WRITTEN STATEMENT OF
JAMES N. ALBERS
SENIOR VICE PRESIDENT OF GOVERNMENT OPERATIONS
MORPHOTRUST USA

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

IMPLEMENTATION OF AN ENTRY-EXIT SYSTEM: STILL WAITING AFTER ALL THESE YEARS

PRESENTED
NOVEMER 13, 2013

Written Statement of James N. Albers
Senior Vice President of Government Operations
MorphoTrust USA
Before the Committee on the Judiciary
United States House of Representatives
November 13, 2013

Good afternoon Chairman Goodlatte, Ranking Member Conyers, and other distinguished members of the Committee. Thank you for inviting me to testify today.

My name is Jim Albers. I am the Senior Vice President of Government Operations at MorphoTrust USA. I have been working in the biometrics industry for 11 years. I am pleased to address the subject of this hearing. I believe we have waited too long to complete a biometric exit control system in the United States. Today, advanced biometric entry and exit control systems are being used in airports and border crossings around the world. These systems are affordable, convenient, and can accommodate high rates of traveler throughput.

Today I would like to address the following topics:

- MorphoTrust's role in large, complex biometrics and identity programs
- The affordability and convenience of biometric exit systems
- The security benefits of biometrics over biographic information
- The importance of collecting multi-modal biometrics at entry and exit
- Different types of biometric exit control systems
- Examples of successful exit systems around the globe

MorphoTrust USA's History and Role in Identity Solutions

MorphoTrust USA, formerly known as L-1 Identity Solutions, is headquartered in Billerica, Massachusetts. Our mission is to simplify, protect, and secure the lives of the American people. MorphoTrust provides end-to-end identity solutions in biometrics, background checks, and secure credentials. We have over 1400 employees at locations across the country.

MorphoTrust develops the technology for, and delivers some of the largest, most complex biometric systems in the world. Our Automated Biometric Identification System (ABIS) is used by the U.S. Department of Defense, the U.S. State Department, the Federal Bureau of Investigation (FBI), and a number of state and local law enforcement agencies to fight terrorism, prevent identity fraud, and provide criminal investigative leads. In addition, Morpho has successfully developed and deployed biometric entry/exit controls in airport environments around the world.

MorphoTrust is also the leading domestic provider of secure credentials. We produce driver licenses for 42 of 50 states, as well as the Passport Card and Border Crossing Card for the U.S. Department of State. Our parent company, Safran, is a global high-technology company with concentrations in aerospace, defense, and security. In the United States, Safran has 32 subsidiaries and joint ventures, with approximately 7000 employees in 22 states.

Biometric Exit Controls are Affordable and Convenient

Based on our history of delivering a range of biometric solutions, we feel confident to be here today delivering a simple message—biometric technologies are fast, convenient, and accurate and can provide increased security without slowing or inconveniencing travelers.

When properly implemented, biometric exit controls can provide a higher degree of identity assurance than biographic exit controls alone. Furthermore, we are sure that this can be done without disrupting operations at airports, seaports, or other ports of entry and at a reasonable cost compared to the benefits.

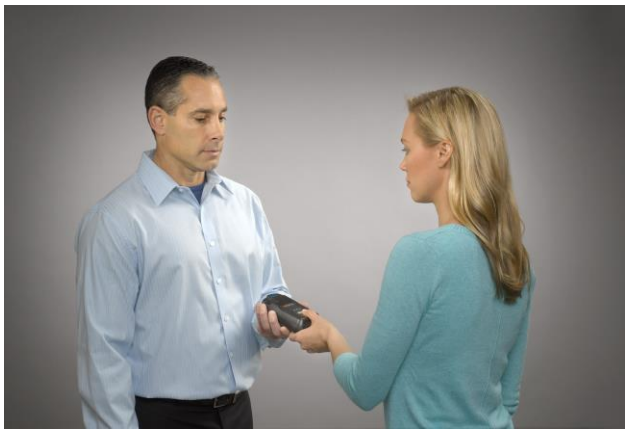
All of this is, we know, in stark contrast to what many of you hear on a regular basis—that biometric exit controls are both costly and difficult to implement. However, we do not believe this to be the case. In reality, the costs associated with biometric capture devices have been trending dramatically downward, while convenience and accuracy of these capture devices continue to improve.

In studying the opposition to biometric exit controls, we know there is significant reliance on a 2008 report commissioned by the U.S. Department of Homeland Security (DHS) that estimates the costs for implementing a biometric exit system at airports and seaports to range from $3 billion to $6 billion.[1] We believe these cost estimates are out of date and orders of magnitude too high, and do not take into account the dramatic price declines in biometric technologies in recent years.

