Meeting Minutes

U.S. Government Facial Recognition (FR) Legal Series
FORUM III: *Striking the Balance – A Government Approach to Facial Recognition Privacy and Civil Liberties*
Sponsored by the Federal Bureau of Investigation's (FBI) Biometric Center of Excellence (BCOE), in conjunction with the Department of Defense (DoD)

Date: March 14, 2012
Location: FBI National Academy, Quantico, Virginia
Attendees: See Appendix

Welcome | Mr. William Casey, Program Manager, FBI BCOE

- Mr. Casey welcomed participants to the third forum of the series. He thanked the presenters for their contribution.

Mr. Casey introduced Mr. John Boyd.

Welcome | Mr. John Boyd, Director, Defense Biometrics and Forensics, Assistant Secretary of Defense, Research and Engineering, DoD

- Mr. Boyd discussed DoD's prioritized list of missions, stating that nearly all of them have a linkage to biometrics and forensics. These include the following:
    - Counterinsurgency and counterterrorism
    - Early deterrence and defeat of aggression
    - Counter weapons of mass destruction
    - Space operation
    - Homeland defense
    - Humanitarian relief operations
- We must ensure privacy and civil liberties protections throughout the biometric processes (collect, match, store, manage, and share) and the operational/business processes. These include data analysis and the decisions and resulting intelligence/military/law enforcement operations that come from the biometric data analysis, such as raids, checkpoint operations, detainee operations, etc.
- There is very little policy or other express legal authority to collect and use biometric and related information. This is an area in need of policy development.
- In developing policy initiatives, the following must be considered:
    - Information technology standards
    - Business rules (i.e., human, operational, technical, and functional factors)
    - Roles, responsibilities, and missions of government agencies
    - High-level governmental goals (e.g., warfighter support, law enforcement assistance, data protection, individual privacy and civil liberties protection, etc.)

Forum Preview and Opening | Ms. Jennifer Alkire McNally, Management and Program Analyst, FBI BCOE and Forum Facilitator

- Ms. McNally invited the audience to actively participate in the discussions. Presentations are intended to initiate dialogue across the agencies represented at the forum.
- Ms. McNally reviewed the Series objectives: to bring together members of the federal law enforcement/national security community who use or plan to use FR to:
    - Understand the unique opportunities and challenges presented by FR
    - Determine the issues that should be addressed by policy
    - Provide a venue to share lessons learned
    - Develop a framework for guidance for government use of FR
- Through Forum 1, which was held on August 31, 2011, participants developed an understanding of the capabilities and limitation of FR technology, discussed current and future FR applications, and discussed the primary legal/policy challenges faced by participants. Information sharing and privacy were prioritized as the two most challenging policy issues. Subsequent forums were designed to address these two issues.
- Forum 2, held on November 2, 2011, focused on information sharing. Through the forum, participants developed an understanding of the governing legal framework, discussed federal and agency-specific biometric sharing policies, discussed the role of system interoperability in data sharing, and applied existing authorities to hypothetical scenarios to determine legal/policy permissibility of particular facial image sharing activities in various contexts.
- In Forum 3, participants will explore where the appropriate balance lies between federal law enforcement/national security use of FR and privacy/civil liberties interests and rights.
- The primary objective of Forum 3 is to identify gaps in, or unaddressed areas of, FR law and policy from a privacy/civil liberties perspective. The outcome of this effort will be a roadmap to guide privacy-and civil liberties-sensitive use of FR by the federal government.

Ms. McNally introduced Professor Peter Swire.

Privacy and Facial Recognition: Legal Landscape | Professor Peter Swire, C. William O'Neill Professor of Law, Moritz College of Law, Ohio State University

- Professor Swire introduced two perspectives on U.S. government use of FR:
    (1) Faces are exposed to the public. Law enforcement has always watched people in public, and it makes good sense to use modern information tools to do this more efficiently.
    (2) FR is a new and different way for law enforcement to acquire real-time identification and location information about citizens. This raises new questions.
- FR is subject to legal authorities including the U.S. Constitution, statutes, and case law. It is also subject to society's values, concerns, and sensibilities about what uses are acceptable.
- <u>Fourth Amendment of the Constitution</u>
    - Protects citizens against unreasonable government searches and seizures
    - Generally requires probable cause to obtain a warrant to search and/or seize
    - Historically, courts have not required a warrant to observe a person in public, reasoning that it is not a "search" and, therefore, does not implicate the 4th Amendment. This supports government use of FR in a public space.

