NTIA MULTISTAKEHOLDER PROCESS ON FACIAL RECOGNITION TECHNOLOGY

Proposed Stakeholder-Drafted Text
July 22, 2014

Definitions

Algorithm

A limited sequence of instructions or steps that directs a computer system how to solve a particular problem or perform a function.[1]

Custodian

The entity or individual that holds Facial Recognition Data

Database

The facial recognition system's database or set of known subjects. May include Facial Templates.

Delete

To make unreadable Facial Recognition Data so that after deletion it cannot be used by reasonable means.[2]
OR
To remove (something, such as words, pictures, or computer files) from a document, recording, computer, etc.[3]

Encryption

The protection of data using reasonable means that have been generally accepted by experts in the field of information security, which renders such data unintelligible or unreadable.

Enroll

The process of storing and maintaining Facial Recognition Data.

---

[1] National Science & Technology Council's Subcommittee on Biometrics - *Biometrics Glossary* definition of "Algorithm": "A limited sequence of instructions or steps that tells a computer system how to solve a particular problem. A biometric system will have multiple algorithms, for example: image processing, template generation, comparisons, etc."

[2] Based on National Science & Technology Council's Subcommittee on Biometrics - *Biometrics Glossary* definition of "Identification:" "A task where the biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity. A biometric is collected and compared to all the references in a database. Identification is "closed-set" if the person is known to exist in the database. In "open-set" identification, sometimes referred to as a "watchlist," the person is not guaranteed to exist in the database. The system must determine whether the person is in the database, then return the identity."

[3] Merrian Webster definition of "delete": "to remove (something, such as words, pictures, or computer files) from a document, recording, computer, etc."

Entity using Facial Recognition

An entity that uses Facial Recognition Systems to Collect and/or Use Facial Recognition Data about Subjects.

Existing Privacy Laws and Regulations

Any state or federal law or regulation that governs the collection or use of personal data from a Subject, where Facial Recognition Data could be considered one type of such data. These laws and regulations may include, but are not limited to, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, the Children's Online Privacy Protection, the California Online Privacy Protection Act, the Electronic Communications Privacy Act, Section 5 of the Federal Trade Commission Act, and state UDAP ("Unfair or Deceptive Acts or Practices") laws.

Facial Authentication

A task where the Facial Recognition System attempts to confirm an individual's claimed identity by comparing the template generated from a submitted face image with a specific known template generated from a previously enrolled face image. This process is also called one-to-one verification.[4]

Facial Detection

A task where the Facial Recognition System distinguishes the presence of a human face and/or facial characteristics without necessarily creating or deriving a Facial Template.[5]

Facial Detection Software

Software used to detect the presence of a human face.[6]

Facial Identification

Searching a database for a reference matching a submitted Facial Template and returning a corresponding identity.[7]

Facial Recognition Data:

Data derived from the application of Facial Recognition Software, including Facial Template and associated metadata.

---

[4] Definition based on comments from Walter Hamilton and John Dowden.
[5] Change based on definition of Facial Profiling created and submitted by Ariel Johnson and the FTC's report refers in the Case Study section to "the detection or recognition of demographic characteristics" (p. 13)
[6] Definition based on comments from stakeholders during May 20, 2014 meeting.
[7] Based on National Science & Technology Council's Subcommittee on Biometrics - *Biometrics Glossary* definition of "Identification" and "Detection Rate": "The rate at which individuals, who are in a database, are properly identified in an open-set identification (watchlist) application. *See also open-set identification, watchlist.*"

Facial Recognition Software

Software used to compare the visible physical structure of an individual's face with a stored Facial Template.[8]

Facial Recognition System

A system that uses Facial Recognition Software.

Facial Template

A digital representation of distinct characteristics of a Subject's face, representing information extracted from a photograph using a facial recognition algorithm.[9]

Facial Image

A photograph or video frame or other image that shows the visible physical structure of an individual's face

Operation of Facial Detection Software

Facial Detection Software is considered "in operation" when the process of Facial Detection is occurring.

Secure Storage of Information

Using commercially reasonable measures to secure information.[10]

Share Information

The disclosure of information to an entity other than the Entity using Facial Recognition or Subject.

Subject

The individual represented in a Facial Recognition System and/or a facial recognition database.[11]

---

[9] Based on National Science & Technology Council's Subcommittee on Biometrics - *Biometrics Glossary* definition of "Template": "a digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison. *See also extraction, feature, model."*

[9] Based on National Science & Technology Council's Subcommittee on Biometrics - *Biometrics Glossary* definition of "Template": "a digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison. *See also extraction, feature, model."*

[10] Based, in part, Article 4A-202 of the Uniform Commercial Code (the "UCC") requirements for bank transfers: "If a bank and its customer have agreed that the authenticity of payment orders . . . will be verified pursuant to a security procedure, a payment order . . . is effective as the order of the customer . . .if: (a) The *security procedure is a commercially reasonable method* of providing security against unauthorized payment orders;"

[11] Based on the National Science & Technology Council's Subcommittee on Biometrics - *Biometrics Glossary* definition of "User": "A person, such as an administrator, who interacts with or controls end users' interactions with a biometric system. *See also cooperative user, end user, indifferent user, non-cooperative user, uncooperative user"* However, separated out to clarify the subject and the user are different.