The study assumed building a system to specifications, without consideration of the range of Commercially Available Off-the-Shelf (COTS) biometric capture devices offered by vendors today that are affordable, highly accurate, and are designed specifically to fit within an airport footprint.

The first "livescan" fingerprint devices were put into use 20 years ago, were big and bulky, and cost $15,000 or more. Today, livescan devices are small and cheap enough to put on an iPhone, and law enforcement agencies buy high volume, "ten print" fingerprint devices for less than $1500.

[1] U.S. Dept. of Homeland Security, DHS-2008-0039-0002, *Air/Sea Biometric Exit Regulatory Impact Analysis* (2008).



AOptix Stratus™ mobile identity solution

Speaking of iPhones- everyone can see how the cost and size of cameras has also declined. My iPhone 5 has an 8 megapixel camera, and the new ones even have autofocus. Nokia now has a 41 megapixel camera. When the study was done in 2008 you could not buy a 41 megapixel camera at any price. This remarkable change has allowed cameras to be ubiquitous, and has facilitated law enforcement activities using face recognition.

Likewise, iris recognition was in its early days in 2008 and has now been recognized as the most efficient and effective biometric when matching one-to-many. A prime example of the scalability of biometric enrollment and verification is the UID program in India. 425 million Indian citizens are now enrolled in that National ID program, with a goal of enrolling 600 million citizens by 2014.

Biometric Exit Offers Greater Security than Biographic-only Exit Controls

It is important to recall that the existing legislative mandates to implement a biometric entry-exit control system are among the recommendations of the 9/11 Commission Report. Coincidently, those tragic events of 12 years ago were the catalyst for the growth of Federal biometrics programs.

Since that time, the U.S. Department of State has initiated and operated the largest face recognition program in the world. The U.S. Department of Defense uses multi-modal biometrics as standard operating procedure. While the FBI has been using fingerprints for a century, their Next Generation Identification (NGI) Program incorporates face recognition and iris recognition tools to also leverage the benefits of multiple biometrics modalities.

Our years of experience in this market have shown us that the use of biometrics is the single best way to quickly and accurately prove an identity. Biographic information, such as a person's name, social security number, and date of birth, and the documents used to verify biographic information are all vulnerable to fraud. All of this information and documentation can be falsified and stolen. Additionally, biographic data is fraught with errors because it is reliant, in most cases, on human collection.

Biographic data is also presented inconsistently around the world; birth dates can

be presented as day/month/year or as month/day/year and names can be presented as first/middle/last or the reverse. This is in addition to limitations associated with transposed or erroneous numbers or letters. Many names—especially those associated with foreign languages—allow multiple spellings or use of hyphens or other marks that can reduce the reliability of biographic systems.

Biometric identification and verification, on the other hand, is based on international standards and is generally not subject to the same vulnerabilities as biographic data. Faces, fingerprints, and irises are completely unique to individuals, and cannot easily be faked. In addition, each distinct biometric modality offers numerous unique identifying features, which, when used together, can dramatically increase identity assurance.

Multi-modal Biometrics

MorphoTrust is confident that a biometric entry-exit control system that incorporates multiple modes of biometrics is a more secure solution than the current biographic exit approach in place today.

Today, when a nonimmigrant arrives at a U.S. port of entry, and applies for admission to the United States by air or sea, the only biometrics that U.S. Customs and Border Protection (CBP) collects are fingerprints and photographs (but the photographs are often not suitable for use by face recognition technology). Because of this, many assume that an exit system should be based on a finger print matching system.

It is our view that DHS should change the entry process and collect additional biometrics from visitors—fingerprints for sure, but also photos of a quality that work with face recognition systems, and iris captures compliant with recently issued National Institute of Standards and Technology (NIST) standards.

Doing so would provide additional flexibility to CBP to employ a system that works most effectively in different airport environments. In some instances, this may include iris scans; in other instances, face recognition; and in still others, perhaps fingerprints.

Regardless, collecting multiple modalities of biometrics at the time of entry would provide CBP with more options for capturing biometrics at exit. CBP would have the ability to conduct contactless biometric capture using either face, fingerprint, or iris scans (or a combination thereof). This would allow operators to take advantage of the relative benefits of each biometric identifier and method of capture, such as accuracy, passenger throughput, convenience, and cost.

In this scenario, fingerprints would continue to be collected during enrollment, allowing for comparison against DHS's Automated Biometric Identification System (IDENT) database and the FBI's NGI database, which until recently was known as the Integrated Automated Fingerprint Identification System (IAFIS). This solution would continue to do that. However, the addition of iris and face recognition scans at the time of entry would provide the added security benefit of allowing matching against face recognition and iris databases maintained by the U.S. Department of

State and the U.S. Department of Defense, as well as other face databases maintained by state and local law enforcement agencies.