    - However, in *U.S. v. Jones*, decided in January 2012, the Supreme Court held, in a 9-0 decision, that the use of a GPS device to monitor a person's car's location was a "search" for purposes of the Fourth Amendment and required a warrant.
    - Under *Jones*, that the car is "in public" is not determinative. Rather, the majority emphasized the physical attachment of the device to the car and the length of time (4 weeks) that the car was tracked led the Court to determine that an unreasonable search had occurred and, as such, a warrant was required.
    - The minority opinion in a recent Montana case, in which State investigators secretly videotaped a worker's comp claimant around town, followed the reasoning in *Jones*, stating that people do retain a reasonable expectation of privacy while in public.
    - "Consent" exception to the Fourth Amendment: a person can consent to a search or seizure by the government. But what constitutes consent? Implied consent and the Third Party Doctrine are "ill suited to the digital age," according to Justice Sotomayor. This issue has direct implications for FR surveillance.
- First Amendment of the Constitution
    - Protects freedom of speech, association, religion, etc.
    - Justice Sotomayor: "Awareness that the government may be watching chills associational and expressive freedoms." Surveillance technology provides information about a person's location, which reveals "a wealth of detail about her familial, political, professional, religious, and sexual associations."
    - *NAACP v. Alabama* speaks to the associational freedom doctrine.
- Due Process/Accountability
    - Standard procedures, audits, accountability and due process are important to mitigate risk associated with databases containing private or other sensitive data about citizens.
- Equal Protection
    - Use great caution in focusing surveillance activities on people based on religion, race, gender, politics, ethnic origin, or other protected class.
- The Privacy Act of 1974
    - Prevents disclosure of information contained in a federal government system of records in which the information is retrieved by name or identifier unless individual consent.
    - Subject to "routine uses," which include major law enforcement exceptions.
    - Privacy Act data is subject to access and redress requests by the individual.
    - Privacy Act applies only to personally "identified" or "identifiable" information (PII). A need for OMB guidance to define PII. The determination of whether data is PII or not is being made more difficult by technology.
- Federal Video Voyeurism Prevention Act of 2004
    - Ban on knowingly capturing an image of the "private area" of an individual on federal lands. Similar state laws exist.
    - Suggests that cameras are intrusive.
- Wiretaps Statutes
    - Imposes strict limits on government inception of phone calls and bugging for sound (Title III).
    - Applies only to audio, not to video.
- Stored Communications Act
    - Requires a medium level of strictness to obtain stored records held by a third party (e.g., a subpoena for photos and/or names from Facebook)

- Location Information
    - Lower courts are split as to whether a warrant is needed to access a person's cell phone location information. Cell phones allow tracking of people in unprecedented ways. Precedents for cell phone location tracking may predict doctrine for FR surveillance.
- Normative considerations
    - Just because an activity does not violate the law does not necessarily mean it is a good thing to do.
    - Tests for what is good to do:
        (1) Friends and family test (does the average person think it is a good thing to do?)
        (2) New York Times test (if it were on the front page of the New York Times, would the media portray the activity positively or negatively?)
        (3) Data minimization (use the least amount of sensitive information necessary for the activity – e.g., facial detection rather than facial recognition)

- Questions from the audience:
    - **Q: Do guidelines exist to help government agencies determine at what point their surveillance activities go from an acceptable law enforcement tool to an unreasonable search?**
        - **A:** It is okay for a police officer to watch a person walk down the street, but at some point, the visual tracking becomes too much. Precisely when is undetermined.
        - Professor Swire encouraged participants to refer to the resource in the handout folder developed by the Department of Justice's (DOJ) Global Justice Information Sharing Initiative entitled, *Justice Agency Framework for Understanding Privacy Risks in Biometrics*, which lists fifteen factors to consider when developing or evaluating a biometric use.
    - **Q: Is potential mission creep the primary concern with FR?**
        - **A:** Yes. Negative responses to FR are not necessarily a function of how the data is intended to be used at collection but how it might be used down the road. Technology makes new uses of the data very attractive.
        - Innovating technology is not the problem. Rather, the use of the technology for a purpose other than that for which it was collected is the problem. If an agency wants to use data that was collection for one purpose for a new purpose, the individuals from whom the data was collected must be notified and consent to the new use. If consent is unreasonable (e.g., certain law enforcement and intelligence purposes), the new use must first be properly vetted and approved. This implicates due process.
    - **Q: Is a sign notifying people that a camera is in use enough to avoid legal concern?**
        - **A:** It depends on whether, in the particular context, the sign feels like actual consent or not. If there is a feeling that surveillance is everywhere, there is likely also a feeling that people are not free to act as they would otherwise.
    - **Q: Do you think there is a generational divide with regard to reasonable expectation of privacy?**
        - **A:** There is clearly a different expectation among people of different ages, but although young people are more likely to expose personal information, they do exhibit privacy concerns. Danah Boyd has conducted significant research on this issue.

