DISCUSSION DOCUMENT

DECEMBER 2015

PRIVACY PRINCIPLES FOR FACIAL RECOGNITION TECHNOLOGY

SUMMARY

Facial recognition technology once seemed like something out of the movies, but it is increasingly being incorporated into our everyday lives. Both public and private sector organizations are incorporating facial recognition into products and services to create substantial benefits for consumers. For example, companies are using facial recognition to make it easier for consumers to organize their photos or secure their devices in lieu of a password. Cruise lines, amusement parks and other venues use facial recognition to more easily provide consumers with collections of relevant photos from their vacations. Many other new uses are contemplated by the commercial sector, but are still in development as the accuracy and useability of the technology progresses. Largely driven by increased demand by government agencies for their security systems, the global market for facial recognition hardware and technology is forecasted to reach $2.67 billion by 2022. [1] Growth in the commercial sector is also expected as facial recognition becomes increasingly integrated with consumer electronics, entertainment, and retail services.2

As discussed in more detail below, although the potential benefits of facial recognition technology are numerous, it is important that commercial entities use the technology in a responsible manner that protects and respects consumer privacy. To facilitate this goal, the Future of Privacy Forum staff proposes the following Privacy Principles for Facial Recognition Technology ("Principles"):

1. Consent, Choice and Respect for Context: Take steps to obtain meaningful consumer consent. For practices that may not be compatible with the context of a transaction or a consumer's relationship with an organization, provide consumers with choices, at a relevant time and context, as to the collection, use, and sharing of facial recognition data.

---

[1] *See Facial Recognition Market Expected to Reach US$ 2.67 Bn by 2022 Globally*, Transparency Market Research (July 23, 2015), http://www.transparencymarketresearch.com/pressrelease/facial-recognition-market.htm.

2 Id.

If consent is not feasible for some consumers, then look for ways to minimize the use or impact of facial recognition technology for them. Companies should seek affirmative consent before identifying an anonymous or unidentified individual to third parties who did not already know their identity outside the context of the individual's relationship or transaction with the company.

2. Transparency: Provide consumers with meaningful notices about how the organization uses facial recognition technology to collect data and how facial recognition data will be used and disclosed.
3. Data Security: Implement reasonable measures to protect facial recognition data and image reference sets against loss and unauthorized access or use during collection, transmission, and storage. Maintain reasonable retention and disposal practices for facial recognition data.
4. Privacy by Design: Build in reasonable privacy and security controls at every stage of product development and throughout the organization.
5. Integrity & Access: Implement reasonable measures to maintain the accuracy of facial recognition data. Offer individuals reasonable access to review or request deletion of facial recognition data.
6. Accountability: Take reasonable steps to ensure that use of facial recognition technology and data by the organization and third-party service providers or business partners adheres to these Principles.

Recommendations for how each of these Principles may be implemented are outlined in more detail below. The Principles are intended to provide a technology-neutral framework for consumer privacy that commercial entities can choose to adopt when developing and using facial recognition technology and similar services. Businesses may implement the Principles in a variety of ways, reflecting the context of the interaction and the differences in technologies, uses, and other factors, and they may elect to incorporate additional privacy protections. The Principles do not replace (and are not intended to create inconsistencies with) applicable laws and regulations.

WHAT IS FACIAL RECOGNITION?

Facial recognition is a type of biometric technology that measures and analyzes the unique mix of a person's identifiable biometric facial characteristics. Computer vision capabilities involving faces can be loosely grouped into a few categories, ranging along a spectrum from simple facial detection to individual identification:

- Facial detection: detecting that a face appears in an image or counting unique faces in an image or across multiple images.
- Classification: analyzing the physiological or behavioral characteristics of a face to classify an individual into any number of categories, such as a particular demographic or emotional or behavioral category.

- Authentication or verification: matching the face print of a specific individual to a previously collected image of that individual for purposes of authenticating or verifying that person, without necessarily associating that face print with other information about the person.

- Individual identification: comparing a face print of an anonymous individual to a reference set of previously identified individuals for purposes of identifying the individual personally.

