Privacy Impact Assessment
for the

Security and Video Quality for the Public Safety Statement of Requirements Project

April 1, 2009

Contact Point
Cuong Luu
Command, Control and Interoperability Division
Science and Technology Directorate
(202) 282-8000

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Security and Video Quality for the Public Safety Statement of Requirements (SoR) project is a research and development effort funded by the Department of Homeland Security's (DHS) Science & Technology (S&T) Directorate. S&T is funding Noblis Inc., a nonprofit science and technology organization, through a cooperative agreement to conduct several research efforts, one of which is to examine facial recognition requirements in emergency response operations. S&T is conducting a Privacy Impact Assessment (PIA) because research staff will use images collected from individuals during this research project. This PIA will only cover the research and testing activities conducted during this project.

Overview

Title 3 of the Homeland Security Act assigns S&T the responsibility for conducting research in support of the Department's mission. Under Subchapter 3 §182, "the Secretary, acting through the Under Secretary for Science and Technology, shall have the responsibility for conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department.

S&T is funding Noblis Inc. through a cooperative agreement to examine facial recognition requirements in the law enforcement and emergency response communities. These requirements will include, but are not limited to, image resolution, megapixels of an image, and the background of an image. This is part of a broader effort, supported by a cooperative agreement between S&T and Noblis, to examine security and video quality requirements for all law enforcement and emergency response application areas, including facial recognition technology. This research will enable the law enforcement and emergency response communities to fill the need for a comparison study between an automated facial recognition system and the use of trained human experts in the field. The anticipated benefit of the work described in this PIA will be the potential development of facial recognition technology that can allow the law enforcement and emergency response communities to conduct facial identification quickly (e.g., to identify suspects or missing children in the field).

Objectives

The objectives of the project will be to establish a strong technical foundation to guide the law enforcement and emergency response communities as they define requirements (e.g., image resolution, megapixels, and background of image) and architecture frameworks, conduct gap analyses, and develop interface standards for emergency response communications. This project will also examine the benefits of using automated facial recognition technologies versus trained human experts in the field. The customers generally are the law enforcement and emergency response communities, but the project specifically targets local, state, tribal, and Federal agencies that currently use some form of facial recognition, whether automated or human.

FERET Database

Under this cooperative agreement, Noblis has entered into a Memorandum of Agreement (MOA) with the University of Maryland to examine facial recognition requirements using facial images of volunteers stored in the Facial Recognition Technology (FERET) database. (All references to "photos" or "images" in this PIA refer to the existing FERET database images. No other photos are created for, collected by, or used in the project.) These images were collected under the FERET program, sponsored by the Department of Defense (DOD) Counterdrug Technology Development Program Office, between December 1993 and August 1996.

University research staff will conduct the research using the facial images of the volunteers stored in the FERET database. The FERET database contains only images of volunteers willing to participate in the FERET program, and the database does not include names, contact information, or any other PII of participating individuals. Since the goal of the FERET program is to develop new techniques, technology, and algorithms for the automatic recognition of human faces according to the website, the research described in this PIA is consistent with this goal.

The use of these photos is critical to the requirements gathering process at this stage in the research for two main reasons: (1) the FERET database images are of a standard size, quality, and orientation (frontal image as opposed to full or partial profile), which provides a basis for comparison and evaluation; and (2) the targeted customer population (i.e., the law enforcement community) already uses similar photos for the purposes of facial identification, thus allowing researchers to utilize relevant photos to inform the collection of requirements.

University research staff will obtain FERET database access from the National Institute of Standards and Technology (NIST) and use the database images for the testing and evaluation portion of the project. Once granted permission to use the FERET database, the university research staff will follow the Color FERET Database Release Agreement, which prohibits further distribution, publication, copying or dissemination of any images stored on the database. The Release Agreement can be found at: http://face.nist.gov/colorferet/release_agreement_v1_.html. During the experiment, university research staff will use trained human experts from the university and existing commercial off-the-shelf (COTS) technologies to match a selected image from the FERET database with the same image from the FERET database while viewing all images in the database. The only images used during this project come from the existing database.