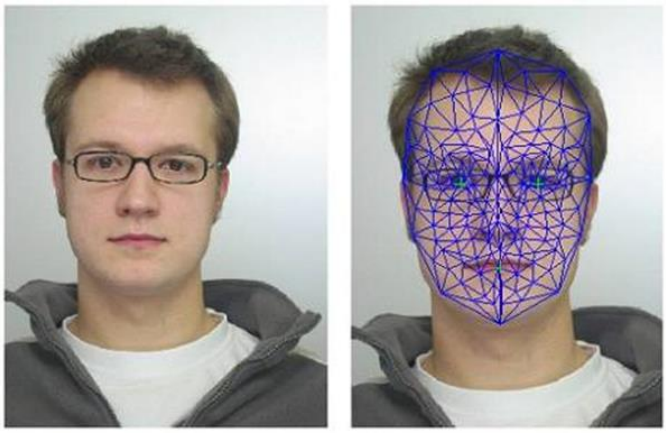
With multiple modalities (face, iris, and fingerprints) implemented, the primary modality used on a given day can be changed, mitigating the ability to plan for methods to spoof any single biometric. A multi-modal system ensures that each visitor would have at least one biometric identifier in the system that can be used to confirm identity. While each of the three biometric technologies has a relative margin of error, collectively they can ensure high probability matches on data sets with tens of millions of records and more, and can be used to reduce the impact of failed biometric capture (for instance, due to dry fingerprints).

Statistics from the Indonesian multi-modal national ID card project, for example, shows that there is only a 0.008% chance of false positive identification and a 0.18% chance of false negative identification on a database of over 100 million records.

In addition, multi-modal biometric entry/exit systems reduce processing times. For example, combination face recognition and document scanning systems can process a passenger in as little as 8 seconds. Iris scanning systems can capture and process an iris image in a few seconds. Contactless, finger-on-the-fly technology can read four fingerprints in as little as 3 seconds.

Face Recognition

Face recognition is not a new concept—police officers have been using face recognition for as long as there have been criminals. However, now the algorithms for face recognition have progressed to the point where software is much better at matching faces than the average humans is.



Illustrations of the areas used by a face recognition algorithm

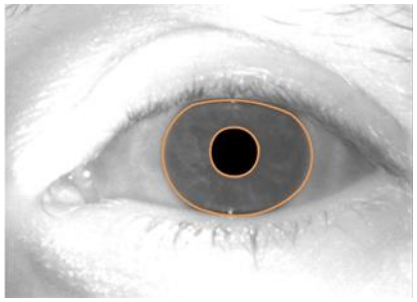
Face recognition is a potential solution for biometric entry/exit as high quality video cameras are already installed at most major airports. These cameras, if mounted in the gates used for international departure, could capture the faces of departing visitors. Face recognition has the additional security benefit of allowing matching against the Department of State's biometric database of visa applicants.

Iris Recognition

One biometric in particular – iris – bears additional discussion, in our view. In 2008, iris was still a niche technology. Today iris enrollment and verification devices have become reasonably priced, as a number of iris camera manufacturers have driven down the costs per unit with high quality image results. Additionally, the recent addition of iris to the NIST Personal Identity Verification (PIV) specifications has added certainty to the technology and gives it room to grow.

Iris recognition starts with capture of a photograph of the iris using a near-infrared illumination. The iris is extracted from the photo and the unique features are identified and converted into a small template. It is this template that is stored and then compared to a template created from the photograph taken when a person is requesting verification of identity. An iris template cannot easily be reverse engineered to the original iris photo thereby protecting the privacy of the traveler's biometric information.

Iris recognition is unobtrusive. The individual does not need to be aware of the collection taking place for a successful collection to occur. High resolution cameras have improved to the point that photographs taken from up to 3 meters away from the subject will have the desired quality, with good focus that is required for iris recognition.



Area within orange concentric circles is extracted for template creation.

Iris recognition systems are contactless and hygienic. There is no need to touch a surface that has been touched by thousands of travelers. This prevents the transmission of disease via contact.

Iris recognition systems are stable. The iris is an internal organ that is protected against damage and wear by the cornea. On the other hand, fingerprints are subject to wear, distortion and alteration through certain types of activities and manual labor. The iris is mostly flat, and its geometric configuration is mainly dictated by pupil dilation. This makes the iris shape far more predictable and stable than an individual's face.

Results are returned quickly. Iris templates are very small, and as a result, database searches are very fast. Current server hardware can match an iris template to tens of millions of templates in less than a second. This means that iris can provide a "lights out match" in a one-to-many scenario faster than any other biometric.