After a break, Ms. McNally introduced Matthew J. Olsen and Jonathan E. Rackoff.

Privacy and FRT: Federal Policy Landscape | Matthew J. Olsen, Detailee, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) and Jonathan E. Rackoff, Assistant General Counsel, OMB

- There is no specific privacy-related OMB guidance relative to biometric identification.
- Technology does not have inherent privacy implications aside from the technology's accuracy. Rather, the context in which it is used requires privacy and civil liberties protections.
- Several relevant authorities include the following:
    - The Privacy Act of 1974 – speaks to the requirement of a system of records notice (SORN), which is a notice published in the Federal Register identifying all potential uses of data contained in a federal system of records and the legal authority by which the data will be used.
    - OMB Memorandum: M-03-22: *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* – sets forth the concepts behind and the guidelines for a Privacy Impact Assessment (PIA).
    - National Security Presidential Directive (NSPD) 59/Homeland Security Presidential Directive (HSPD) 24 – entitled *Biometrics for Identification and Screening to Enhance National Security*, this 2008 policy requires federal agencies to make available to other agencies, to the fullest extent permitted by law, "all biometric and associated biographic and contextual information associated with persons for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security."
- Under the Office of Science and Technology Policy (OSTP), the National Science and Technology Counsel (NSTC) has published several relevant papers:
    - *Privacy & Biometrics: Building a Conceptual Foundation*, published in 2006, provides a primer on facial recognition technology, privacy, and their intersection.
    - *Biometrics in Government Post 9/11*, published in 2008, highlights key U.S. Government initiatives in advancing the science of biometrics and its utilization in meeting pressing operational needs.
    - *2011 National Biometrics Challenge* provides an overview of current challenges related to strengthening the scientific foundation of biometrics and improving identity management system capabilities. It also clarifies biometrics-related priorities for Federal agencies.
- Appendix J to NIST 800-53, Revision 4 of which is currently out for public comment, provides a standard set of controls to provide privacy of federal information systems and organizations.

- Questions from the audience:
    - **Q: How do societal perceptions play into the difference between U.S. policy and European countries' policy on FR?**
        - **A:** Countries like the United Kingdom tolerate greater use of surveillance cameras than the U.S. The public's awareness of cameras in public spaces is less important than the public's understanding of why the cameras are there – for what purpose images are being collected, whether the collected images will be retained, etc. Transparency is the key.

- **Q: How should privacy concerns arising from cloud computing be addressed?**
  - **A:** Cloud computing presents a unique context in which data collected from multiple sources is stored in a central, remote location. To adequately address issues such as redress and third party sharing of data, there must be a discussion of roles and responsibilities.
  - The data collector is responsible for data it stores in a cloud. The collector needs to know to whom its data will be shared, for what purposes, whether each of these are within the scope of initial collection, whether appropriate notice was provided to the individuals from whom data was collected, etc.

Ms. McNally introduced Mr. Tony Brown.

