Meeting Minutes

U.S. Government Facial Recognition Series
FORUM I: *Facial Recognition Technology — Baselining Uses and Legal Challenges*

Sponsored by the Federal Bureau of Investigation's Biometric Center of Excellence, in conjunction with the Office of the Director of National Intelligence (ODNI)

Date: August 31, 2011
Location: The Analytic Sciences Corporation (TASC) Heritage Conference Center, 4803 Stonecroft Blvd., Chantilly, Va.
Attendees: See Appendix

Overview and Objectives of Meeting | Mr. Tony Brown, Facilitator

Mr. Brown:

- Welcomed participants to the meeting.
- Introduced Mr. Richard Miller, TASC Security Manager, who reviewed the conference center use guidelines. He noted that the meeting is unclassified and that discussions should remain unclassified.
- Stated that this is the first of a four part series:
    - The goal of the forum series is to identify the primary legal and policy challenges to the deployment of facial recognition technology.
    - The next forum is scheduled for November 2, 2011 at BRTRC in Fairfax, Va.
    - Forum 2 topic is information sharing.
    - Forum 3 topic is privacy.
    - Forum 4 topic is TBD.

Welcome and Forum Preview | Mr. William Casey, Mr. Steve Burmeister, and Mr. Brown

Mr. Brown introduced Mr. Casey, Program Manager, Biometric Center of Excellence (BCOE), FBI

Mr. Casey:

- Welcomed participants.
- Explained that the BCOE is the focal point for FBI biometrics and is tasked with fostering conversation and outreach on biometrics.
- Stated the forum is intended to provide an opportunity for interagency dialogue about legal and policy challenges to facial recognition deployment.
- Noted that the forum series had been suggested by facial recognition technology stakeholders.

Mr. Casey introduced Mr. Burmeister, Assistant Deputy Director of National Intelligence for Science and Technology, Office of the Director of National Intelligence (ODNI)

Mr. Burmeister:

- Thanked everyone for allowing his involvement in the forum.
- Proposed that the group look at science based on DNA, quoting Mr. Milan Kundera: "The serial number of a human specimen is the face, that accidental and unrepeatable combination of features. It reflects neither character nor soul, nor what we call the self. The face is only the serial number of a specimen."
- Noted that facial recognition technology originated in the 1960s and has advanced each year.
- Posed the questions:
    1. Is the public ready for this rapidly developing technology?
    2. Can DNA mapping create a recognizable facial image?
- Stated that:
    1. The technology needn't be perfect, but it must work.
    2. It is necessary to understand and address policy issues while protecting privacy and civil liberties.
- Gave an example from his visit to the aircraft carrier U.S.S. Midway, docked in San Diego, where photos taken of each visitor verify presence at a certain place at a certain date and time.
- Noted that Scotland Yard used photos in an attempt to identify and locate perpetrators of the recent London riots.
- Said that these examples show that facial recognition uses are available, in use, and play a significant role in our lives.
- Announced that ODNI has started working with Mr. B. Scott Swann, FBI, on facial recognition applications.
- Stated that facial recognition has uses not only within the intelligence community, but also in law enforcement, industry, and military communities.
- Encouraged attendees to discuss facial recognition challenges, quoting Mr. Bill Gates: "Your most unhappy customers are your greatest source of learning."
- Applauded the participation of attendees and encouraged everyone to engage in the debate.

Mr. Brown presented the following findings from questions posed to the attendees during the registration process:

- The majority of attendees have worked with facial recognition technology for one year or less.
- Most in attendance work in legal and policy sectors.
- Most reported that the primary impediments to broad acceptance and deployment of facial recognition technology are legal and policy concerns, including privacy and data sharing.

