



UNITED STATES DEPARTMENT OF COMMERCE  
National Institute of Standards and Technology  
Gaithersburg, Maryland 20899-

MEMORANDUM FOR Mei Ngan

OCT 20 2015

From: Charles Romine, Director *CR*  
Information Technology Laboratory

Subject: Determination for ITL Project #ITL-0012, entitled, "Face and tattoo recognition research and evaluations with Michigan State Police collected data"

On October 19, 2015, the Director, Human Subjects Protection Office (HSPO) determined that your research is not human subjects research.

Before starting your work you must:

- Submit the following documents to Office of the Chief Counsel (OCC) at [nistcounsel@nist.gov](mailto:nistcounsel@nist.gov) for review. An OCC attorney assigned to the project will contact you.
  1. Data Transfer Agreement between Michigan State Police, Dataworks Plus, and NIST
  2. NIST Human Subjects Research Determination Form with the following attachments:
    - Schematic Face and Tattoo Data Usage, 9/3/2015
    - Steven G. Beatty (MSP) email 10/7/2015
    - Biometrics Research Laboratory (BRL) Policies
  3. This memorandum with the attached Director, Human Subjects Protection Office (HSPO) Determination Memorandum, along with a clarification email between HSPO and the principal investigator.
- Provide a fully signed copy of the Data Transfer Agreement to Ginger White.

Once the signatures and approvals are complete, and you have provided the signed copy to Ginger White, you may start your work.

You are responsible for:

1. Conducting this project as outlined in the above documents as this determination is valid only for this project,

**NIST**

2. Submitting revised documents if you propose to make any changes to this project as the change may affect the current determination (e.g., an updated determination form that incorporates the changes with a new version number or date with highlighting or track changes, and /or listing the specific changes in a cover memo). You may implement the changes to the project only after being notified in writing,
3. Notifying the Human Subjects Protection Office through your ITL Lab Office of changes to any agreements that may affect this determination,
4. Keeping other NIST offices, (e.g., Office of Acquisitions and Agreements Management, Technology and Partnership Office, etc.), and external collaborators informed about this determination or any approved changes to the project as appropriate,
5. Notifying your Supervisor and the ITL Lab Office when the project is complete, and
6. Maintaining complete records about the determination for this project from inception to completion.

If you have any questions, please contact Jim St. Pierre.

**Attachments:**

- Director, HSPO Memorandum of 10/19/2015, with 10/19/2015 clarification email
- NIST Human Subjects Research Determination Form with the following attachments:
  - o Schematic Face and Tattoo Data Usage, 9/3/2015
  - o Steven G. Beatty (MSP) email 10/7/2015
  - o Biometrics Research Laboratory (BRL) Policies

cc: Craig Watson, Group Leader  
Shahram Orandi, Division Chief  
Charles Romine, Director, ITL  
Anne Andrews, Director, Human Subjects Protections Office  
Office of the Chief Counsel

## NIST Human Subjects Research Determination Form

### **Instructions:**

If proposed work/project involves (1) humans, (2) biological specimens from humans, or (3) data or information about humans, use this form to determine if your work meets the definition of research with human subjects. This is the first step in determining whether the regulations for protecting human subjects apply to proposed work.

### **1. NIST Project Lead (the Investigator accountable for the project)**

Name	Mei Ngan
Title	Computer Scientist
Building/Office	225/A210
Division/Group	ITL/IAD/774.03

### **2. Type of Work (check one or both and indicate location, if applicable)**

<input checked="" type="checkbox"/>	NIST work
<input type="checkbox"/>	Contract/Grant to non-NIST party Location where work will be performed:

**3. Title of Proposed Work:** Face and Tattoo Recognition Research and Evaluations with Michigan State Police collected data

### **4. Description of Proposed Work:**

- Goals/Objectives of the work: To conduct biometric algorithm research, evaluation, and technology standardization using coded face and tattoo images.

Importance of the problem that the proposed work addresses: NIST has been conducting research in biometric algorithms and technology standardization for many years as part of its measurement science and standards mission and meeting mandates from the USA PATRIOT Act and Enhanced Border Security and VISA Entry Reform Act. Coded biometric samples (in this case, face and tattoo images) are essential for conducting research in algorithmic matching capabilities.

- Data, specimens or information from humans needed for this project: Coded face and tattoo images and corresponding data including date of birth (year only), gender, race.

Source for the data, specimens or information: The Michigan State Police is providing a set of face and tattoo images extracted from their Statewide Network of Agencies Photos (SNAP) Database.

- Identifiability of the data, specimens or information: The MSP has coded the dataset and retains the key that links the de-identified data to the individual's personally identifiable information (PII). No personally identifiable information about the individuals is required to develop the algorithms (e.g. no PII is in the algorithms or collected by the algorithms). The face and tattoo image data is coded for each subject and the code key is never provided to NIST.