The Impact of Public Perception on Law and Policy | Tony Brown, Senior Vice President, BRTRC

- Attempts to measure the impact suggest that public opinion affects policy 75% of the time. The more salient an issue, the more impact opinion has on policy development.
- People tend to be supportive of emerging technologies; however, public opinion can change and often polarize when issues arise in the political arena.
- A lack of facts does not prevent people from developing a strong opinion. In the absence of facts, people make assumptions. Once opinions are formed, they often overlook evidence to the contrary. For these reasons, it is important for the government to clearly communicate the facts surrounding particularly salient issues, such as FR, with the public at the outset.
- People generally fall into one of three categories of concern regarding privacy in new technologies:
  (1) Privacy Fundamentalists: most concerned about privacy. Support stricter privacy-protective laws.
  (2) Privacy Unconcerned: least concerned about privacy. Benefits of technology outweigh the risks. Do not favor expanded regulation. Smallest percentage of people.
  (3) Privacy Pragmatists: weigh the pros and cons and then decide. Generally willing to give up some privacy if something important is provided in return. Majority of people.
- According to a SEARCH survey, people were willing to see the benefits of biometric identification and downplay the risks immediately after 9/11. The further from 9/11, the more privacy and civil liberties concerns arise.
- Confusion and misunderstanding around emerging technologies argues for early engagement to educate and counteract vocal minorities (e.g., advocacy groups, media, popular culture).
- Public trust is key.

Ms. McNally introduced Mr. Louis Grever.

Facial Recognition: The Rule of Threes | Mr. Louis Grever, Retired Executive Assistant Director, Science and Technology Branch, FBI

- Public trust is fundamental. The federal community must engage in open dialogue with the public so they understand what the government is and is not doing with FR.
- The public's opinions of the use of FR by other agencies, the private sector, and international entities will impact the public's opinions about U.S. government use of FR.

- There are three realities:
  (1) What you do
  (2) How it is perceived
  (3) The politics
- Justice Sotomayor's opinion in *U.S. v. Jones* is a harbinger for what is to come with regard to use of surveillance technologies that are ubiquitous and less visible.
- Engage Congress, the public, and privacy advocacy groups now to establish public trust. This should be a coordinated effort across the government to get the message out about how FR is really being used by the government.
- 3 challenges:
  (1) Listen **-** It is important to listen to concerned citizens and detractors. They often have important perspectives that we need to think through and use to inform our actions. Read the privacy groups' concern letters.
  (2) Inform – Provide the facts about the capabilities and limitations of FR and its uses. Don't oversell the technology. Be clear about its risks.
  (3) Convince - Win hearts and minds with evidence of the promise that FR holds to dramatically improve how we investigate and prosecute criminals and protect the nation.

- Questions from the audience:
  - **Q: What do you think about a national ID card (e.g., Real ID)?**
    - **A:** The public is not ready. The arguments in favor of it, security and efficiency, have not been sufficiently compelling. Perhaps it should be left to the states if it is pursued by government at all.

The forum broke for lunch. When the group reconvened after lunch, Ms. McNally introduced the four panelists of the next session: Mr. Samuel P. Jenkins, Jr., Mr. Christopher Lee, Ms. Teresa Stasiuk, and Ms. Elizabeth Withnell.

Biometrics Privacy Policies by Agency | Mr. Samuel P. Jenkins, Jr., Director for Privacy, Defense Privacy and Civil Liberties Office, DoD; Mr. Christopher Lee, Directorate Privacy Officer, Science and Technology Directorate, Department of Homeland Security (DHS); Ms. Teresa Stasiuk, Privacy Advisor, Civil Liberties Protection Office, Office of the Director of National Intelligence (ODNI); and Ms. Elizabeth Withnell, Chief, Privacy and Civil Liberties Unit, Office of the General Counsel, FBI

Mr. Jenkins:
- Scope of FR use in DoD includes intelligence/counter terrorism, law enforcement (limited), and access control
- Three criteria that must be met before a facial image is collected include whether there is legal authority to collect, whether collection is Constitutional, and whether collection is socially acceptable (the Washington Post test).
- DoD collection facial images only directly from individuals, for a narrowly specified purpose, and with notice/consent (where possible). Images are not collected on First Amendment activities. Image accuracy is also a collection concern.
- If an agency wants to use a photo for a purpose other than that which was intended at collection, the agency must add that purpose to the notice and republish in the Federal Register.

