Privacy Principles for Facial Recognition Techology in Commercial Applications

FUTURE OF PRIVACY FORUM

September 2018

Summary of Privacy Principles

FUTURE OF PRIVACY FORUM

1.) CONSENT

Obtain express, affirmative consent when: 1) enrolling an individual in a program that uses facial recognition technology for verification or identification purposes; and/or 2) identifying an individual to third parties who would not otherwise have known that individual's identity.

2.) USE - RESPECT FOR CONTEXT

Commit to collecting, using, and sharing facial recognition data in ways that are compatible with reasonable consumer expectations for the context in which the data was collected.

3.) TRANSPARENCY

Provide consumers with meaningful notice about how the facial recognition software templates are created and how such data will be used, stored, shared, and maintained.

4.) DATA SECURITY

Companies will maintain a comprehensive data security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of personal information against risks - such as unauthorized access or use, or unintended or inappropriate disclosure - through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information.

5.) PRIVACY BY DESIGN

Companies should seek to implement technological controls that support or enforce compliance with these principles in addition to policy, legal, and administrative measures.

6.) INTEGRITY & ACCESS

Implement reasonable measures to maintain the accuracy of facial recognition data. Offer individuals reasonable access to review or request correction of inaccurate identity labeling, and the ability to request deletion of facial recognition data.

7.) ACCOUNTABILITY

Take reasonable steps to ensure that use of facial recognition technology and data by the organization, and in partnership with all third party service providers or business partners, adheres to these Principles.

PRIVACY PRINCIPLES FOR FACIAL RECOGNITION TECHNOLOGY IN COMMERCIAL APPLICATIONS

INTRODUCTION

The consumer-facing applications of facial recognition technology continue to evolve and appear in new contexts. There are several key functions that benefit from facial recognition technology, including: (1) safety and security; (2) access and authentication; (3) photograph and video storage identification and organization; (4) accessibility to platforms, accounts, or services, and (5) marketing and customer service. There are also, however, specific concerns about the privacy protections needed for the responsible use of this expanding technology. These Principles are meant to apply to personally identifiable information (PII) based on the development and use of facial recognition technology as defined and described here.[1]

The Principles have been designed to drive responsible data use by those businesses and on-line platforms developing and using facial recognition technology in commercial settings; to establish a foundation of protections for personal data that is deserving of user trust; and to inform the conversation behind various legislative initiatives on the specifics of the technology, and the technical and policy protections available. These Principles are intended to set industry best practices, inform consumer expectations, and educate policymakers regarding the various technologies discussed. They are not intended to be used directly as a model bill or legislative language since, as with any technology, new business practices and consumer needs may evolve and warrant ongoing evaluation.

It is important to first clarify the distinctions between various types of facial scanning systems, generally understood to encompass a spectrum from facial detection (no PII collected), through facial characterization (no personal templates or enrollment), and ultimately including facial verification and identification purposes (personalized templates created and stored).[2] Not all public camera usage, or even all facial scanning, constitutes "facial recognition" or even involves

[1] There are also non-privacy considerations for responsible FR practices. Discriminatory outcomes resulting from insufficiently diverse training sets is one of the non-privacy related harms that can result from improper use of facial characterization or recognition systems. Deliberate care should be taken in designing and training a facial recognition system to ensure that facial recognition algorithms have comparable levels of accuracy across demographic variances such as race, gender, and age. An ability to demonstrate or audit this testing is highly desired. Of course, companies may not use facial recognition technology to enable illegal discrimination based on race, color, sex, national origin, disability, or age.

[2] All terms are defined in Annex A.

the creation of personal data. The creation or storage of a photo or video on its own does not inherently implicate facial recognition privacy concerns, nor do basic facial detection systems that do not create or collect personalized information about an individual consumer's image. Data collected by these detection programs is not a template, is not identifiable, linked, or linkable to individuals, and does not trigger the protections provided by these principles. Likewise, facial characterization programs do not routinely create or retain personably identifiable facial templates. Facial characterization technology is evolving rapidly, however, particularly with some applications employing artificial intelligence and machine learning techniques, and should continually be evaluated when used in new contexts for the potential future need to apply these Principles when PII is implicated.

The following seven principles provide key protections and are each important as part of an overall framework for the collection and use of facial recognition data. In some circumstances, a principle may not be as applicable given particular data use or technological limitations. In such circumstances, the other protections play a commensurately larger role.