See the NIST Face and Tattoo Recognition Technology Research schematic – Attachment 1.

- A. Agreements or permission to use the data, specimens or information: The Michigan State Police is providing a set of face and tattoo images to NIST following the terms and conditions stated in Attachment (2), a Data Transfer Agreement, as allowed by and Attachment (3) from the MSP.
- Storage plan for data, specimens or information that will ensure privacy and confidentiality: The coded face and tattoo data supplied to NIST will be stored in the NIST Biometrics Research Lab (NIST BRL); will never leave the NIST BRL; and will be accessed only by NIST researchers, which is consistent with the requirements under the Material Transfer Agreement (See Attachment (2)).

The BRL has specific policies and procedures in place to lock down the data (both image samples and annotations), restrict access and use of the data, and prevent readily ascertaining the identity of individuals' information (Attachments (4) – (7))

The specific annotations that will be used in this research are noted in Attachment (4).

- Dissemination plan for sharing results: The coded face and tattoo data supplied to NIST will never leave the NIST BRL and will never be disseminated. NIST may publish the results of the research.

## **5. Collaborations with Others:**

List other institutions or agencies involved in this work. Describe how each collaborator will be involved with data, specimens or information from humans as well as any other specific contributions.

Not applicable

## 6. CONFLICT OF INTEREST

The PI certifies on behalf of self, spouse, registered domestic partner, and dependent children, as well as on behalf of all investigators and their spouses, registered domestic partners, and dependent children. "Investigator" means anyone with responsibility for the design, conduct, or reporting of the research.

### PRINCIPAL INVESTIGATOR

Do you, your spouse, dependent children or household members have any direct, indirect, or related financial interest(s) related to the work to be conducted as part of this proposed project? Interests are related to the research if those interests:

could be affected by the results or outcome of the research,  
are in the sponsor of the research (even if unrelated to the research being proposed), or  
are in another entity conducting research or business that could be affected by the research.

☒ No

☐ Yes -- Please identify investigator and describe conflict on separate page.

### INVESTIGATORS (others who have responsibility for design, conduct, or reporting of the research)

Do any other Investigators, their spouses, dependent children or household members have any direct, indirect, or related financial interest(s) related to the work to be conducted as part of this proposed project? Interests are related to the research if those interests:

could be affected by the results or outcome of the research,  
are in the sponsor of the research (even if unrelated to the research being proposed), or  
are in another entity conducting research or business that could be affected by the research.


☒ No

☐ Yes - Please identify investigator and describe conflict on separate page.

## 7. Certification and Signatures

I hereby certify that the information furnished concerning the procedures to be taken for the protection of the human subjects is correct. As required under NIST policies for research involving human subjects, I will seek and obtain prior HSPO approval, including any required Institutional Review Board (IRB) approval(s), for any substantive modification of this protocol, including source(s) of funding, and will promptly report any unexpected or otherwise significant adverse effects encountered in the course of this study.

PRINCIPAL INVESTIGATOR

Mei Ngan 

Date:

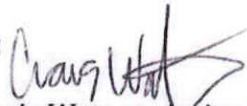
10/13/2015

NIST/ITL Information Access Division

I hereby certify that this research activity has been assessed for scientific merit, anticipated contribution to the field, and feasibility. This assessment evaluated the qualifications of the research team, the scientific question, and appropriateness of the methods planned to answer the scientific question and to justify the inclusion of human subjects in research.

Group Leader Review:

Initial:



Date:

10/14/15

Type Name: Craig Watson, Acting Group Leader, Image Group

Division Chief Review:

Initial:



Date:

10/13/15

Typed Name: Shahram Orandi, Chief, Information Access Division

OU Laboratory Official Review:

Initial:



Date:

16 Oct 2015

Typed Name: Charles Romine, Director, ITL

Attachments:

- (1) Schematic Face and Tattoo Data Usage, September 3, 2015
- (2) Data Transfer Agreement between NIST, MSP, and DataWorks (draft)
- (3) Steven G. Beatty (MSP) email October 7, 2015
- (4) BRL Biometric Repository Annotations - July 8, 2011 with ITL-0012 Notations, September 3, 2015
- (5) BRL Prevents Readily Ascertained Identity - March 5, 2015
- (6) BRL SSP Review Affirmation - November 12, 2014
- (7) BRL User Agreement (2) - June 15, 2015



NIST uses (A) and (B) to research biometric algorithms and develop standards that are supported by the data characteristics – in this case face and tattoo images.

### MSP Face and Tattoo Data Usage at NIST

NIST publishes research & best practices, and contributes actionable comments to standards bodies. Reports may go on the NIST web site and may be published in conference papers and journals. Face and tattoo data from this dataset will never be published in these reports and will not be redistributed by NIST in compliance with terms in a Material Transfer Agreement.