- DoD maintains specific criteria for FR searching. The person represented in the probe image must have done something to trigger a screening (consent or involvement in a pertinent incident), and verification may be required to ensure authorization to search. For a person's image to be included in a database against which a probe image is searched against, the person must have done something to be included in this population, his/her record must be retained only for the requisite period, and only minimal information about the person should be provided unless "need to know," per the Privacy Act.
- Dissemination from one federal agency to another requires a routine use be established in the sending agency's SORN, including to whom and for what purpose the data will be shared.
- Image quality is critical for image conversion and storage. The Privacy Act requires that PII be relevant, accurate, and timely.
- Are facial images PII? Policy does not explicitly say so, but facial images uniquely identify an individual even if the original image is not retained.
- When possible, images should be deleted after comparison. Screener should be provided only relevant information on matches (i.e., red/green/yellow checks), masking sensitive or unnecessary data.
- Accuracy is a concern. An individual cannot be denied a benefit s/he is entitled to because of an inaccuracy. Therefore, a secondary process, such as human verification, must be used to screen out inaccurate results.
- Redress is a legal responsibility of the agency.

Mr. Lee:
- Primary FR use cases at DHS include the Biometrics Optical Surveillance System (BOSS), law enforcement FR/high resolution cameras, and the biometric entry/exit program.
- DHS is taking high quality, although not FR quality, photos through the biometric entry/exit program. FR quality photos could be built into the program.
- Governing biometric privacy authorities include as follows:
    - HSPD 24
    - Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (Public Law 104-208)
    - Secure Travel and Counterterrorism Partnership Act of 2007
    - Enhanced Border Security and Visa Entry Reform Act of 2002 (Public Law 107-173)
- There is limited authority specific to surveillance cameras. Authority is needed to fill this gap.
- Another unaddressed issue involved unmanned aerial vehicles (UAVs). UAVs identify movement across the border between the U.S. and Mexico. It cannot see faces or license plates. Should we monitor legal border crossings? What if a UAV is used to monitor a drug safe house? How long is appropriate? What if it turns out not to be a drug safe house?

Ms. Stasiuk:
- Privacy and civil liberties are important to consider throughout the FR process. Public trust is critical.
- When collecting facial images and associated data, ask the following questions:
    - Under what authority was the data collected? Did collection occur under the parameters of that authority?
    - How was the data collected? What techniques were used? (This goes to the Fourth Amendment "search" issue.)

    - Did you get consent to collect? If so, in what form? If not, is there authority to support this decision?
    - For what primary purpose was data collected? How will you ensure that this purpose is complied with?
- When searching against facial images, ask the following questions:
    - What are you searching against? Is there authority to support searching against this database?
    - What is the quality of the images being searched and/or searched against? How does this impact accuracy of the search results?
    - How are results validated? What secondary measures are used to verify a match?
- When accessing and/or disseminating images and associated data, ask the following questions:
    - What disclosures are provided to a receiver of search results regarding the data's accuracy?
    - Is there a published SORN that clearly governs dissemination?
    - Are routine uses clearly established?
    - If the data is not contained in a Privacy Act system of records, are Memoranda of Understanding developed that provide privacy safeguards?
- When retaining and/or disposing of images and associated data, ask the following questions:
    - Are policies developed that prescribe privacy controls?
    - How long do you keep the data? How does this length of time relate to the documented elements of the SORN?
    - See NIST Special Publication 800-53, Appendix J, *Privacy Control Catalog: Privacy Controls, Enhancements, and Supplemental Guidance*, currently out for public comment
- Policies should also exist for purposes of redress. These should include as follows:
    - How may individuals access data about them to check its accuracy?
    - If an individual determines that his/her data is inaccurate, how does s/he have the inaccuracy corrected?
    - What exemptions to the opportunity for redress exist?
    - How is this process communicated to individuals?
- Trust by the American people is key. Trust must be established through transparency.

Ms. Withnell:

- The FBI's face-related initiatives include Next Generation Identification; Facial Analysis, Comparison, and Evaluation (FACE) Services; and BCOE applied research and development.
- Before using FR, ask what authority exists to use photographs to identify individuals?
- In the absence of specific authority, look to general authority and extrapolate. For example, statutory law grants the FBI authority to obtain and use identification records and information; however, it is unclear whether this includes photos. *28 USC § 534 (2005).*
- Agencies might engage in rulemaking to provide a firmer foundation on which to use FR. Rulemaking would include an explanation of legal authority and description of uses. It would be put out for comment and the agency would go from there to formalize.
- Data retention raises major privacy issues.

After a break, Ms. McNally introduced Theodore "Ted" Yoneda.