Mr. Brown reviewed the format for the rest of the day:

1. An overview of the current status of facial recognition technology;
2. A panel discussion including representatives of the FBI, ODNI, Department of Defense (DoD), and Department of Homeland Security (DHS)/U.S. Immigration and Customs Enforcement, covering current uses of the technology and the legal and policy challenges it poses;

3. Selection by the participants of four topics posing the greatest challenge to the effective use of facial recognition technology;
4. Breakout group discussion of the four topics, in which each group would create a clear problem question, identify stakeholders, list the legal and policy obstacles, and brainstorm potential solutions.

Mr. Brown introduced Dr. Jonathon Phillips, Electronics Engineer, National Institute of Standards and Technology (NIST) and Dr. Richard Vorder Bruegge, Senior Photographic Technologist, Operational Technology Division, FBI

Facial Recognition: The State of the Art with Q&A | Dr. Vorder Bruegge and Dr. Phillips

Dr. Vorder Bruegge and Dr. Phillips:

- Gave a joint presentation on the capabilities of facial recognition technology, including social, legal, and ethical challenges.
- Identified factors affecting the reliability of facial recognition, including: automatic vs. human recognition, forensics, eyewitness accounts, and facial expressions.
- Reviewed the steps comprising facial recognition:
    1. finding the face
    2. finding the center of the eyes
    3. "cutting out" the face
    4. enrolling the face
- Noted that human ability to recognize faces varies according to the level of familiarity with the subject.
- Stated that humans are capable of using outside information — such as clothing, gait, hair and posture — more accurately for identification purposes than the actual face.
- Demonstrated the Colorado State University facial recognition capture system, FaceL Facile Face Labeling. The FaceL application does not store images, but uses an algorithm to store recognition numerically.
- In response to audience questions, the following was discussed:
    - It is possible to use numbers to recreate someone's facial image based on the algorithm, but the image would not be an exact match to the actual image.
    - Because algorithms improve regularly, most systems save images over time to match against several sets of images.
    - It is possible that one standard algorithm could enable a number set across platform, but it is unlikely to occur in our lifetime because algorithms evolve so frequently.
    - There are some limitations to algorithms, which identify the face by locating the center of the eyes, such as if the subject is wearing sunglasses.
    - The most accurate facial recognition technology currently available will result in 93 percent correct identification in a closed set gallery of 1.6 million distinct file image photos.
    - Because the face constantly changes, accuracy improves with more images of the same individual, against which the database can search for a potential match.
    - When using mug shots or other types of photos, older people match better than younger because older people's faces change less dramatically over the same period of time.
    - Clustering involves the collection of images of the same person. Clustering scenarios are most often used in digital photo libraries, such as Facebook.

    - There are two common types of clustering errors: incorrect split identity and incorrect merge identities.
    - Lighting plays a role in clustering errors (i.e. photos taken outside vs. inside); however, these errors have not been quantified.
- Several examples of successful face recognition uses were provided, including:
    1. A fugitive from California living in North Carolina in 2009 was recognized from his North Carolina driver's license records, despite the photos being taken 14 years apart. As a result, the FBI is now negotiating Memorandums of Understanding (MOUs) with state Departments of Motor Vehicles (DMVs) to utilize their facial recognition systems to search for fugitives.
    2. A criminal enterprise involved multiple IDs sold to individuals — in one state alone, more than 14,000 cases were discovered. The mastermind of the crime was located utilizing the clustering technique.
- Automated Face Detection And Recognition (AFDAR) software, used for clustering images from videos with still photographs, was discussed. AFDAR was developed for the Office of Military Commissions to assist in reviewing large quantities of available video, such as surveillance video containing Guantanamo detainees involvement in terrorist acts.
- A false accept, or false positive, occurs when the system accepts an invalid identity claim. A false reject, or a false negative, occurs when the system rejects a valid identity claim. The usual rate is 1 in 1000. The technology has significantly progressed since 1993 — from Face Recognition Technology (FERET) to the 2010 Multiple Biometric Evaluation (MBE) Challenge — through eight evaluations, six challenge problems, three biometrics and 250,000 images, resulting in a decreased error rate of .3 percent from 79 percent.
- It was emphasized that verification and all FBI investigations must be peer reviewed, with a second reviewer confirming the outcome.
- The experts noted that the face is not the only factor considered in facial recognition; ears and tattoos are also studied. Facial hair can be a source of error, so technologists are working on ReproMatch, a 3D tool to augment facial recognition.
- Two scenarios involving facial verification were offered:
    1. One was the 2002 verification of the 1985 *NATIONAL GEOGRAPHIC* image of an Afghani woman.
    2. Another was a case where a passport photo was brought into question when it was matched to the defendant's photo.
- Research challenges in facial recognition technology include:
    1. Mimicking humans' use of many characteristics (face, gait, body, voice, etc.) for identification; algorithms use just one characteristic. We need to incorporate more from the human visual system into algorithm design.
    2. Detecting facial images that are off-angle or low resolution.
    3. Large volumes of data demand smaller templates and "smarter" searches.
    4. Standards are needed for examination practice, including a basis for conclusion and automated tools for feature extraction.
    5. Duplicative research should be eliminated.
    6. More data sets are needed for testing and basic research.
    7. Policy/legal issues need to be overcome, and information should be shared across agencies.