Where these Principles are clearly applicable is in the context of facial recognition programs (currently defined to include verification and identification systems) that create, collect, compare and retain facial templates when created and correlated to a particular individual.[3] These Principles define a standard of privacy requirements for those situations where technology collects, creates, and maintains a facial template that be used to identify an individual. Inherently, the companies developing the underlying technologies, enterprise (B2B) activities, and those businesses which employ public-facing facial recognition systems all compete on intrinsic attributes of the technology such as reliability and security, and so should be motivated to make them as accurate as possible.[4] All such companies should therefore support these Principles with the goal that by following these principles to collect, use, and share facial recognition data, they will deserve and retain consumer trust.[5]

---

[3] "Identification" means the facial recognition template is subsequently tied to other PII from alternate sources or databases. See attached chart for detailed breakdown of categories of technology, collection, privacy concerns, and consent.

[4] System development companies are evaluated by NIST to meet acceptable and steadily improving standards of accuracy and reliability in the On-going Vendor Test program at https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing. In addition, market pressures should be leveraged to create a strong incentive for the facial recognition technology industry to prioritize accuracy, privacy, and data security. A competitive industry is the best insurance for consumers the choice not to do business with companies that do not respect these principles.

[5] *See* The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

PRIVACY PRINCIPLES:[6]

1. Consent	***Obtain express, affirmative consent when: 1) enrolling an individual in a program that uses facial recognition technology for verification or identification purposes; and/or 2) identifying an individual to third parties who would not otherwise have known that individual's identity.[1]***

- Obtain express, affirmative consent in line with existing FTC standards, accepted practices, and expectations. No new or different meaning for consent as discussed here is intended.[7] Exceptions to this consent requirement are described below.
- No unique biometric identifier should be created and maintained over time without appropriate consent. [8] As applied to each technology:[9]
  - Characterization – consent is not required when simple characterization (estimating gender, age, or general emotional state) programs are used, and no enrollment takes place.[10]
  - Verification – one-to-one matching requires express, affirmative consent upon enrollment in the database.
  - Identification – one-to-many matching requires express, affirmative consent upon collection, prior to the matching process being initiated.

---

[6] For additional resources see: NTIA Multi-stakeholder Working Group (https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology); IBIA Privacy Best Practice Recommendations for Commercial Biometric Use (https://www.ibia.org/resources/white-papers).

[7] Express affirmative consent may be written or oral. Simple acceptance of a privacy policy or terms of service notice may not constitute consent if facial recognition is not clearly intrinsic in the service provided. Likewise, simply allowing one's photo to be taken, without clear acknowledgement of the notice about the use of FR technology for that photo, is not sufficient.

[8] Once consent is obtained, this consent should include future compatible uses during the period a user continues to maintain an account.

[9] See attached chart for further detail.

[10] While there are no equivalent privacy risks associated with Facial Characterization, the FTC has identified requirements for notice based on Consumer Expectations: https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

Exemptions to the requirement for express, affirmative consent may be in a use case that does not require consent, or in a limited set of circumstances where opt-out consent is sufficient. Exemptions include:

Cases where notice is provided but no consent is required:

- Collections of data (including collection of facial recognition templates from security systems) for physical security, fraud, and asset protection programs do not require express consent. Data collected may be subject to the other privacy principles, and should never be used outside the security program context.
- When sharing the identification of individuals occurs within a vendor management framework, where the third party is a contracted services partner necessary to provide the good or service requested by the individual, and who is bound by the same controls.

Circumstances where notice is provided and opt-out consent is sufficient:

- Limited collection/limited use programs that create or collect facial template data tied to a unique persistent identifier are exempt if the identifier is not linked or linkable to any other personally identifiable information, including purchase or payment data.[11]
- Templates created within photo organizing platforms and tools for internal photo sorting or management, when limited to a single user's account, not linked by the provider to any other identifying information, and not shared, suggested, or linked to other users of that platform or service without express consent.
- Templates created within on-line platforms or services, such as social media, which may identify users to each other when the affected user accounts are already linked through some intentional connection or action by the individual users (such as photo "tagging suggestions" made to a user about other users to whom s/he is already affirmatively connected).

[11] One example of such a limited use program would be tracking in a retail environment to monitor individual behavior during the visit, or between visits over time, without otherwise connecting to any additional information which would identify the particular consumer.