Gaps in FR Privacy Law and Policy: Exploration of Use Cases | Facilitated by Mr. Theodore K. Yoneda, Attorney Advisor, Office of the General Counsel, FBI

Hypothetical Scenario #1: A large number of individuals gather at a special event (e.g., a major sporting event, a music concert, a protest rally near the White House). Assume that during such an event, law enforcement officials believe a known or suspected terrorist (KST) might be masquerading as a spectator or protester. The officials want to use facial recognition technology to identify the KST and monitor his activities.

Hypothetical Scenario #2: An adult female is known (by her friends) to have a contentious relationship with her boyfriend. Her friends also know that the couple had individual Facebook accounts and both were frequent users of the social media service. One morning the woman fails to report to work, and the boyfriend also cannot be located. After friends provide law enforcement officials with recent photographs of the woman and her boyfriend, officials seeks authority to search the photographs against Facebook images with the hopes of returning a match. Such a match could reveal the location of the Internet Protocol (IP) address either of them are using to access their respective Facebook accounts.

- The discussion of issues raised in these scenarios included:
    - Collection:
        - Is there authority to collect the images?
            - Is there express authority to identify individual via photographs? If not, is there implied authority? (See *28 USC § 534* re: U.S. Attorney General's authority to collect, store, and disseminate identification records and information)
            - See also Executive Order 12333 for collection guidelines for the Intelligence Community.
            - Facial images for identification have always been used, first from memory, then through sketches, then through photographs. Does social custom provide authority?
            - Video is distinct from photographs in that video collects images in "real time." How does this impact the legal analysis?
            - What if instead of watching the video in real time, investigators record the video to view later? This introduces the privacy/civil liberties risk of collecting and retaining images of innocent individuals.
        - What constitutes collection?
            - See 28 USC § 534 (law enforcement) and Executive Order 12333 (intelligence).
        - Notice should be provided to the individual(s) from whom images are being collected.
            - What constitutes notice may depend on the context. An easily visible sign at a sporting event that explains the purpose of collection and subsequent uses may satisfy the notice requirement. What about a White House rally?
        - Purpose drives collection.
        - The *Jones* decision and the privacy issues that arise through "tagging" photographs on social media sites raise the civil liberties question of whether there is a fundamental right of a person to be left alone.
    - Search:

- What authority allows the FR search of an individual for identification purposes?
- What authority allows a search against a particular database?
- What verification procedures exist to validate a match?
    - Investigation should not continue unless there is human verification of a match.
- The purpose of the search drives what is searched and how the search is conducted.
- In the second scenario, law enforcement's ability to search the victim's Facebook account without a warrant may depend on whether the victim is deceased, in which case the victim has little or no privacy rights, or simply missing, in which case further analysis may be required.
- Are there different rules for publicly available data, such as Facebook profile pictures?
    - Historically, publicly available information has received decreased privacy protection; however, the *Jones* decision (GPS case) may have changed that. The length of time that tracking occurred and the non-consensual physical touching of the suspect's vehicle by law enforcement may be the factors that the U.S. Supreme Court relied on in *Jones*. In that case, these factors wouldn't apply to FR in this context and, therefore, may not be relevant precedent.
    - The privacy settings of an individual's Facebook or other social media account determine legal permissibility to search.
    - What if the victim is missing and assumed to be alive, and her friends provide a photo of the woman to law enforcement. Can law enforcement conduct a Google image search of publicly available images?
    - What if the photo provided by the woman's friends was taken without the woman's consent? Does this matter?

- <u>Access and Dissemination:</u>
    - This includes:
        - Internal access of a facial image,
        - Searching a facial image against another agency's system (image is not retained by the other system), and
        - Sharing data with another agency's system (image is retained by the other system).
    - Only those with a legitimate "need to know" should have access to data.
        - Access controls, such as passwords and clearances, and access/dissemination audits help ensure compliance.
    - Notice should be provided to the data owner when its data is being used.
        - If there is an exigent threat that requires data sharing, notice must not be given.
    - Data should be encrypted before sharing.
    - Data should be minimized to the extent possible before sharing.
        - One data minimization example cited is a Green/Yellow/Red flag return notification, in which the contributing agency (that which collected the images and associated data) assigns a level of sensitivity to all data in its system. When another agency searches against the

database, a return will be accompanied by a green, yellow, or red flag. Green, which accompanies data of low sensitivity, indicates that all information is sharable. Yellow, which signifies mid-level sensitivity, indicates that the contributing agency will not disclose the information through the automated return, but contact information for the contributing agency is provided for further information. Red accompanies highly sensitive data. It indicates a "silent hit" in which the user receives no return information, but the contributing agency receives an electronic notification that an agency hit against its information.