Current and Near Future Facial Recognition Applications Panel | Mr. B. Scott Swann, Mr. Neal Gieselman, Mr. T. Gregg Motta, and Mr. Steven W. Cooper

1. *Mr. Swann, Science and Technology Identity Intelligence Lead (ODNI):*

- The FBI/NIST relationship goes back several years. NIST develops benchmarking, standards, and steering the research community with challenges. Data is sourced from academics and independent research boards (IRB). IRB approvals are necessary to gather research data, which can be provided to vendors.
- Carnegie Mellon's Face Recognition Study, *Face of Facebook: Privacy in Age of Augmented Reality,* harvested facial images from Facebook and Match.com without logging into the sites and found that:
    1. One of out of ten people had a pseudonym on Match.com.
    2. Surveillance photos identified individuals using the images from their Facebook accounts and gathered social security numbers and other identifying information as a result.
    3. Computers are much less accurate than humans at recognizing faces.

2. *Mr. Gieselman, Lead Engineer, DoD/Biometrics Identity Management Agency (BIMA):*
    - BIMA is tasked with operational maintenance of DoD Automated Biometric Identification System (ABIS), which is on its second generation since 2009. ABIS includes fingerprint, face, iris, palm, and latent prints.
    - DoD has a much lower throughput (rate of processing information) than the Integrated Automated Fingerprint Identification System (IAFIS).
    - ABIS accepts multiple modalities, although intermixing and inconsistent data quality are problems.
    - ABIS has 6 million enrollments, and most come in as multi-modality.
    - Fingerprints and iris matches are 90 percent accurate, and face is 28 percent accurate.
    - Facial biometrics have the lowest accuracy of biometric measurements, and the accuracy rates range monthly from 28 to 40 percent. Four BIMA tests over the last year showed a potential to increase accuracy to 60 percent.
    - It is important to know and manage your data — all data has value — and train your algorithm.
    - BIMA and the biometrics community need to define "better" facial searching. BIMA would like to introduce the term "forensic facial searching," and have the community discuss and define it.
    - BIMA shares its data with the FBI's Criminal Justice Information Services (CJIS), NIST, Massachusetts Institute of Technology (MIT)'s Lincoln Labs, National Gang Intelligence Center (NGIC), National Security Agency (NSA), and some vendors, as needed.
    - MOUs vetted by legal personnel are used, and a U.S. person's Personally Identifiable Information (PII) is scrubbed.
    - With the exception of latent print searches, ABIS is a lights out (automated) system.

3. *Mr. Motta, Section Chief, Digital Evidence Section, FBI:*
    - Police departments decide how to use biometric technology, which is then used to try court cases.
    - Cited the *Daubert v. Merrell Dow Pharmaceuticals, Inc.* case, which says the judge is the gatekeeper for admitting technical and scientific evidence.
    - The National Institute of Justice performed a study of eyewitness error rates, which are very high.