2. Use – Respect for Context	***Commit to collecting, using, and sharing facial recognition data in ways that are compatible with reasonable consumer expectations for the context in which the data was collected.***

- Use facial recognition technology in a way that is fair to consumers, including weighing the privacy risks against clear and articulable benefits to consumers and providing opportunities for consumers to make choices to mitigate or avoid risks.[12]

- Determine whether a prospective use is compatible by considering factors to include the context of collection; a reasonable expectation of how the data will be used; whether facial recognition is merely a feature of a product or service vs. integral to the service itself; and how the collection, use, or sharing of facial recognition data will likely impact consumers.

- Consider how the use of facial recognition technology will impact both consumers who purposefully avail themselves of products or services which incorporate that technology and consumers who incidentally come into contact with facial recognition systems or cannot reasonably avoid a company's use of facial recognition technology.[13]

- Give special consideration to the age, sophistication, or degree of vulnerability of those individuals, such as children, in light of the purposes for which facial recognition technology is used, including whether additional levels of transparency, choice, and data security are required. This includes awareness and compliance with any additional legal requirements that may apply.

- Services offered by a company may evolve over time, and compatible uses can potentially include instances of facial recognition that may not have been detailed at the time of collection but nonetheless are consistent, and non-materially different from those out-lined in the initial description. Such new uses should be evaluated carefully, and any change in scope that would reasonably be considered a "material change" must be implemented only after new notice and consent have been obtained, consistent with established FTC guidance.[14]

---

[12] The FTC Act's guidance as to what constitutes an unfair practice generally is equally useful for companies using facial recognition technology: 15 U.S.C. §45(n) provides that an act or practice is not unfair "unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."

[13] *Accord* Article 29 WP Opinion at 8.

[14] "Mergers and Privacy Promises," FTC blog at https://www.ftc.gov/news-events/blogs/business-blog/2015/03/mergers-privacy-promises, March 25, 2015 (written in context of corporate mergers, but outlining the FTC's prior holdings and expectations regarding practices being consistent over time with the privacy policies in place at the time of data collection).

3. Transparency	*Provide consumers with meaningful notice about how the facial recognition software templates are created and how such data will be used, stored, shared, and maintained.*

- Companies implementing facial recognition systems should develop and publish privacy policies describing their use of facial recognition systems in clear terms and a detailed description of the data collected. Privacy policies, educational help centers, and other materials are ways to ensure consumers and other stakeholders can understand:
  - Purposes for which facial recognition data is collected;
  - Whether facial recognition data may be shared;
  - Retention, deletion, or de-identification policies for facial recognition data;
  - Choices consumers may have regarding their facial recognition data;
  - Where consumers may direct questions about their facial recognition data;
  - What contracted third party partners routinely receive the data as part of supplying the product or service;
  - When collection, use, and sharing practices materially change, companies should update their public privacy policies or publicize those changes as appropriate to the context of the change and its impact on consumers;
  - When unique persistent identifiers are used under the allowed exception to express, affirmative consent, and provide clear opt-out procedures.
  - Notice may differ based on forms of tracking in place: real time v. recorded; hidden v. visible; and duration, etc. Where appropriate, contextual and just-in-time notices should be used.[15]
- Companies which design and develop facial recognition technology hardware and software systems, should seek to take reasonable steps – such as making recommendations and

[15] See e.g. FTC, Facing Facts at 12 ("If the company is storing the [facial recognition] images for a purpose that is not consistent with the context of the transaction taking place, it should provide additional information about why it is storing the images – at a 'just in time' point. For example, if the company stores the images for purposes of sharing them with third parties, it should explicitly provide consumers with a choice about this practice before they upload their image – outside of a privacy policy or similar document."). See also Article 29 WP Opinion at 6-7 ("[I]nformation relating to the facial recognition feature of an online or mobile service should not be hidden but be available in an easily accessible and understandable way … [C]onsent for [collecting facial recognition data] cannot be derived from the general user's acceptance of the overall terms and conditions of the underlying service unless the primary aim of the service is expected to involve facial recognition…. To this end, users should be explicitly provided with the opportunity to provide their consent for this feature either during registration or at a later date, depending on when the feature is introduced.")

providing guidance – to facilitate transparency and privacy compliance by third-parties using that company's facial recognition technology. For example:

- including reasonable limitations on use in contract language,
- providing companies with model language for physical location signage or inclusion in their privacy notices,
- recommending signage if the facial recognition technology will be deployed in public places; and
- recommending other reasonable efforts to promote provision of clear, meaningful notice to consumers.

