members of this Committee and the members of this panel. We hope this testimony has helped the committee to better understand the technology of facial recognition and the perspective of the industry who develops it. We believe the ethics and privacy of biometrics and identity technology are important issues that will continually evolve over time. As an industry group, we look forward to participating in that debate by providing subject matter expertise on biometric and identity technology. Thank you very much.

Works Cited

American Association of Motor Vehicle Administrators, Driver Standing Committee & Law Enforcement Standing Committee, Facial Recognition Working Group. 2015. "Facial Recognition Program Best Pracitces." Best Practices, 28-29.

American Association of Motor Vehicle Administrators, Driver Standing Committee & Law Enforcement Standing Committee, Facial Recognition Working Group. 2015. "Facial Recognition Program Best Practices." Best Practices, 48.

Government Accountability Office. 2015. "Facial Recognition Technology, Commercial Uses, Privacy Issues, and Applicable Federal Laws." GAO, 5.

IBIA. n.d. *Face Biometrics.* https://www.ibia.org/biometrics-and-identity/biometric-technologies/face.

International Biometrics + Identity Association. n.d. *IBIA Face Biometrics.* https://www.ibia.org/biometrics-and-identity/biometric-technologies/face.

National Institute of Standards and Technology. n.d. *Face in Video Evaluation (FIVE), Face Recognition of Non-Cooperative Subjects.* NISTIR, NIST, Gaithersburg: NIST.

National Institute of Standards and Technology. 2014. *Face Recognition Vendor Test (FRVT): Performance of Face Identification Algorithms.* NIST, Gaithersburg: NIST.