A number of factors can influence the accuracy of facial recognition technology. First, a facial recognition system can at most recognize a person whose face is stored in the system's reference set. Second, images must be of sufficient quality to be used reliably, and variables such as lighting, glasses, facial hair, makeup, and photo angle must be taken into account. In addition, the system's sensitivity threshold must be set appropriately so that there are not too many false positives, where the wrong person is identified, or too many false negatives, where a person who should be identified is not.

The accuracy of facial recognition technology has been increasing as companies hone their recognition algorithms[3] and the physical components of the systems improve. In addition, the increase of photos of identified individuals online[4] has lowered the costs of obtaining proprietary reference sets, which in turn lowers costs and makes facial recognition increasingly viable for a broader spectrum of commercial entities.

USES OF FACIAL RECOGNITION TECHNOLOGY

Facial Recognition in the Public Sector

In the public sector, facial recognition technology is currently used primarily for public safety and security purposes. For example:

- The Federal Bureau of Investigation ("FBI") has agreements with numerous state departments of motor vehicles ("DMVs") that allow the FBI to use facial recognition to compare subjects of FBI investigations with the millions of license and identification photos retained by participating state DMVs.[5]

---

3 See generally National Institute of Standards and Technology, NIST Rep. 8009, Face Recognition Vendor Test: Performance of Face Identification Algorithms (May 26, 2014), http://biometrics.nist.gov/cs_links/face/frvt/frvt2013/NIST_8009.pdf.

4 *See* Jim Edwards, *Planet Selfie: We're Now Posting a Staggering 1.8 Billion Photos Every Day*, Business Insider (May 28, 2014, 11:30 AM), http://www.businessinsider.com/were-now-posting-a-staggering-18-billion-photos-to-social-media-every-day-2014-5.

5 See Jessica Hughes, FBI Facial Recognition System Gives Officers an Investigative Lead, Government Technology (Oct. 20, 2014), http://www.govtech.com/public-safety/FBI-Facial-Recognition-System-Gives-Officers-an-Investigative-Lead.html.

- U.S. Customs and Border Protection is experimenting with using facial recognition technology to compare digital passport photos to the faces of individuals carrying those passports through customs.[6]

- Police forces at the local level in the U.S. and in other countries are employing facial recognition to fight crime.[7] For example, law enforcement may use facial recognition technology to live-scan a crowd at a public event to identify criminals or terrorists.[8]

- State DMVs use facial recognition technology as a way to prevent license duplications and fraud.[9]

- Some schools have implemented facial recognition systems to confirm attendance[10] and control access to their facilities.[11] One California school district is launching a facial recognition pilot program that will log elementary school children into their iPads through a biometric system rather than a manual password.[12]

Facial Recognition in the Private Sector

The commercial applications of facial recognition technology continue to evolve. Industry trade organizations and companies employing or developing facial recognition software cite four types of functions at this time that can benefit from facial recognition technology: (1) safety and security;

---

6 See U.S. Customs and Border Protection, U.S. Customs and Border Prot. Pub'n No. 0316-0415, Facial Recognition Technology Testing: Fact Sheet (2015), http://www.cbp.gov/sites/default/files/documents/501194_1to1%20Face%20ePassport_Fact%20Sheet%208.5x11_OFO_04232015_FINAL_Online.pdf.

7 See, e.g., Lorena Mongelli, NYPD Uses High-Tech Facial-Recognition Software to Nab Barbershop Shooting Suspect, New York Post (Mar. 16, 2012, 11:38 PM), http://nypost.com/2012/03/16/nypd-uses-high-tech-facial-recognition-software-to-nab-barbershop-shooting-suspect/; Tim Cushing, UK Cops Brag about Using Facial Recognition Software to Capture... A Shoplifter, TechDirt (July 23, 2014, 12:18 AM), https://www.techdirt.com/articles/20140721/13152827957/uk-cops-brag-about-using-facial-recognition-software-to-capture-shoplifter.shtml.

8 See, e.g., Vickie Chachere, Biometrics Used to Detect Criminals at Super Bowl, ABC News (Feb. 13, 2002), http://abcnews.go.com/Technology/story?id=98871; Justin Lee, UK Police to Use Facial Recognition at Music Festival, Biometric Update (June 10, 2015), http://www.biometricupdate.com/201506/uk-police-to-use-facial-recognition-at-music-festival.