Threshold

A user setting for Facial Recognition Systems for authentication, verification or identification. The acceptance or rejection of a Facial Template match is dependent on the match score falling above or below the threshold. The threshold is adjustable within the Facial Recognition System.[12]

[12] Based on National Science & Technology Council's Subcommittee on Biometrics - *Biometrics Glossary* definition of "Threshold": "A user setting for biometric systems operating in the verification or open-set identification (watchlist) tasks. The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application. *See also comparison, match, matching."*

Stakeholder Issue No. 2. What obligations should the code impose when Facial Detection[13] *occurs but no Facial Template is created and no individual is enrolled?*

a. In Facial Detection, where a face is detected ("this is a human face") but no Facial Template is created, is transparency and consent possible?

b. If so, what transparency would be required and how would it be implemented?

c. Is it appropriate to require consent? How could this be implemented?

Stakeholder-Drafted Text.

I. A general notice is recommended when biometric technology is deployed but will not be used for individual identification. An example is using facial recognition technology to just detect and count people or to estimate the gender and age of a person observing a store display (for marketing research purposes).[14]

II. An entity may not use a face recognition system to determine an individual's race, color, religion, sex, national origin, disability or age.[15]

III. Prior to the creation of any faceprint, a commercial entity must provide in (accessible) writing, and with online examples, how the process has been designed and operates. […] Companies must also identify for approval whether any racial/ethnic data will be generated and how it will be used.[16]

IV. Companies using facial recognition technologies that operate anywhere along the spectrum should implement privacy protections for the context of their relationship with consumers.[17]

[13] Stakeholder Definition: "A task where the Facial Recognition System distinguishes the presence of a human face and/or facial characteristics without necessarily creating or deriving a Facial Template."
[14] (submitted by International Biometrics & Identification Association)
[15] (submitted by ACLU)
[16] (submitted by Center for Digital Democracy)
[17] (submitted by Internet Association)

Stakeholder Issue No. 11. How should the code address storage of Facial Recognition Data?

a. Should the code address retention periods? Should retention periods depend on the Subject's reasonable expectations regarding use and retention of the template?

b. Should the code define Secure Storage of Information? Should context matter and, if so, how?

Stakeholder-Drafted Text:

I. An entity must [should] describe its policies for compliance with these principles including the duration it retains data, [(preferably a defined length) or the policy that determines the period of retention.][18]

II. Companies should maintain reasonable retention and disposal practices.[19]

III. An entity must keep securely [use reasonable security protections] [use reasonable security measures] [use commercially reasonable measures] information contained in a face recognition system [to protect facial recognition templates] [to protect the images and data they store].[20]

IV. We recommend that implementers and operators of commercial biometric technology publish their privacy policies and that the principles listed be included: […]

a. **Security Safeguard Principle –** Protection of any information collected or retained (whether biometric or otherwise) with good cyber-security practices; disassociating the data to the extent allowed by the applications to limit exposures if a cyber or other privacy breach does occur; encryption of data at rest and data-in-motion to limit exposures in the event of a breach.[21]

V. Storing facial recognition images as proprietary vectors is a form of encryption.[22]

[18] (submitted by ACLU, bracketed language from International Biometrics & Identification Association)
[19] (submitted by Internet Association)
[20] (submitted by ACLU), bracketed language from Marketing Research Association, Interactive Advertising Bureau, and Internet Association)
[21] (submitted by International Biometrics & Identification Association)
[22] (submitted by Marketing Research Association)

Stakeholder Issue No. 11A. How should the code address transmission of Facial Recognition Data?

a. Should the code address security of Facial Recognition Data in transmission and, if so, how?

b. Do recognized technical standards exist that pertain to transmission?

Stakeholder-Drafted Text:

I. We recommend that implementers and operators of commercial biometric technology publish their privacy policies and that the principles listed be included: […]

a. **Security Safeguard Principle –** Protection of any information collected or retained (whether biometric or otherwise) with good cyber-security practices; disassociating the data to the extent allowed by the applications to limit exposures if a cyber or other privacy breach does occur; encryption of data at rest and data-in-motion to limit exposures in the event of a breach.[23]

[23] (submitted by International Biometrics & Identification Association)

Stakeholder Issue No. 12. *Risk: Security: commercial facial recognition data could be subject to data breaches that result in sensitive biometrics being revealed to unauthorized entities; insufficient security procedures could result in biometric identity theft.*

a. Which entities would be best situated to provide for security?

b. What data should be subject to security obligations in the code?

c. Most states currently have breach notification laws. Should the code impose additional data breach notification obligations (not otherwise subject to state law)?

d. Are there contexts in which the code should require encryption of Facial Recognition Data?

e. Should the code distinguish between unencrypted data and those that are Encrypted? Could the code do so by establishing a "material risk of harm" threshold for notice, where a "material risk of harm" would arise when unencrypted templates are revealed to unauthorized entities? Would treating Encrypted data as not triggering a material risk of harm provide companies with appropriate incentives to design and implement robust security protections?