Testing Procedure

Once the photo is obtained from the database, university research staff will assign each photo a corresponding internal photo control number with no relationship to the individual. This internal photo control number serves as a dummy name and allows researchers to determine whether image matches are correct or incorrect. For example, if a trained human expert matches "image 123" with "image 124," then the researchers can verify that it is an incorrect match.

Using the images collected from the FERET database, university research staff will conduct facial recognition testing using both trained human experts from the university and automated COTS systems. The facial recognition testing described in this PIA cannot (and will not attempt to) identify the individual

himself/herself; rather, the testing will attempt to recognize matches of identical images—indicating whether the technology and human experts can match a select sample image from the FERET database with the same image in the FERET database from a larger group of images.

University research staff will provide both the trained experts and COTS systems with an artificial watch list of approximately 10 photos. Again, all photos are from the existing FERET database collected with the consent of the volunteers. University research staff will ask the trained human experts and the automated COTS system to match the photo from the watch list to a larger group of volunteer photos streaming across a computer monitor. Each trained human expert may have his/her own approach to this matching activity; researchers will observe how these different approaches may or may not impact the accuracy in matching the photos.

Ultimately, the types of data produced through this process will consist of Match and No Match ratios of success and failure. This data will allow university research staff to evaluate human assessments versus those of automated systems; the project will also afford university research staff the opportunity to dissect the advantages and disadvantages of human and automated assessments.

The project will use the results of test matching activities to identify what requirements are necessary to successfully match an image to the corresponding internal photo control. This project will not involve the development of facial recognition technologies.

Security

University research staff will store the data in a physically secure facility that meets the physical access standards established in the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (i.e., locked 24/7, specific permission for entry, escorted entry for non-background checked and CJIS-certified personnel). University research staff will store electronic data in a secure, password protected, permission-based file system that will only allow access to administrators, developers, and the test application itself. All administrators and developers have undergone background checks and are certified by CJIS. Only University research staff with a need to know will have access to this data.

Participants

The following groups will participate in this project:

- DHS Science & Technology Directorate: S&T's role in the project is limited to providing funding. S&T will receive quarterly reports and an annual report to discuss the status of the research and an analysis of the results; no deliverable reports to S&T will contain any PII, and S&T will not receive any other deliverables. S&T will not have access to, and will not be authorized to grant access to, the FERET database images used in the project.
- Noblis: Noblis will deliver quarterly reports and an annual report to discuss the status of the research and analysis of results. Noblis will not have access to nor receive any information collected during the research activities.

- University of Maryland CapWIN program: The University of Maryland provides access to both trained human experts and the Capital Wireless Information Net (CapWIN) program, a University of Maryland program comprised of university research staff. CapWIN has established partnerships between the State of Maryland, the Commonwealth of Virginia, and the District of Columbia. University research staff will perform the match testing activities. University research staff will examine FERET database images from volunteers for the purpose of gathering requirements necessary for developing future facial recognition technologies and to analyze the advantages and disadvantages for the public safety community's use of trained human experts in facial recognition versus an automated system.

University research staff will only use photos from the existing FERET database. Researchers will retain the FERET database images for the duration of the project to conduct testing and evaluation, and then the research staff will purge the research records of all PII at the conclusion of the project.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

University research staff will collect volunteers' images from the FERET database and will then assign a corresponding internal photo control number. This internal photo control number will help to make certain that image matches are correct or incorrect. University Research staff will purge the FERET database images from research records at the conclusion of the project. No additional PII will be collected or generated during this project.

1.2 What are the sources of the information in the system?

The FERET database is approximately 8.5 gigabytes. The FERET database was originally developed under the FERET program, sponsored by the Department of Defense Counterdrug Technology Development Program Office, between December 1993 and August 1996. This database was specifically created to facilitate the development of new techniques, technologies, and algorithms for the automatic recognition of human faces. Additional information on the FERET program and DOD's development of the FERET database can be found at: http://www.itl.nist.gov/iad/humanid/feret/feret_master.html. The FERET database contains only images of volunteers willing to participate in the FERET program, and the database does not include names, contact information, or any other PII of participating individuals. NIST serves currently as the Technical Agent for distributing the FERET database. The database is available to researchers via NIST website download only, and users can only gain access to the database once they receive approval from NIST. The images are available in ppm format; no other image formats or methods

of distribution are permitted. The project will only use images in this database, which is online at: http://face.nist.gov/colorferet/.