9 See, e.g., State of Oregon, Facial Recognition FAQs, http://www.oregon.gov/ODOT/DMV/pages/faqs/facial_recognition.aspx. (last visited Sept. 1, 2015).

10 See, e.g., Dan Gould, UK School Uses Facial Recognition Software to Take Attendance, PSFK (Mar. 9, 2009), http://www.psfk.com/2009/03/uk-school-uses-facial-recognition-software-to-take-attendance.html.

11 See, e.g., Justin Lee, St. Louis-Based High School Installs Facial Recognition System, Biometric Update (Mar. 10, 2015), http://www.biometricupdate.com/201503/st-louis-based-high-school-installs-facial-recognition-system; Paul McCloskey, Nashville District To Test Face Recognition Security, The Journal (Nov. 13, 2007), http://thejournal.com/articles/2007/11/13/nashville-district-to-test-face-recognition-security.aspx.

12 See Merrill Hope, Facial Recognition 'Biometrics' Coming to California School System, Breitbart News Network (Mar. 21, 2015), http://www.breitbart.com/texas/2015/03/21/facial-recognition-biometrics-coming-to-california-school-district/.

(2) secure access and authentication; (3) photograph identification and organization; and (4) marketing and customer service.[13]

1. Safety and Security. Across industries, facial recognition technology can be integrated into organizations' security systems to deter crime faster than through traditional means. Retailers are integrating facial recognition technology with their closed-circuit security systems to run visitors' faces against databases of known shoplifters, members of organized retail crime syndicates, or other persons of interest.[14] Casinos use facial recognition technology keep out card counters.[15]

2. Secure Access and Authentication. Facial recognition can be used to control and track physical access to facilities and areas that need increased security. Existing applications allow users to unlock or log onto personal computers, smartphones, and video game consoles or to record workplace time and attendance in place of a password or PIN.[16] Apartment buildings are starting to deploy systems that unlock doors when a camera recognizes a resident approaching.[17] In addition, some financial institutions have installed facial recognition at access points to verify the identity of staff and external contractors who need access to areas containing sensitive information.[18] MasterCard and other financial institutions are also starting to use facial recognition to authenticate payments or other financial transactions and to reduce fraud in mobile banking applications and at ATMs.[19] In fact, biometric technology is forecasted to become the main banking identity authorization method by 2020.[20]

---

14 See, e.g., Michael Casey, Facial Recognition Software is Scanning You Where You Least Expect It, CBS News (June 25, 2015, 6:00 AM), http://www.cbsnews.com/news/facial-recognition-software-is-scanning-you-where-you-least-expect-it/.

15 See, e.g., Rob Gallo, Facial Recognition Technology, iGaming Bus. North America, Aug./Sept. 2013, 30, http://www.peakgaminggroup.com/uploads/articles/iGBNA_Issue8_p30-31.pdf.

16 See GAO Report at 9.

17 Natasha Singer, *Never Forgetting a Face*, The New York Times (May 17, 2014), http://www.nytimes.com/2014/05/18/technology/never-forgetting-a-face.html.

18 ISFEC Global, *HSBC Banks on Facial Recognition Technology*, ISFEC Global, http://www.ifsecglobal.com/hsbc-banks-on-facial-recognition-technology/.

19 See, e.g., Deidre Richardson, MasterCard's New "Selfie Authentication" Takes Advantage of Photo Feature Popularity, Inferse (July 5, 2015), http://www.inferse.com/34105/mastercards-selfie-authentication-takes-advantage-photo-feature-popularity/; Penny Crosman, Biometric Tipping Point: USAA Deploys Face, Voice Recognition, American Banker (Feb. 3, 2015), http://www.americanbanker.com/news/bank-technology/biometric-tipping-point-usaa-deploys-face-voice-recognition-1072509-1.html ; Jason Hahn, The World's First ATM With Facial Recognition Technology is Unveiled to The Public in China, Digital Trends (May 31, 2015), http://www.digitaltrends.com/cool-tech/the-worlds-first-atm-with-facial-recognition-technology-is-unveiled-to-the-public-in-china/; Jose Pagliery, MasterCard Will Approve Purchases By Scanning Your Face, CNN Money (July 1, 2015), http://money.cnn.com/2015/07/01/technology/mastercard-facial-scan/.