Stakeholder-Drafted Text:

I. An entity must keep securely [use reasonable security protections] [use reasonable security measures] [use commercially reasonable measures] information contained in a face recognition system [to protect facial recognition templates] [to protect the images and data they store].[24]

II. We recommend that implementers and operators of commercial biometric technology publish their privacy policies and that the principles listed be included: […]

a. **Security Safeguard Principle –** Protection of any information collected or retained (whether biometric or otherwise) with good cyber-security practices; disassociating the data to the extent allowed by the applications to limit exposures if a cyber or other privacy breach does occur; encryption of data at rest and data-in-motion to limit exposures in the event of a breach.[25]

III. Storing facial recognition images as proprietary vectors is a form of encryption.[26]

[24] (submitted by ACLU, bracketed language from Marketing Research Association, Interactive Advertising Bureau, and Internet Association)
[25] (submitted by International Biometrics & Identification Association)
[26] (submitted by Marketing Research Association)

Stakeholder Issue No. 16. Risk/Issue: Withdrawal of Facial Template from a database?

a. Is there a difference between withdrawal from a database and deletion from a database?

b. Should the code address withdrawal/deletion from the database? If so, how can organizations best provide individuals with the ability to withdraw or request deletion from enrollment in facial recognition databases? Is there anything to be withdrawn other than a Facial Template?

c. Should the code address withdrawal/deletion in situations where the individual maintains an ongoing commercial relationship with the User?

d. Are there contexts in which the User need not allow a Subject to withdraw or request deletion?

e. How would withdrawal/deletion of a Facial Template from a database compare with withdrawal/deletion of other personal data?

Stakeholder-Drafted Text:

I. We recommend that implementers and operators of commercial biometric technology publish their privacy policies and that the principles listed be included: […]

   a. **Problem Resolution and Redress –** Description of the process consumers can follow if they believe that the privacy of their personal information has been compromised; publication of the contact information for the person or organization to which such concerns should be escalated, along with possible redress options, including revocation, deletion, or change of biometrics used for identification purposes.[27]

II. An individual must have the right to access, correct, and delete his or her faceprint information. […] [Consent may be withdrawn by the individual at any time … A company must make it convenient and accessible for an individual to withdraw use of their FR data, such as through a prominent link that removes consent.].[28]

III. Public Information Exception: Organizations should be able to process and communicate information where the images are related to matters of public interest, such as news, public affairs, politics, sports, and public figures.[29]

[27] (submitted by International Biometrics & Identification Association)
[28] (submitted by ACLU)
[29] (submitted by Interactive Advertising Bureau)

Stakeholder Issue No. 18. Access by Law Enforcement

What should the code say about government (*e.g.*, law enforcement) access to Facial Recognition Data obtained by the commercial sector? What standards do holders of Facial Recognition Data believe should apply to requests by governments to gain access to this information, what concrete risks would occur if this standard is set too low or too high, and what, if any, obligation should exist to notify the Subject where allowed by law?

Stakeholder-Drafted Text:

I. We recommend that implementers and operators of commercial biometric technology publish their privacy policies and that the principles listed be included: […]

   a. **User Limitation Principle –** Limitation of access to the data to certain specified individuals or applications and restricting third party access unless disclosed and necessary to the original purpose or application as stated in the Purpose Specification or in response to a legal order.[30]

II. An entity must treat a faceprint and other information associated with its collection, use, and sharing as the content of communications. Government access to information from a face recognition system that is not covered by the Privacy Act of 1974 should only be authorized pursuant to a warrant issued with probable cause.[31]

[30] (submitted by International Biometrics & Identification Association)
[31] (submitted by ACLU)

Stakeholder Issue No. 19. Audit Trails and Access

a. Should the code address whether and, if so, how a Subject may have a right to audit how an Entity using Facial Recognition uses Facial Recognition Data pertaining to that Subject, and including accessing the type and accuracy of Face Recognition Data?

b. Should the code address whether and, if so, how an Entity using Facial Recognition Data pertaining to a Subject should track how it uses that Data?

Stakeholder-Drafted Text:

I. An individual must have the right to access, correct, and delete his or her faceprint information. An individual may also access and request correction of information about him or her derived from operation of a face recognition system including information maintained in the audit trail.[32]

II. We recommend that implementers and operators of commercial biometric technology publish their privacy policies and that the principles listed be included: […]

a. **Accountability Principle –** Adhering to these best practices recommendations by maintaining audit logs sufficient to the published purposes and conducting periodic audit reviews by an independent audit.[33]

[32] (submitted by ACLU)
[33] (submitted by International Biometrics & Identification Association)