1.3 Why is the information being collected, used, disseminated, or maintained?

University research staff will collect the information to gather the requirements necessary to compare and successfully match photos from the database and then use the corresponding internal control numbers to verify correct or incorrect matches, thus informing the development of future facial recognition technologies. The objectives of the project will be to establish a strong technical foundation to guide the law enforcement and emergency response communities as they define requirements (e.g., image resolution, megapixels, and background of image) and architecture frameworks, conduct gap analyses, and develop interface standards for emergency response communications. The anticipated benefit to the law enforcement and emergency response communities is to fill the need for a comparison study that shows how advantages and disadvantages differ between an automated facial recognition system and the use of trained human experts in the field.

1.4 How is the information collected?

All images stored on the FERET database were collected directly from the volunteer. Researchers will access and download the images via FERET's website.

1.5 How will the information be checked for accuracy?

All images used in this project are from the FERET database. This project does not manipulate the images in any way. There is no correlation of the images to the identities of individuals; therefore accuracy, in terms of the correlation of a person to a photo, is not relevant for this project.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information

The Homeland Security Act of 2002 [Public Law 1007-296, §302(4)] authorizes the Science and Technology Directorate to conduct "basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs." In exercising its responsibility under the Homeland Security Act, S&T is authorized to collect information, as appropriate, to support R&D related to improving the security of the homeland.

1.7 Privacy Impact Analysis: What privacy risks were identified given the amount and type of data collected, and how were those risks mitigated?

The privacy risks associated with the collection of images are that the information may be collected without the individual's knowledge, and that the information may be used by unauthorized personnel or for an unauthorized or harmful purpose.

To mitigate this risk, university research staff will only use images from the existing FERET database for this project. Individuals whose images appear in this database have previously signed a Volunteer Release Form for inclusion in research projects such as this. Researchers will only collect and use volunteered images during the testing and evaluation process. University research staff will purge research records of all PII at the conclusion of the project, thus ensuring that the individual's image cannot be used for an unauthorized purpose. University research staff will use the images for research purposes only.

To mitigate the risk of unauthorized access, University research staff will store the data in a physically secure facility that meets the physical access standards established in the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (i.e., locked 24/7, specific permission for entry, escorted entry for non-background checked and CJIS-certified personnel). University research staff will electronically store data in a secure, password protected, permission-based file system that will only allow access to administrators and developers. All administrators and developers have undergone background checks and are certified by CJIS. Also, University research staff can only access the FERET database using valid username and password provided by NIST.

In addition to these privacy risks, there is the risk of unintentional sharing of the PII. To mitigate this risk, all PII collected during the testing activities will be destroyed at the conclusion of the project. In addition, university research staff will ensure that all deliverables, reports, or subsequent publication resulting from this project will not contain any PII.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 What are the uses of the information?

University research staff will use the photos to conduct testing to gather requirements necessary for developing future facial recognition technologies. The objectives of the project will be to establish a strong technical foundation to guide the law enforcement and emergency response communities as they define requirements (e.g., image resolution, megapixels, and background of image) and architecture frameworks, conduct gap analyses, and develop interface standards for emergency response communications. University research staff will provide the photos to trained human experts and existing COTS technologies, along with an artificial watch list, and instruct both the human experts and the technologies to make accurate matches. Ultimately, the project will attempt to determine what requirements are necessary to match successfully the photos based on facial recognition. The types of data produced through this process will consist of Match and No Match ratios of success and failure. This data will allow researchers to evaluate human assessments versus those of automated systems; the project will also afford researchers the opportunity to dissect the advantages and disadvantages of human and automated assessments. In turn, this data will serve as a study on the requirements needed to match photos to one another successfully. The anticipated benefit to the law enforcement and emergency

response communities is to fill the need for a comparison study between an automated facial recognition system and the use of trained human experts in the field. This project will not involve the development of actual facial recognition technologies.