20 *See* Justin Lee, *Biometrics Will be Main Banking Identity Authorization Method by 2020, Says Report*, Biometric Update (June 2, 2015), http://www.biometricupdate.com/201506/biometrics-will-be-main-banking-identity-authorization-method-by-2020-says-report.

3. Photograph Tagging and Management. Many consumers' first interactions with facial recognition technology have come through photo tagging integration on social networks or private photo management software.[21] These applications help users manage their ever-expanding library of digital photos by, among other things, allowing users to quickly find a photo, efficiently add photos to an album, and share photos with others. They also may make it easier for people to learn about photos of themselves that are being distributed.

4. Marketing and Customer Service. Facial recognition technology has the potential to help organizations conduct market research, provide more tailored and relevant marketing, and customize and improve products and services.[22] Facial recognition technology in digital advertising signage can better target ads based on the demographic characteristics of passersby.[23] Dozens of shopping malls in the U.S. and abroad may be using facial recognition technology to count and categorize shoppers based on demographic attributes such as age, gender, and ethnicity.[24] Facial recognition systems could someday track customer movements around a store to provide the customer with a better shopping experience.[25]

Additional 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] 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. For example, entertainment companies can measure viewer engagement and reactions to movies and games, and medical researchers are studying how such software can help treat people with autism or identify patients with depression.[27] One facial recognition software company even offers churches the ability to scan congregants' faces to keep track of attendance.[28]

---

21 See GAO Report at 7; Josh Lowensohn, Facial Recognition Face-Off: Three Tools Compared, CNET (Sept.30, 2009, 9:36 AM), http://www.cnet.com/news/facial-recognition-face-off-three-tools-compared/; Geoffrey A. Fowler, The Best Way to Organize a Lifetime of Photos, The Wall Street Journal, (Apr. 21, 2015, 1:37 PM), http://www.wsj.com/articles/the-best-way-to-organize-a-lifetime-of-photos-1429637857.

22 See id. at 9.

[24] *See* Michael Casey, *Facial Recognition Software is Scanning You Where You Least Expect It*, CBS News (June 25, 2015, 6:00AM), http://www.cbsnews.com/news/facial-recognition-software-is-scanning-you-where-you-least-expect-it/.

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.

[28] *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/.

POTENTIAL PRIVACY CHALLENGES ASSOCIATED WITH FACIAL RECOGNITION

As with any new technology, innovative capabilities can present new or expanded privacy risks. Facial recognition data is personal and sensitive, making privacy an important challenge for companies to address.

Consumer Knowledge and Consent. A key consideration with the capture of facial recognition data from potentially large numbers of people is whether and how to obtain their informed consent, especially if those individuals are then identified or profiled against other datasets.[29] Individuals may not be able to meaningfully consent to or opt out of facial recognition data collection as such systems become widespread in public areas, and parties have recognized that in some instances, it would be impractical or impossible to require every individual seeking to use a facial recognition camera in public to obtain prior permission from any other person who may be identified.[30]

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 and long-lasting, as it is much harder for a person to change their face than their credit card number. Also, social networks and other large databases of identified individual images could increasingly become the targets of access by unauthorized individuals, leading to consumers' facial recognition data being used in ways that consumers cannot anticipate or control, and without their knowledge.

Some privacy advocates predict that the convergence of improved facial recognition technology and contemporary uploads of billions of photos linked to identifying information on the Internet[31] could one day make it technically feasible to identify almost any individual anywhere that they appear in public.[32] These privacy advocates worry that if the technology is deployed widely enough, and if businesses share facial recognition data or systems with each other, a seamless network of cameras might be created that could track a consumer from location to location.[33] Stakeholders also reference concerns that consumers have expressed about commercial tracking of their online viewing habits.[34]

Chilling Effects on Civil Rights 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 systems.[35] These

---

29 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.

30 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.