### NIST Face and Tattoo Recognition Technology Research

Report research results to the public

(A) Face and Tattoo data and (B) reference annotations

## NIST

- NIST funded research tasks

- MSP collected face and tattoo images as a part of their Statewide Network of Agencies Photos (SNAP) Database. Such data enables research by USG agencies on new techniques and algorithms for automatic recognition of face and tattoos.
- MSP face and tattoo data is distributed to NIST under Material Transfer Agreement
- NIST conducts biometric algorithm research and technology standardization using Biometric Initiative STRS under the mandate of the USA PATRIOT Act.
- The MSP data provided to NIST:
  - Will be securely stored in the NIST Biometrics Research Lab (BRL);
  - Will never leave the BRL;
  - Will be accessed only by NIST researchers
  - Is coded to ensure that the identities of the contributing subjects cannot be readily ascertained.

### Face and Tattoo Data From MSP

The (B) reference annotations include anonymously coded subject IDs. NIST will never receive subject identities. NIST uses (B) as algorithm inputs and answers.

NIST research activities are on image and algorithm technology and automated algorithm development. No human data are in the algorithms nor collected by the algorithms.

## ATTACHMENT 1

BRL Biometric Repository Annotations

07/08/2011

(Noted 9/3/2015)

A. Encounter Descriptors

- Supplier Name
- Supplier Transaction Type
- **Supplier-Coded Encounter ID\* (ITL-0012)**
- Collection Site
- **Collection Date (ITL-0012)**
- Collection Device ID
- Collection Device Type
- Data Quality Source (s)

B. Subject Descriptors

- Supplier-Coded Subject ID\*
- **Date of Birth (ITL-0012, year only)**
- Country of Birth
- Country of Citizenship
- **Gender (ITL-0012)**
- **Race (ITL-0012)**
- Hair Color
- Eye Color
- Height
- Weight
- Occupation

C. Image Descriptors

- Wearing Glasses?
- Wearing Contacts?
- Facial Expression

\* Supplier encodes the data creating unique IDs; supplier maintains the code book; and the supplier never shares the key to the code book with NIST.

**ITL-0012 – contained in dataset for ITL-0012, Face and Tattoo Recognition Research and Evaluations with Michigan State Police collected data**



## ATTACHMENT 5

### Controls Applied to the NIST Biometrics Research Laboratory Prevent Readily Ascertained Identity

The Biometrics Research Laboratory (BRL) supports NIST biometrics research in standards development and technology evaluation. Essential to this research is a large and growing repository of biometric image samples including fingerprints, facial photos, and irises. These samples have associated characteristics useful for measurement science. (The list of annotation types in the repository is documented in [BRL-Anno].) A large portion of this data has been collected by other U.S. Government agencies as part of their normal operations; and therefore, the data was not originally collected for research purposes. In each case the organization (referred to hereon as the *supplier*) has determined the legal authority by which it is permitted to share its operational data with NIST. This data is treated as Controlled Unclassified Information (CUI), which is alternatively labeled by some suppliers as Sensitive But Unclassified (SBU). Therefore, protective controls have been implemented to lock down this data (both image samples and annotations) in the BRL, restricting access and use of the data, and preventing readily ascertained identity. The categories of controls applied are privately coded samples, restricted access, and training as described below.

The biometric samples are provided by the supplier to NIST as privately coded data using a generic unique identifier that does not convey the identity of the subject. These codes are created and assigned by the supplier. The supplier maintains the code book, and the code book is never shared with NIST.

The biometric data warehoused in the BRL is protected through logical access control (i.e., restricting access via electronic means such as over the network) and through physical access controls (i.e., restricting access via doors and locks). These controls are documented in the [BRL-SSP] System Security Plan (SSP) required by the NIST OCIO. (Note that the SSP references the "Verification Test Bed (VTB) Sub-System", which is more generally referred to here as the BRL.) In addition, the BRL goes through a continuous monitoring review yearly. The BRL passed its most recent (Assessment and Authorization) A&A on November 12, 2014.

Controls have been put in place to create a computer research laboratory (the BRL) on a certified and accredited private network. As stated in [SSP 1.4 a] routers running firewalls separate the BRL from the NIST domain and restrict access from the NIST Network. Controls for logical access are documented in detail in [SSP 2.1] and summarized as follows. The BRL firewall restricts access to the BRL via packet filtering and machine lists with explicit access. All unnecessary ports have been closed and unnecessary services have been disabled. No CUI data is permitted outside of the BRL. General users of the BRL are issued individual accounts that do not have system administrator privileges; users must authenticate when logging into the BRL [SSP 2.7], and BRL accounts are logged for audit and accountability purposes [SSP 2.3]. These controls restrict login access to the BRL; they restrict users from exporting CUI data out of the BRL; and they restrict internet access and database search once logged into the BRL.