Iris recognition is highly reliable, with the ability to reach extremely low false accept

rates, comparable to that of any other biometric modality. In addition, considering fingerprints are sometimes associated with criminal behavior, iris may be less offensive to some subset of travelers.

Stand-off simultaneous face and dual iris capture

Additional benefits may be derived by stand-off dual capture units, which simultaneously capture both face and iris images. This is accomplished by the use of two cameras:

1. A high resolution near-infrared camera that takes a photograph of the irises.
2. A digital camera that takes a high resolution color picture of the face.

Today's dual face and iris cameras are of sufficiently high resolution that a photograph taken, with the appropriate lens and lighting, from the distance shown in the photograph below, still has the resolution necessary to perform accurate matches. With faster computer systems and advances in computer vision algorithms, these systems will just keep getting better.

AOptix *Insight*® dual face and iris capture at check-in

Stand-off technologies allow for photographs to be taken unobtrusively, in seconds, and can be configured to fit into natural chokepoints at airports—such as check-in counters, security checkpoints, or at the departure gate.

Within seconds, a stand-off simultaneous face and dual iris biometric collection device can take photographs of your face and eyes and send the images to a back-end search engine. Depending on the complexity of the search workflows, results can return in seconds. At natural document handling points, search results could be returned before the document examination is completed.

Contactless Fingerprint Capture Devices

There are also exciting advances in fingerprint capture devices that provide new options for exit configurations. Morpho has developed a contactless fingerprint capture solution called Finger-on-the-Fly. Other companies have developed similar technologies.

Speaking to our device, it captures four finger images with a single movement of the hand in less than a second. Its fast acquisition capability allows subjects to provide fingerprints while on the move, which makes it suited for high-traffic environments. This method of fingerprint capture also alleviates hygienic concerns when using a commonly touched surface.

Morpho Finger-on-the-Fly contactless fingerprint reader

Biometric Exit Systems Internationally

With this in mind, it is also worth noting that biometric entry/exit control systems are operating successfully in airports around the world. In fact, when talking about exit in the United States, we are often asked what other nations are doing.

Morpho was the first company in the world to deploy an eGate project based on face recognition and ePassports in Australia. SmartGate has since been expanded to New Zealand, processing a combined 15.1 million passengers since 2007. Currently, Morpho has deployed over 150 eGate systems in 24 international airports across 8 countries within 24 international airports, processing over 1 million passengers per month.

MorphoWay™ fully automated eGates

Other major deployments include fingerprint based systems in France and Indonesia, iris recognition systems in the United Kingdom and the United Arab Emirates, and face recognition systems in Germany and the Czech Republic. Many of these systems are not limited to ePassport holders of the host country. Of the systems mentioned, holders of second generation U.S. ePassports are able to use the Australia and New Zealand's SmartGate and the French Parafe, and the systems in France, the United Kingdom, Germany and the Czech Republic are open to all second generation ePassport holders of the European Union.

MorphoWay™ eGates read biometric information contained in travel documents and compare it with the document holder's biometric data.

Exit Controls for Land Border Ports of Entry

I can confidently say that, based on successful implementation around the globe, and using COTS solutions, biometric exit controls for airports, seaports, and pedestrian land border crossings can be implemented affordably and within a relatively short time frame. Vehicular land border crossings present a unique challenge—in part due to the need for infrastructure improvements at exit points, as well as the difficulties in capturing biometrics of passengers inside the vehicle, without slowing down border traffic.

Multi-modal biometric capture systems, such as dual face/iris cameras, could be configured within a gantry to capture biometrics of drivers and passengers while seated in their vehicles. Additionally, handheld iris/face/fingerprint readers can quickly capture biometrics (similar to the HIIDE™ and SEEK® devices used by the U.S. military) for all vehicle occupants quickly—but, this would require facilitation by a trained CBP officer.

With emerging and improving biometric capture technologies, additional options will be available in the future.

We would recommend addressing biometric exit controls at land border crossings through a series of pilot and demonstration projects, in advance of implementation at busy border crossings.

Conclusion

I believe that MorphoTrust speaks for much of the biometric industry when we say that a fully functioning biometric exit system is affordable, and can be implemented today without disrupting legitimate trade and travel. Other countries have successfully deployed and are operating biometric entry and exit controls at airports and other ports of entry. The Federal Government has already embraced multi-modal biometrics as a means to establish and verify identity.

We stand ready to work with the Congress, the Department of Homeland Security, and other stakeholders to help develop a biometric exit program that can be deployed within a short period of time and at a reasonable cost, making Americans safer while improving the traveler experience.

Thank you for the opportunity to address the Subcommittee on these important issues. I look forward to answering your questions.