Title – Guidelines for the Collection and Use of Facial Recognition

Section 1 – 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]

Collection of facial recognition data - When enrollment occurs.

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

Encryption - To transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable, using generally accepted practices[2].

Enroll - The process of storing and maintaining Facial Recognition Data.

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

Existing Laws and Regulations - Any state or federal law or regulation including those 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.[3]

Facial Detection - A task where the Facial Detection System distinguishes the presence of a human face and/or facial characteristics without creating or deriving a Facial Template.[4]

Facial Detection Technology - Technology used to detect the presence of a human face using Facial Detection.[5]

Facial Detection System – A system that uses Facial Detection Technology.

---

[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] Maine Revised Statutes, Title 10: Commerce And Trade, Chapter 210-B

[3] Definition based on comments from Walter Hamilton and John Dowden.

[4] 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)

[5] Definition based on comments from stakeholders during May 20, 2014 meeting.

Facial Identification - Searching a Facial Recognition Database for a reference matching a submitted Facial Template and returning a corresponding identity.[6]

Facial Recognition Data - Data derived from the application of Facial Recognition Technology, including Facial Template.

Facial Recognition Technology - Technology used to compare the visible physical structure of an individual's face with a stored Facial Template.[7]

Facial Recognition System - A system that uses Facial Recognition Technology.

Facial Template - A digital representation of distinct characteristics of a Subject's face, representing information extracted from a photograph using a facial recognition algorithm.[8]

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

Secure Storage of Information - Using commercially reasonable measures to secure information.[9]

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

Subject - The individual represented in a Facial Recognition System and/or a Facial Recognition Database.[10]

Section 2 – General Requirements

An entity using facial recognition technology is in compliance with these guidelines if the entity fulfills the requirements set forth in Sections 3-10.

Section 3 – Transparency

Entities that use facial recognition technology should make available to subjects the entity's policies regarding its collection and use of facial recognition data.

Notice regarding the use of facial recognition technology should be given before or at the time the facial recognition technology is employed. Alternatively, notice may be given when reasonably possible after

---

[6] 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."*

[8] 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, 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;"

[10] 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.

facial recognition technology is employed if the entity provides appropriate choices to control the use of the subject's facial recognition data.

Section 4 - Control

An entity using facial recognition technology should provide a subject with meaningful control over when their facial recognition data is shared with others who would not otherwise have access to, or are not authorized to have access to, that information.

An entity using facial recognition technology should provide a subject with an opportunity to challenge a determination when their facial recognition data is used as a barrier to access.

Section 5 - Compliance with Existing Law

Nothing in these guidelines should limit an entity using facial recognition or facial detection from complying with existing laws and regulation.

Section 6 – Disclosure of facial recognition data

The limitations of these guidelines do not apply to an entity disclosing facial recognition data with the consent of the person to whom the facial recognition data pertains, or when based on a good faith belief that such disclosure is necessary:

- To prevent death or bodily harm;
- To comply with a legal request, such as a valid warrant or subpoena issued pursuant to proper legal process;
- When used exclusively for the purposes of securing a physical location.

Section 7 - Limitations on Use

No entity using facial recognition may use facial detection or recognition technology, or facial recognition data, to engage in unlawful or illegal practices.

Section 8 - Protecting information

[NEED TO ADD LANGUAGE]

Section 9 – Technology Neutrality

These guidelines apply to all uses of facial recognition technologies, regardless of medium. These guidelines do not apply to uses of facial detection technologies, except for the prohibitions in Section 7 – Limitations on Use.

[FREE SPEECH LANGUAGE TO ADD]

Section 10— Public Information Exception

Nothing in these guidelines should be construed to preclude entities' rights to process and communicate information where images are related to matters of public interest, such as news, public affairs, politics, sports, and public figures.[11]

[11] Based on first amendment and journalistic concerns raised by the ACLU and Alvaro Bedoya.