4. Data Security	*Companies will maintain a comprehensive data security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of personal information against risks – such as unauthorized access or use, or unintended or inappropriate disclosure – through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information.*

- Choose security technologies and procedures that best fit the scale and scope of the facial recognition data collected and maintained, subject to the obligations under applicable data security statutes, regulations, and contractual or other binding commitments to consumers and other stakeholders. Most states have existing breach notification laws, and other state or federal regulations may apply.

- Update and maintain reasonable data security over time to address and anticipate evolving threats and identified vulnerabilities.

- Implement data security practices and procedures commensurate with the sensitivity of the facial recognition data, the context in which facial recognition technology and facial recognition data is employed or used, the likelihood of harm to consumers, and other relevant factors.

- As with all personal data, provide data security appropriate to the sensitivity of facial recognition data when at rest and in transit.[16] Reasonable security should include a default of data encryption, along with a combination of virus protection, access controls, employee training, and other standard security practices.

[16] The Article 29 WP Opinion recommends that, where possible, and especially in the case of authentication or verification activities, local processing of data should be favored. See Article 29 WP Opinion at 8.

- Set reasonable retention and disposal practices for facial recognition data based upon the particular product or service for which it is collected. Facial recognition template data should be retained no longer than necessary for legitimate business purposes, and then deleted or destroyed in a secure manner.

5. Privacy by Design	*Companies should seek to implement technological controls that support or enforce compliance with these principles in addition to policy, legal, and administrative measures.*

- Privacy by design should be incorporated by companies who manufacture, resell, install, or employ consumer-facing facial recognition systems, although the ways in which it is implemented will vary based on role and application of the specific technology or system.
- Implement privacy by design into all organizational practices, including assigning personnel to oversee privacy issues, training employees on privacy, and periodic privacy reviews.
- Promote consumer privacy and data security throughout the organization, and proactively incorporate privacy and security into facial recognition products and services at every stage of product development and deployment. Privacy by design requirements may include:
- Embedding privacy controls into the design and architecture of facial recognition products and services, as well as the company's internal IT systems and business practices, rather than considering consumer privacy implications after the fact.
- Incorporating privacy protections throughout the entire lifecycle of the data involved.
  - Implementing an internal review process designed to identify and mitigate potential privacy risks in products and services that use facial recognition technology before such products and services are deployed or made available to consumers.

6. Integrity & Access	*Implement reasonable measures to maintain the accuracy of facial recognition data. Offer individuals reasonable access to review or request correction of inaccurate identity labeling, and the ability to request deletion of facial recognition data.*

- Take steps to ensure that facial recognition data and its connections to other PII are accurate. Companies should seek to avoid mislabeling by sufficiently testing their systems to identify and eliminate meaningful accuracy disparities, specifically with regard to demographic variances in race, age and gender.

- Establish and publish policies and practices that inform individuals of the means available to review their personal data in a meaningful format, identify potential errors and request correction, and request deletion of their account or any personal data, where applicable. Mechanisms for consumers to report their concerns should be readily identifiable and available.

- Law Enforcement Access: Facial Recognition template data may be disclosed, or commercial databases searched, in response to law enforcement entities with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena, or to comply with other state or local laws for law enforcement actions. Voluntary release may occur in cases of "exigent circumstances" for immediate emergency or public safety, such as Amber alerts or active shooter notices.[17]

- When possible, companies will attempt to notify individuals on the occurrence of personal information releases in response to law enforcement requests.

7. Accountability	*Take reasonable steps to ensure that use of facial recognition technology and data by the organization, and in partnership with all third-party service providers or business partners, adheres to these Principles.*

Implement transparent policies, procedures, and practices to ensure that these Principles underlie the use of facial recognition technologies by the company in all consumer-facing contexts, and to the fullest extent applicable.

- Implement training programs and routine audits for the employees and offices that handle facial recognition data.

- Consider creating internal privacy review boards to evaluate and approve new applications and services involving facial recognition data.

- Take reasonable steps to ensure that third-party service providers, business partners, or companies using their facial recognition technology or facial recognition data adhere to these Principles, and deny access to third parties who fail to comply.[18]

---

[17] Exigent circumstances - "circumstances that would cause a reasonable person to believe that entry (or other relevant prompt action) was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts." See https://www.law.cornell.edu/wex/exigent_circumstances.