- Similarly, only information that is necessary for a specific purpose should be accessed from an internal system.
- If data is being shared from or through a system that has a published SORN under the Privacy Act, recipient agency must follow Privacy Act guidelines.
- The contributing agency is the data owner and is responsible for access integrity through the data's lifecycle.
    - If the contributing agency received corrected or updated information, it must not only modify the information in its own system but must also notify all recipient agencies to correct and update its information.
    - If a private entity, such as a sports arena, collects the images and shares with a federal agency for a law enforcement or national security purpose, who is the data owner and, therefore, has ultimate responsibility for data integrity?
- A Memorandum of Understanding (MOU) should formalize the use requirements of the agency to which data is shared.

- <u>Retention and Disposition:</u>
    - Retention schedules are dictated by the provisions of the SORN. There must be a nexus between collection purpose and length of data retention.
    - Where images are stored or where video is collected for later review, privacy implications arise and should be mitigated.
    - Technology should be designed to mimic human processes. Did it find what it was trying to find? If not, do not retain.
    - Where agencies between which data is shared have different retention schedules, National Archives and Records Administration (NARA) rules govern.
    - Policy should be established to update and correct stored data at regular intervals and immediately upon receipt from a contributing agency that the data requires correction or updating.

After a break, Ms. McNally reconvened the forum.

Roadmap for FR Law and Policy Development | Ms. McNally

- Based on the discussion generated through this FR legal/policy series, a roadmap to guide FR use that safeguards privacy rights and civil liberties in federal law enforcement and national security contexts will be developed.
- Ms. McNally presented a draft roadmap outline. She asked participants to consider whether this framework successfully addresses the community's goals for FR privacy policy development and, if not, how it should be modified to do so.

- The outline will be posted on a wiki through the legal series webpage for forum participants to help populate the issues that should be addressed in the document. The resulting outline will be added to and vetted at Forum 4.
- The resulting document will be published as an addendum to the NSTC Subcommittee on Biometric and Identity Management's revision to its 2006 publication, *Privacy & Biometrics: Building a Conceptual Foundation*.
- Ms. McNally asked participants to contact her with names of people who were not present but should be involved in this initiative.

Ms. McNally thanked everyone for their participation and reintroduced Mr. William Casey for closing remarks.

Closing Remarks | Mr. Casey

- Mr. Casey thanked the audience and the presenters for their participation.

Mr. Casey reintroduced Mr. Boyd for closing remarks.

Closing Remarks | Mr. Boyd

- Mr. Boyd thanked everyone for their participation.
- He encouraged participants to work together to develop policy needed for FR to be an effective tool while protecting individuals' privacy and civil liberties.

Adjourned at 1630

Appendix: Attendees (partial list)

Last	First	Agency	Title
Andrew	Emily	Department of Homeland Security	Senior Privacy Officer
Baldwin	Charles Reid	Department of Homeland Security	Deputy Chief
Ballard	Traci	Department of Homeland Security	Attorney, Information Disclosure Officer
Beale	Steven	Ohio State University	Policy Analyst
Becker	Mark	Department of Homeland Security	Senior Policy Advisor
Bhatia	Anita	Department of State	Attorney Advisor
Blackburn	Duane	MITRE	Multi-Discipline Systems Engineer
Boyd	John Michael	Department of Defense	Director, Defense Biometrics and Forensics
Brown	Tony	BRTRC	Senior Vice President, Public Affairs SME
Buhrow	William C.	Biometrics Identity Management Agency	Organizational Operations Chief
Calogero	Valerie	Federal Bureau of Investigation	Assistant Attorney General
Casey	William	Federal Bureau of Investigation	Program Manager
Cavis	Les	Federal Bureau of Investigation	Unit Chief
Clark	Lloyd	U.S. Marshals Service	Senior Inspector
Consaul	Sheila	BRTRC	Director, Communication Strategies
Coppock	Craig	Defense Intelligence Agency	Forensic/Biometric Specialist
Cutshall	Charles	Department of Homeland Security	Policy Analyst
Danisek	Debra	Department of Homeland Security	Privacy Analyst
DeLeon	Anthony	Federal Bureau of Investigation	Assistant General Counsel