2.2 What types of tools are used to analyze data and what type of data may be produced?

University research staff will use existing COTS facial recognition technologies to match a test photo from the artificial watch list against a larger group of photos. Individuals with formal training and expertise in facial recognition from the University of Maryland will also attempt to make these matches. The types of data produced through this process will consist of Match and No Match ratios of success and failure. This data will allow university research staff to evaluate human assessments versus those of automated systems; the project will also afford researchers the opportunity to dissect the advantages and disadvantages of human and automated assessments. In turn, this data will serve as a study on the requirements needed to match photos to one another successfully. The anticipated benefit to the law enforcement and emergency response communities is to fill the need for a comparison study between an automated facial recognition system and the use of trained human experts in the field. This project will not involve the development of actual facial recognition technologies.

2.3 Does the system use commercial or publicly available data? If so, please explain why and how it is used.

University research staff will not use commercial or publicly available data during this project.

2.4 Privacy Impact Analysis: What types of controls are in place to ensure that information is handled in accordance with the above described uses?

University research staff will store the data in a physically secure facility that meets the physical access standards established in the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (i.e., locked 24/7, specific permission for entry, escorted entry for non-background checked and CJIS-certified personnel). University research staff will electronically store data in a secure, permission-based file system that will only allow access to administrators, developers, and the test application itself. All administrators and developers have undergone background checks and are certified by CJIS.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

University research staff will retain the images from the FERET database for the life of the project; university research staff will purge research records of all PII at the end of the project. University research staff will only retain the volunteers' images for testing and evaluation purposes. The project's period of performance currently stands to expire on June 30, 2009. S&T will not have access to, be authorized to grant access to, or retain any PII for this project.

3.2 How long is information retained?

S&T will not retain any PII. University research staff will retain the images for the life of the project, after which all images will be destroyed. The period of performance currently stands to expire on June 30, 2009.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. The S&T Records Retention Officer approved the use of General Records Schedule 20 to cover all program control files.

3.4 Privacy Impact Analysis: What are the risks associated with the length of time data is retained and how are those risks mitigated?

A privacy risk associated with retention is the unauthorized use of data. To mitigate this risk, University research staff will destroy all PII at the conclusion of the project to ensure that the information cannot be used for an unauthorized purpose.

Another privacy risk is the unintentional sharing of data. To mitigate this risk, University research staff will ensure that only authorized personnel have access to PII and that deliverable reports to S&T contain no PII (i.e., no names, driver's license numbers, or photos will appear in any project reports).

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Neither S&T nor its contracted researchers will share the information with any internal organizations.

4.2 How is the information transmitted or disclosed?

Neither S&T nor its contracted researchers will transmit or disclose information to any internal organizations.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, what are the privacy risks associated with the sharing and how were they mitigated?

There is no internal sharing of the PII collected during this project.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Neither S&T nor its contracted researchers will share the information with any external organizations.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Neither S&T nor its contracted researchers will share the information with any external organizations.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Neither S&T nor its contracted researchers will share the information with any external organizations.

5.4 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and how were they mitigated?

There is no external sharing of the PII collected during this project.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Yes. All volunteers in the existing FERET database signed a Volunteer Release Form, which provided explicit notice of and obtained consent for the use of their images for facial recognition research purposes.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes. Individuals had the opportunity to decline participation in the FERET database when they were originally approached between December 1993 and August 1996. The FERET database only includes images and does not include names or contact information for participating individuals; therefore, there is no way the individuals can be contacted by NIST and given the opportunity to decline specifically for this research project. Again, the database only consists of willing individuals who signed a Volunteer Release Form during the initial collection of images.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Yes. Individuals had the right to consent to particular uses of the information. These uses of the information were outlined in the Volunteer Release Form. By signing the Volunteer Release Form, the volunteers agreed to the particular uses of the information. This database was specifically created to facilitate the development of new techniques, technologies, and algorithms for the automatic recognition of human faces.