[18] FTC Settlement Agreement In the Matter of GMR Transcription Services, Inc., finding that GMR failed to adequately verify a service provider implemented reasonable measures to protect PII. Further discussion at A Primer on FTC Expectations for Your Partner and Vendor Relationships, at https://www.wilmerhale.com/uploadedFiles/Shared_Content/Editorial/Publications/Documents/a-primer-on-ftc-expectations-for-your-partner-and-vendor-relationships.pdf last viewed January 18, 2018.

ANNEX A

Definition Of Terms

Algorithm

A limited sequence of instructions or steps that directs a computer system how to solve a particular problem or perform a function.[19] May include algorithms with "machine learning" applications and outcomes as well.

Custodian

The entity or individual that holds Facial Recognition Data, usually the CIO or CISO in the US; the Controller under the GDPR.

Database

The facial recognition system's database of facial images or set of known subjects. The set against which the collected image is compared. May include Facial Templates.

Delete

To make Facial Recognition Data unreadable so that after deletion it cannot be retrieved or used by reasonable means.[20]

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. The process of changing plaintext into ciphertext for the purpose of security or privacy.

Enroll

The process of storing and maintaining Facial Recognition Data in a way that permits association with a specific human identity at the time of storage.

---

[19] 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."

[20] 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."

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. As of publication, Illinois, Texas, and Washington states all have commercial biometrics laws in place.

Express, Affirmative Consent

Any freely given specific and informed indication of the consumer's wishes by which the individual signifies his agreement to personal data relating to him being collected or processed. Having received clear and meaningful notice, the consumer has taken an additional affirmative step that indicates their agreement to the data collection. Express, affirmative consent may be written or verbal.[21]

Facial Authentication (see Facial Verification)

Facial Characterization

A task where a system uses an automated or semi-automated process to discern a data subject's: 1) general demographic information or 2) emotional state (i.e. a smile), without creating a unique identifier tracked over time. Templates should not be enrolled, maintained, or tracked over time or location.

Facial Detection

A task where the Facial Recognition System distinguishes the presence of a human face and/or facial characteristics without creating or deriving a Facial Template. No PII is created by the use of facial detection software.

Facial Detection Software

Software used to detect the presence of human features in an image. Facial detection software is generally a different technology than the programs that are used for Characterization, Verification, or Identification, all of which – unlike Detection software – create a unique facial template.

Facial Identification

Searching a database for a reference matching a submitted Facial Template and returning a corresponding identity. Also known as "one-to-many" matching.

---

[21] Written consent may include "click through" wizards (consistent with FTC-accepted practices and contexts). Verbal consent may occur in voice-activated or controlled systems, and may be recorded for verification.

Facial Image

A photograph or video frame or other digital image that shows the visible, physical structure of an individual's face. Includes digital photographs or videos that have not been subject to facial recognition software.

Facial Recognition Data

Data derived from the application of Facial Recognition Software, including the Facial Template, the algorithmic string created by the program, the hashed version of the output, and any associated metadata. Data that represents, or is derived from, or is extracted from an image of a data subject's body.

Facial Recognition Software

Software used to compare the physical structure or digital image of an individual's face with a stored Facial Template via creation of the enrolled template and application of the recognition matching process.

Facial Recognition System

A system that uses Facial Recognition Software.

Facial Template

A digital representation of distinct characteristics of an individual's face, representing information extracted from a photograph or a live individual, using a facial recognition algorithm.[22]

Facial Verification

A task where the Facial Recognition System confirms an individual's claimed identity by comparing the template generated from a submitted facial image with a specific known template generated from a previously enrolled facial image. This process is also called one-to-one verification, or authentication.

[22] 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.*"

Security Applications

Loss prevention and other applications intended to detect or prevent shoplifting, fraud, misappropriations or other malicious and criminal activities. Facial recognition processes or the creation of facial templates from surveillance videos may be included in security practices.

Secure Storage of Information

Using commercially reasonable measures to protect digitally stored information.[23]

Share Information

The disclosure of information to an entity other than the entity using the Facial Recognition software, or the Subject. Distinctions apply when authorized sharing is done with contracted third party providers to deliver the product or service, versus independent entities with rights to use the data for their own purposes.

Subject

The individual represented in a Facial Recognition System and/or a facial recognition database.[24]

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.[25]

---

[23] 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;"

[24] 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.