Devabhakthuni	Bharatha	Federal Bureau of Investigation	Management and Program Analyst
Dolf	Shelley	Federal Bureau of Investigation	Assistant General Counsel
Espina	Dr. Pedro I.	Office of Science and Technology Policy, Executive Office of the President	Executive Director, National Science and Technology Council
Ford	William	Department of Justice	Division Director
Frenkel	Jonathan	Federal Bureau of Investigation	Assistant General Counsel
Garofolo	John S.	IARPA/National Institute of Standards and Technology	Senior Advisor for Strategic Planning
Givan	Natalie	Federal Bureau of Investigation	Management and Program Analyst
Gonzalez	Jose	Defense Logistics Agency	Physical Security Specialist
Grever	Louis E.	Federal Bureau of Investigation, Retired	Former Executive Assistant Director, S&T Branch
Hawkins	Frederick	Department of State	
Horbatak	Michael	BRTRC	Strategic Support
Jenkins	Samuel P.	Department of Defense	Director for Privacy
King	Maurice	Department of Homeland Security	Management and Program Analyst
King	John E.	Federal Bureau of Investigation	Assistant General Counsel, Unit Chief
Lee	Christopher	Department of Homeland Security	Privacy Officer
Linger	Jodie	Federal Bureau of Investigation	Management & Program Analyst
Look	Timothy	Department of Defense	Forensic SME Level IV
Loudermilk	James	Federal Bureau of Investigation	Senior Level Technologist
Marks	Mary	Federal Bureau of Investigation	Assistant General Counsel
Martin	Dennis	Federal Bureau of Investigation	Management & Program Analyst

Mathews	John	Department of Homeland Security	Senior Privacy Analyst for Intelligence
Mazel	Joe	Federal Bureau of Investigation	Assistant General Counsel
McNally	Jennifer	Federal Bureau of Investigation	Management & Program Analyst
Meinhardt	Kristin	Federal Bureau of Investigation	Assistant General Counsel
Miller	Christopher S.	Department of Defense, Biometric Identity Management Agency	Identity and Mission Assurance
Murphy	Justin	Department of Justice	Senior Law Enforcement Advisor
Murphy	Paulette	Department of Navy	Attorney
Oleinick	Lewis D.	Defense Logistics Agency	Chief Privacy and FOIA Officer
Olsen	Matthew J.	Office of Management and Budget	Detailee, Office of Information and Regulatory Affairs
O'Reilly	Sean	Department of Homeland Security	Identity Management Specialist
Patnode	Jay “Mike”	Federal Bureau of Investigation, Terrorist Screening Center	Biometric Program Manager
Phillips	William	Department of Defense, Biometric Identity Management Agency	Plans and Policy Branch Chief
Rackoff	Jonathan E.	Office of Management and Budget	Assistant General Counsel
Reeves	Terrance	Department of Homeland Security	Privacy Analyst
Reimers	Gerald F.	National Ground Intelligence Center	Head Agency Counsel
Santa Ana	Steven	Federal Bureau of Investigation, Terrorist Screening Center	Biometric Program Manager
Schilling	Linda Beth	National Institute of Standards and Technology	Director, Project Management Office
Sessions	Andrew	Naval Criminal Investigative Service	Lead Biometric Policy Analyst
Shaw	Adam	Department of Defense, Biometric Identity Management Agency	Policy Analyst
Sherman	Michael	Federal Bureau of Investigation	Assistant General Counsel

Sprouse	Doug	Federal Bureau of Investigation	Management and Program Analyst
Swire	Peter	Ohio State University	Professor of Law
Velvel	Douglas R.	Department of the Navy	CDR
Vorder Bruegge	Dr. Richard	Federal Bureau of Investigation	Senior Photographic Technologist
Withnell	Elizabeth	Federal Bureau of Investigation	Assistant General Counsel, Unit Chief
Yoneda	Theodore	Federal Bureau of Investigation	Assistant General Counsel
Young	Brian A.	Federal Bureau of Investigation	Assistant General Counsel
Young	Carla E.	Bureau of Alcohol, Tobacco, Firearms and Explosives	Senior Counsel, Field Operations
Zoladz	Bradley	Federal Bureau of Investigation	Training Instructor