32 See GAO Report at 13.

33 Id.

34 See id. at 14.

35 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-

concerns are particularly acute in the area of government surveillance. Facial recognition tools developed for military deployments overseas are increasingly utilized for domestic law enforcement purposes in the U.S. "with few guidelines and with little oversight of public disclosure."[36]

Misidentification. Potential inaccuracy of facial recognition systems poses 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.[37]

Access and Control. Even if individuals can identify the commercial entities that have collected data about them with facial recognition systems, it could be difficult or impossible for those individuals to determine what data has been collected about them, how it is being used, who it has been shared with, and to request access to correct errors or delete the information.

Disparate Treatment. Some stakeholders are apprehensive that use of facial recognition technology for classification purposes based on demographic characteristics could lead to profiling that results in adverse effects for certain groups.[38]

FACIAL RECOGNITION PRIVACY PRINCIPLES ARE NEEDED

Currently, U.S. Federal laws do not specifically address facial recognition. However, states may also individually decide to regulate facial recognition technology, posing a threat of interstate inconsistency that could potentially raise Dormant Commerce Clause concerns. Already, two states—Texas and Illinois—have adopted laws regulating commercial use of biometric identifiers gathered through certain types of facial recognition technology, and legislation is pending in the state of Washington.[39]

Following the direction of a 2012 White House privacy framework, the National Telecommunications and Information Administration ("NTIA") launched a multistakeholder process in February 2014 to address privacy issues associated with facial recognition technology that involves convening industry and consumer advocate stakeholders to develop a voluntary, legally enforceable code of conduct for industry participants.[40] The NTIA process is ongoing,

---

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/.

36 See Timothy Williams, Facial Recognition Software Moves From Overseas Wars to Local Police, The New York Times (Aug. 12, 2015), http://www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=0.

37 GAO Report at 17.

38 Id.

39 See Tex. Bus. & Com. Code Ann. § 503.001; 740 Ill. Comp. Stat. 14/1-99; Wash. HB-1094.

40 *See* National Telecommunications and Information Administration, *Privacy Multistakeholder Process: Facial Recognition Technology* (2015), http://www.ntia.doc.gov/other-publication/2015/privacy-multistakeholder-process-facial-recognition-technology.

but in June 2015, nine privacy and consumer groups withdrew from the multistakeholder process, issuing a joint statement that the process was unlikely to yield a privacy framework that offers adequate consumer protections.[41] Regardless, NTIA, industry representatives, and other stakeholders plan to continue the multistakeholder process.[42]

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 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.[43]

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 building of principles for facial recognition use, such as providing notice and choice, to be deployed in practical 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 the data is collected and the facial recognition technology is 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.[44] 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;

---

41 See Democratic Media, https://www.democraticmedia.org/sites/default/files/field/public/2015/privacy_advocates_statement_on_ntia_facial_recognition_process_-_final.pdf (last visited Aug. 12, 2015).

42 See Andrea Peterson, The Government's Plan to Regulate Facial Recognition Tech is Falling Apart, The Washington Post (June 16, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/06/16/the-governments-plan-to-regulate-facial-recognition-tech-is-falling-apart/ (noting NTIA's and industry representatives' intentions to continue the process).

43 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).

44 *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 .

- 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.[45]

Finally, the FTC recommended that companies seek consumers' affirmative consent before collecting or using biometric data from facial images for practices that are not consistent with the context of a transaction or a consumer's relationship with a business.[46]

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.[47] 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.[48]

PRIVACY PRINCIPLES FOR FACIAL RECOGNITION

Although the potential benefits of facial recognition technology are numerous, it is important that private sector entities use the technology in a responsible manner that protects and respects consumer privacy. To facilitate this goal, the Future of Privacy Forum proposes discussion of the following Principles, which are intended to provide a flexible, technology-neutral approach to consumer privacy. Given the impossibility of a one-size-fits-all approach, businesses may implement the Principles in a variety of ways, reflecting the context of the interaction and the differences in technologies, uses, and other factors, and they may elect to incorporate additional privacy protections. They do not replace (and are not intended to create inconsistencies with) applicable laws and regulations.

---

45 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.

46 *See* FTC, Facing Facts at 7.

47 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).

48 *See* https://www.priv.gc.ca/information/research-recherche/2013/fr_201303_e.pdf.