- The media has a protected interest in photographing people in public. Constitutional and case law support their right to do so.

4. *Mr. Cooper, Executive Director, Law Enforcement Information Sharing Initiative (LEISI) PMO, U.S. Immigration & Customs Enforcement, DHS:*
   - Facial recognition is a tool to be utilized like any other law enforcement tool.
   - Transparency will assist in gaining public approval.
   - Emphasis should be placed on establishing guilt or innocence as quickly as possible.
   - There is a need to discuss what technologies are available, and what their standing is in a court of law.
   - What is the difference, from a legal perspective, between the media taking a photo and law enforcement doing the same thing?

Audience Q&A:

Q. Has DHS considered the difference between taking airport photos and law enforcement taking photos?
A. The public accepts border entrance and exit photos. [Mr. Cooper]

Q. Has DHS found a high accuracy algorithm it could test in video in airports?
A. This would depend if you are looking at border entry/exit or law enforcement. [Mr. Cooper]

Q. What is the target error rate for facial recognition? Is it the same as DNA?
A. The error rate is contextual. For example, J. Edgar Hoover's study of signature recognition found that 70 percent of people could not detect their own signature. [Mr. Motta]

Q. Are we aiming for probable cause or conviction?
A. Jury instructions are so broad that there is no threshold for the various biometric modalities. However, investigative tools are contested all the time. Forensic use is the highest bar we need to achieve, but that should be the bar we aim for overall. [Mr. Motta]

Q. What can be done to combat falsified passport photos?
A. DHS inspects documents and performs secondary checks. Each agency will use its expertise to try to prevent false positives and false negatives. [Mr. Cooper]

Q. Can closed circuit television (CCTV) images from a public street be used to identify someone?
A. It depends on the context. CCTV footage has limited use for facial recognition. [Mr. Motta] In London, where surveillance cameras are everywhere, only about 5 percent of collected video/images are useable; for CCTV to capture quality facial video, there must be a controlled environment. [Dr. Vorder Bruegge]

Breakout Group Reporting and Facilitated Discussion | Mr. Brown

The four issues that will be discussed by the breakout groups are as follows:

1. Blue Group: Performance Levels
2. Red Group: Public Information/Social Media
3. Yellow Group: Data Sharing
4. Green Group: Civil Liberties Considerations

Blue Group — Performance Levels:

Problem Question: What are acceptable performance levels across various government contexts?

Q. Is it possible to define a performance level, since there isn't as much experience using face versus other biometrics?
A. It depends on whether facial recognition is being used as a primary or secondary identifier.

Q. Is it possible to define a common performance level for use across government stakeholders?
A. It is difficult, given the multitude of stakeholders. The TSA pilot has limited verification.

Q. Would standards help?
A. There are some standards: American National Standards Institute (ANSI)/NIST for collection and American Association of Motor Vehicle Association (AAMVA) for driver's license standards. But there is a lack of case law applying these standards to the face.

- Mr. Mike Garris, NIST, suggested a model that categorizes performance level profiles to applications, allowing stakeholders to identify which levels apply to them.

- Mr. Swann suggested a black box study to determine the advantages of human input versus technology, and suggested there is value to human intervention in "fly or no fly" decisions.

- It was noted that the few times facial recognition has been challenged in court, prosecutors have simply shown the probe and match images to the judge, who has concurred with the facial recognition results on sight alone.

- An attendee noted that facial recognition is simply an enhancement of an inherent human ability, with which Dr. Vorder Bruegge agreed in the case of small data sets. With large sets of data, however, facial recognition increases the level of error but also increases the possibility of finding someone who may otherwise go unfound.

Red Group — Public Information/Social Media:

Problem Question: How should the federal community proceed when private citizens can access PII using the Internet, public data, and photography in the public domain?