[25] 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."

ANNEX B

Why Facial Recognition Privacy Principles Are Needed

Potential Privacy Challenges Associated With Facial Recognition

As with any new technology, innovative capabilities bring benefits and services, but can present new or expanded privacy risks. Facial recognition data is personal and sensitive, making privacy an important aspect of data management for companies to address.

- Commercial uses abound. For example, facial recognition is bringing a new dimension to video game systems, allowing players to put their faces in the game.[26] Likewise, some software can analyze a face to determine whether that person is feeling joy, sadness, surprise, anger, fear, disgust, contempt, or any combination of these emotions offers countless beneficial applications. One facial recognition software company offers churches the ability to scan congregants' faces to keep track of attendance.[27]

- Consumer Knowledge and Consent. A key consideration with the capture of facial recognition data from potentially large numbers of people is when and how to provide meaningful notice and to obtain their informed consent, especially if those individuals are then identified or profiled against other datasets.[28] [29]

- Data Security. Commercial use of facial recognition technology raises many of the same security concerns applicable to sensitive personal information generally. The consequences of a breach of facial recognition data, however, are potentially more serious, as it is not generally feasible for a person to change or hide their face, as compared to other personal information. Therefore, to the extent that systems are interoperable or subject to spoofing, they represent an increased risk. Likewise, large databases of identified individual images could lead to facial recognition data being used in ways that consumers cannot anticipate or control, and without their knowledge.

- Chilling Effects on Civil Liberties from Loss of Anonymity. Some stakeholders point to the potential chilling effects on freedoms of speech, action, and association and other civil rights caused by the loss of anonymity in public and perpetual tracking by facial recognition

---

[26] Ian Koskela, 2014 Year in Review: Top 5 Applications of Facial Recognition, Biometric Update (Mar. 3, 2015), http://www.biometricupdate.com/201503/2014-year-in-review-top-5-applications-of-facial-recognition.
[27] *See* Kashmir Hill, *You're Being Secretly Tracked with Facial Recognition, Even in Church*, Fusion (June 23, 2015, 10:58AM), http://fusion.net/story/154199/facial-recognition-no-rules/.
[28] See Carl Gohringer, Article: Face Recognition: Profit, Ethics and Privacy, Allevate (Jan. 7, 2013), http://allevate.com/index.php/2013/01/07/face-recognition-in-retail-profit-ethics-and-privacy/; GAO Report at 13.
[29] See Joseph Lorenzo Hall, Facial Recognition & Privacy: An EU-US Perspective, (Oct. 8, 2012), https://www.cdt.org/files/pdfs/CDT_facial_recog.pdf at 13.

systems.[30]

- Misidentification. The levels of inaccuracy of facial recognition systems pose additional risks. Adverse information – such as an incorrect identification of an individual as a shoplifter – could propagate and survive across different commercial databases, even without the individual's knowledge.[31] This requires particular attention given early development challenges for many FR systems to perform reliably on racial minorities, on the old and young, and other vulnerable classes.

- Access and Control. Basic privacy principles require that individuals be aware of commercial entities that have collected data about them with facial recognition systems, that they have the ability to request to know what data has been maintained on them, and to request access to correct errors or delete the information.

- Disparate Treatment. Facial recognition technology for classification purposes based on demographic characteristics must not be used in ways that could lead to illegal profiling that results in adverse effects for certain groups.[32]

Currently, U.S. federal laws do not specifically address facial recognition. However, states may individually decide to regulate facial recognition technology, posing a threat of interstate inconsistency that could potentially raise Dormant Commerce Clause concerns. Already, three states—Texas, Illinois, and Washington—have adopted laws regulating commercial use of biometric identifiers gathered through certain types of facial recognition technology, and legislation is under discussion in multiple other states.[33]

Following the direction of a 2012 White House privacy framework, the National Telecommunications and Information Administration ("NTIA") launched a multi-stakeholder process in February 2014 to address privacy issues associated with facial recognition technology that involved convening industry representatives, trade associations, and consumer advocate stakeholders to develop a code of conduct for industry participants.[34]

Privacy principles have the real potential to advance facial recognition privacy. The Fair Information Practice Principles ("FIPPs"), a set of globally recognized, high-level principles guiding the collection, use, and disclosure of data, provide an excellent framework for such