The BRL is also physically locked down as documented in [SSP 2.11]. Doors to the BRL are kept locked and remain closed. BRL doors are fitted with locks activated by a registered PIV card and pin number. A limited list of BRL users (authorized to have physical access into the BRL) is managed and maintained by the NIST Office of Security. Each attempt to physically access the BRL is logged for audit and accountability purposes. In case of emergency, the BRL doors are also secured with a conventional keyed lock. The locks are all keyed alike and can be opened only with a specific BRL key. A very restricted list of NIST staff designated as BRL emergency personnel possess this key, one key is on file

with NIST Police, and another key is on file with NIST Fire & Life Safety. NIST janitorial services do not possess a key and are restricted from BRL access. The BRL doors are wired such that if the BRL is accessed by any means other than by PIV card and pin number (e.g., accessed via BRL key), then NIST Police will receive an automated alarm and will dispatch an officer to the BRL.

Orientation and training is given to each BRL user. (The objectives of the training are covered in the BRL User Agreement [BRL-Users].) The user is informed of the CUI nature of the warehoused data; the requirement that no CUI data is permitted outside of the BRL and that no attempt should be made to ascertain the identity of any subject in the CUI biometric data repository; and the risk of harm if the confidentiality, integrity, or availability of the CUI data were to be compromised [SSP 1.7]. In the rare and unlikely event that a BRL user does recognize the identity of a subject in the biometric data repository (for example, a subject is recognized from their facial photo on file), the BRL user is instructed to maintain confidentiality and not disclose to anyone the knowledge that the specific individual is included in the repository. Upon training, the BRL user must read and sign the User Agreement; they receive a copy of the agreement for their own reference; and a copy is kept on file.

The BRL user agreement specifies rules for using and maintaining BRL assets. The BRL includes all systems on the private network contained in 225/B45, 225/B63, 222/B251 and 222/B247. The BRL does not include other Image Group systems for example the 129.6.61.??? subnet.

The BRL (Biometric Research Lab, previously referred to as VTB – Verification Test Bed) supports NIST biometrics research in standards development and technology evaluation. Essential to this research is a large and growing repository of biometric image samples including fingerprints, facial photos, and irises. The BRL uses CUI (Controlled Unclassified Information, previously referred to as SBU - Sensitive But Unclassified) data for biometrics research and technical evaluations. It is important to remind all Image Group staff about the importance of protecting this biometric data as well as the Software Development Kits (SDKs) submitted to each biometric evaluation performed in the BRL. While this data is not classified, there is a significant risk of harm if the confidentiality, integrity, or availability of the CUI data or SDKs were to be compromised. CUI data or SDK compromise could result in a serious adverse effect on BRL operations, for example loss of NIST reputation or customer trust, loss of confidence in data, or loss of external funding.

While all Image Group computer users are bound by the NIST computer user policies and directives <http://inet.nist.gov/oism/directives> and specifically, [https://inet.nist.gov/oism/directives/iss\\_aup](https://inet.nist.gov/oism/directives/iss_aup), there are additional requirements for those with BRL access both physical and computer account. Physical access is by NIST PIV card and pin. Video cameras are used to record activity inside the BRL. Computer access to the BRL is made through "gateway" systems ("vtba" and "vtbb"). Please take a few moments to review each of these items. Item five is a requirement mainly related to the use of facial images but applies to all biometric data.

- 1) The SSP (System Security Plan) states that "No CUI data is permitted outside of the BRL."
- 2) No SDKs should be unencrypted outside the BRL. Evaluation procedures must require that SDKs be encrypted by the participant before sending to NIST and any unencrypted SDK should be rejected for participation and immediately deleted.
- 3) Only NIST employees will have access to participant's SDK software.
- 4) BRL systems are for biometrics research and technical evaluations work only. Firewalls are configured to only allow incoming ssh connections. No email or internet access is allowed from inside the BRL.
- 5) BRL users should make no attempt to ascertain the identity of any subject in the CUI biometric data repository. In the rare and unlikely event that a BRL user does recognize the identity of subject in the CUI biometric data repository (for example, a subject is recognized from their facial photo on file), the BRL user is instructed to maintain confidentiality and not disclose to anyone the knowledge that the specific individual is included in the repository. They should let their supervisor know that the incident occurred without disclosing the identity of the individual.

Thanks for everyone's continued cooperation in protecting the CUI biometric data repository and SDKs contained in the BRL. By signing this form you agree to comply with the requirements for BRL physical and computer access. Any exceptions must be approved in writing. Any violations should be reported immediately to your supervisor.

BRL User: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Annual Refresh: Initials: \_\_\_\_\_ Date: \_\_\_\_\_

Annual Refresh: Initials: \_\_\_\_\_ Date: \_\_\_\_\_

Annual Refresh: Initials: \_\_\_\_\_ Date: \_\_\_\_\_