A. The government is prevented from using that information for research because of the perception that it will lead to a criminal investigation. There has to be a predicate, a clear

reason, for government to proceed with a search (i.e., a person who posts a photo to a social networking site does not knowingly consent to its use by the government).

- The public perceives that there is a lot of technology available to law enforcement, yet they feel it would be reprehensible to use the technology to invade privacy.

- ODNI published guidance in July 2011 regarding Internet use and open source data. The guidance is at a very high level and written for IT professionals regarding usage, but is not intended to impose any legal restrictions.

Q. How long is data retained?
A. TSA keeps its data on suspicious activity for 25 years.

Yellow Group — Data Sharing:

Problem Questions: What are the information sharing criteria? When do you share data and with whom?

Q. Does the existing policy framework establish a precedent to sharing facial recognition data?
A. Interagency sharing depends on different missions and different stakeholders.

Q. Is the data different from what is out there now? Are existing MOUs sufficient if they cover sharing data? Is facial unique, or is it simply another biometric?
A. Face is inherently PII. Show a face and you immediately can know the person's name, unlike a fingerprint or DNA. All biometrics are PII. Lack of standards hampers sharing. [Dr. Vorder Bruegge]. The U.S. Dept. of Health and Human Services handles faces differently. [Mr. Motta]

Q. Who are the stakeholders in information sharing?
A. There are five distinct communities to consider:
1) National Security (intelligence)
2) Defense
3) Criminal Justice/Law Enforcement
4) Research/civilian
5) Public/commercial/private sector, which breaks down to advocacy and business interests

Q. How is facial recognition different from data that is currently being shared, such as fingerprints?
A. The difference is public perception.

Q. What are the risks to information sharing?
A. Risks include not being able to guarantee the quality of data at a level that people might expect. Standards development is a possible mitigation of this risk. Another risk is using human subjects in testing. Risk mitigation should include transparency, education, and working with all stakeholder groups. It is important to get consent in data collection and to be aware that there are different forms of consent.

Q. Is facial recognition different from other biometrics?

A. It depends. Research use of facial images versus other biometrics is treated differently because other biometrics' PII can be masked. But with facial images, the researcher may know/recognize the individual.

Green Group — Civil Liberties Considerations:

Problem Question: How can civil liberties be balanced with government need to use social media and its availability in the public domain?

- The group determined that this is an area of currently evolving law that does not directly address known issues. Policy isn't keeping up with technology, which will always be the case. As a result, we can apply existing law, have Congress address it directly with agency input, and/or rely on the courts to determine policy.
- Next steps in civil liberties regarding facial recognition technology should include continued interagency discussions/work, inclusion of advocacy groups (such as the ACLU), and determining what will be acceptable to society.

Q. Are there other technologies that have had similar issues?
A. Facial recognition is different from other biometrics because faces are visible and, therefore, collection is relatively unobtrusive. Other biometrics, including DNA, fingerprint, etc. are more intrusive to collect.

- It was noted that the more secretive the government is about its use of facial recognition technology, the harder it will be to gain public approval.

Summary of Proceedings | Mr. Brown

Insights and questions:

1. Do existing policies and regulations that govern use and sharing of other biometric data (e.g. fingerprints) sufficiently apply to the use and sharing of facial images?
2. Are facial images fundamentally different from other biometrics and PII? To what extent or in what ways? How can policy or legislation address those differences?
3. One critical factor in determining conditions for sharing facial images is the degree to which consent is obtained at image capture. For instance, an image collected by a hidden surveillance camera should be handled differently from an image collected for a driver's license.
4. Government use of publicly available facial images requires reasonable and articulated suspicion.
5. Can/should we develop policies to address shortcomings in the law, or should we rely on the legislature to make the law?

Closing Remarks | Mr. Casey

- Mr. Casey expressed thanks for participating and requested that people register for the next forum, to be held on November 2, 2011, and to ask their colleagues to participate.

Adjourn