---

[30] See, e.g., Richard Blumenthal, What Facial Recognition Technology Means for Privacy and Civil Liberties, Richard Blumenthal, U.S. Sen. for Conn., (July 23, 2012), http://www.blumenthal.senate.gov/blog/what-facial-recognition-technology-means-for-privacy-and-civil-liberties; Sarah A. Downey, The Top 6 FAQs About Facial Recognition, The Online Privacy Blog (Dec. 8, 2011), https://www.abine.com/blog/2011/facial-recognition-faqs/.
[31] GAO Report at 17.
[32] GAO report at 17.
[33] See Tex. Bus. & Com. Code Ann. § 503.001; 740 Ill. Comp. Stat. 14/1-99; Wash. HB-1094.
[34] *See* National Telecommunications and Information Administration, *Privacy Multi-stakeholder Process: Facial Recognition Technology* (2015), http://www.ntia.doc.gov/other-publication/2015/privacy-multistakeholder-process-facial-recognition-technology.

principles. In various formulations with different emphases, the FIPPs have been woven into U.S. and EU privacy laws and serve as the basis for a range of privacy frameworks established by legislatures, government agencies, and international bodies.[35]

Thus, the foundational concepts of the FIPPs are important to incorporate into facial recognition technology. A targeted application of the FIPPs concepts will allow for the principles to be used for facial recognition practices, such as providing notice and choice, to be deployed in reasonable ways that protect consumers while allowing for innovative and beneficial uses. These Principles take into account the uniquely sensitive nature of facial recognition data while respecting the context in which facial recognition data is collected and used.

The Federal Trade Commission ("FTC") has also demonstrated its interest in facial recognition technology by publishing a 2012 staff report that provides some guidance as to best privacy practices based on a targeted application of FIPPs.[36] Building on three core principles—privacy by design, simplified consumer choice, and transparency—the FTC recommends that companies using facial recognition technologies do the following:

- Take steps to ensure consumers are aware of facial recognition technologies when they come in contact with them;
- Provide consumers with clear notice about how facial recognition features or technology works, what data is collected, and how the data will be used;
- Provide consumers with choices as to data collection and use;
- Design their services with consumer privacy in mind;
- Develop reasonable security protections for the information they collect, and sound methods for determining when to keep information and when to dispose of it; and
- Consider the sensitivity of information when developing their facial recognition products and services.[37]

Finally, the FTC recommended that companies seek consumers' affirmative consent before collecting or using biometric data from facial images "before using consumers' images or any biometric data in a different way than they represented when they collected the data" and that "companies should not use facial recognition to identify anonymous images of a consumer to

---

[35] See, e.g., The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf ; FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; See generally John W. Kropf, Independence Day: How to Move the Global Privacy Dialogue Forward, Bloomberg BNA Privacy & Security Law Report (Jan. 12, 2009).

[36] *See* Federal Trade Commission, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies* (2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf .

[37] See generally id; *Federal Trade Commission, FTC Recommends Best Practices for Companies that Use Facial Recognition Technologies* (Oct. 22, 2012), https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition.

someone who could not otherwise identify him or her, without obtaining the consumer's affirmative consent first."[38]

Privacy protections for facial recognition data may also be required abroad. Under the current EU Data Protection Directive, facial recognition data is considered "personal data," an interpretation confirmed in the Article 29 Working Party's Opinion 02/2012 (the "Article 29 WP Opinion") on facial recognition in online and mobile services.[39] The Article 29 WP Opinion also recommended best practices that, along with the FTC recommendations for commercial use of facial recognition, have been incorporated into the Principles below. In addition, the Office of the Privacy Commissioner of Canada has published guidance on the collection of biometric information, including facial recognition data.[40]

[38] *See* FTC, Facing Facts at 7.
[39] Article 29 Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services (Mar. 22, 2012), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf (last accessed Sept. 1, 2015).
[40] *See* https://www.priv.gc.ca/information/research-recherche/2013/fr_201303_e.pdf.

MISSION

Future of Privacy Forum is a nonprofit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies.

WHO WE ARE

FPF brings together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

FPF helps fill the void in the "space not occupied by law" which exists due to the speed of technology development. As "data optimists," we believe that the power of data for good is a net benefit to society, and that it can be well-managed to control risks and offer the best protections and empowerment to consumers and individuals.

Future of Privacy Forum
1400 Eye Street NW, Suite 450
Washington, D.C. 20005
www.fpf.org