6.4 Privacy Impact Analysis: How is notice provided to individuals, and how are the risks associated with individuals being unaware of the collection mitigated?

The risk to individuals would be the collection of PII without notice or consent. To mitigate this risk, all volunteers whose images are included in the FERET database signed a Volunteer Release Form, which provided explicit notice of and obtained consent for the collection and use of information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Individuals are not permitted to gain access to their information. No name or identifying information is associated with the images; therefore, the only way for an individual to locate his or her photo would be to review all images in the database, thus exposing the other images.

7.2 What are the procedures for correcting inaccurate or erroneous information?

The existing FERET database consists only of volunteers' images; no other information (i.e. name, address, phone number) is collected or stored on the database. All images were collected directly from the volunteer. University research staff will match the photos against each other; therefore, there is no foreseeable possibility of collecting inaccurate or erroneous information.

7.3 How are individuals notified of the procedures for correcting their information?

Again, the existing FERET database only consists of volunteers' images; no other PII, including contact information, is linked to the images. Thus, volunteers were not notified of procedures for correcting their information, as there was no information that could be corrected.

7.4 If no formal redress is provided, what alternatives are available to the individual?

The FERET database consists of volunteers who willingly signed a Volunteer Release Form. These individuals had the opportunity to either participate or refrain from participation at the time the Volunteer Release Form was supplied.

7.5 Privacy Impact Analysis: What privacy risks are associated with the redress available to individuals and how are those risks mitigated?

A privacy risk associated with redress is that an individual would be unable to access or correct any erroneous or inaccurate information. To mitigate this risk, the database only contains the images of volunteers who willingly signed a Volunteer Release Form. Additionally, no other personal identifiers were collected or are linked to the image; therefore, there is no foreseeable possibility of collecting erroneous or inaccurate information.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

University research staff will store the data in a secure, password protected, permission-based file system that will only allow access to administrators and developers with a need to know. University research staff will limit access to those directly involved in the testing activities.

8.2 Will Department contractors have access to the system?

Yes. Only university research staff working directly on the project will have access to the FERET database.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All DHS S&T personnel that will accept reports on the project received initial and annual privacy awareness training. S&T will provide web-based privacy awareness training to all university research staff involved in the project. The training will provide guidance to research staff on how to properly safeguard, store, and handle PII.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The S&T Chief Information Officer has determined that C&A is not required for this project.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

University research staff have their own set of technical safeguards protecting against harmful access and misuse of data related to the project. University research staff will store electronic data in a secure, password protected, permission-based file system that will only allow access to administrators and developers with a need-to-know. All administrators and developers will have undergone background checks and will be certified by CJIS. Only those University researchers with a need to know will have access to the images used in this project. In terms of auditing measures, the secure, password protected, permission-based file system will be stored on a Windows server which logs invalid log on attempts.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The risk to privacy would be unauthorized access to the PII. To mitigate this risk, University research staff will not share PII outside the research team. To enhance security of the PII, the University research staff will store data in a physically secure facility. This set up meets the physical access standards established in the FBI CJIS Security Policy (e.g., locked 24/7, specific permission for entry, escorted entry for non-background checked and CJIS-certified personnel). University research staff will store electronic data in a secure, password protected, permission-based file system that will only allow access to administrators and developers with a need-to-know. All administrators and developers will have undergone background checks and will be certified by CJIS.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

This project is a research effort funded by S&T Directorate to determine the necessary requirements for developing future facial recognition technologies. This project will not develop any new programs or systems; it will only use existing COTS technologies and compare those technologies against trained human experts.

9.2 What stage of development is the system in and what project development lifecycle was used?

The technologies involved in the project are available commercially off the shelf.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

Yes. Facial recognition technologies could raise privacy concerns. To address these concerns, University research staff will only utilize the images of volunteer participants and will only utilize the images for research purposes.

The purpose of this research is to evaluate the requirements for successful facial recognition; therefore, there is no intent to transfer any technologies to operational components of DHS. The results of this research will inform the development of future facial recognition technologies.

Approval Signature

Original signed and on file with the DHS Privacy Office.

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security