Principle 1: Consent, Choice, and Respect for Context

Take steps to obtain ***affirmative*** consent. If consent is not feasible for some consumers, then look for ways to minimize the use or impact of facial recognition technology for them. Commit to collecting, using, and sharing facial recognition data in ways that are compatible with the context in which the data was collected, taking into account the likely impact on the individuals and the potential for innovative, pro-consumer uses of the data.

Companies should seek affirmative consent before identifying an anonymous or unidentified individual to third parties who did not already know their identity outside the context of the individual's relationship or transaction with the company.[49] For companies that, in contrast, do not have a direct relationship with the individual, consent may be required.

Further, the Respect for Context principle calls on companies that collect, use, and share facial recognition data to act as stewards of data in ways that retain consumer trust.[50]

Factors that will determine whether a prospective use is compatible, include, for example, the notices offered to consumers, context of collection, reasonable expectations 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. [51]

Companies should consider how the use of facial recognition technology will impact both consumers who purposefully avail themselves of that technology and consumers who incidentally come into contact with facial recognition products or services or cannot reasonably avoid a company's use of facial recognition technology. As an example, where facial recognition data is used to match an individual's face print to a reference set of registered users, a company should attempt to delete all facial recognition template data in the case of a no-match result.[52]

Companies also should not use facial recognition technology to engage in discrimination based on race, color, sex, national origin, disability, or age. Care should also be taken in designing and training a facial recognition system to minimize mislabeling of persons; for example, companies should seek to ensure that their facial recognition algorithms have comparable levels of accuracy across demographic variances in race, gender, and age.

---

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

[50] *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.

[51] For example, where an organization discloses in a privacy policy accepted by its subscribers that it uses facial recognition technology to identify its subscribers in photos submitted to it and a person continues to subscribe, future use of the technology is likely consistent with the context understood by a reasonable subscriber.

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

The Respect for Context principle also calls on companies whose facial recognition technology may interact with or otherwise encounter children under 13 to give special consideration to the age and sophistication of those individuals in light of the purposes for which facial recognition technology is used, including whether additional levels of transparency, choice, and data security are required.

The Respect for Context principle also recognizes that the relationship between a consumer and company may evolve over time and that compatible uses can include uses of facial recognition data that may not have been imagined at the time of collection but nonetheless are presently compatible uses and can benefit consumers. Such new uses may, despite their novelty, be consistent with context.

The Respect for Context principle is important to the successful implementation of other Principles. For example, certain contexts may require heightened measures of Transparency, Consent and Choice, and Data Security. Information and choices that are meaningful to consumers in one context may be more or less important in others. The Respect for Context principle requires companies to use facial recognition technology in a way that is fair to consumers, which would, among other things, require companies to weigh the privacy risks against clear and articulable benefits to consumers and provide opportunities for consumers to make choices to mitigate or avoid risks to their privacy.[53]

Principle 2: Transparency

Provide consumers with ***meaningful notice*** about how your organization ***collects*** facial recognition ***template*** data and how ***such*** data will be used and disclosed.

Facial recognition data collection and use should be transparent. Two important ways companies can facilitate transparency are by (1) developing and publishing privacy policies or similar educational statements describing their use of facial recognition technology and data, and (2) providing notice that facial recognition technology is being used. Applying the Respect for Context principle, required levels of transparency should be tailored to the sensitivity of facial recognition uses and the impact on the consumer.

Notice should be provided in a form and manner that is reasonably accessible to consumers before or at the time that facial recognition technology is used.

Privacy Policies and Educational Materials

Privacy policies, educational help centers, and other materials can help consumers and other stakeholders understand how a company uses facial recognition technology and collects, uses, or shares facial recognition data. In addition, developing a privacy policy or other educational materials can be a way for a company to assess and develop rules for its data collection practices.

---

53 The FTC Act's guidance as to what constitutes an unfair practice is 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."

A facial recognition privacy policy or related educational materials might include information illustrative of the following:

1. the purposes for which facial recognition data is collected;

2. whether facial recognition data may be shared;

3. the retention, deletion, or de-identification of facial recognition data;

4. the choices consumers may have regarding their facial recognition data; and

5. where consumers may direct questions about the collection, use, and sharing of facial recognition data.

Facial recognition technology vendors and companies that employ facial recognition technology or use facial recognition data should make their privacy policies publicly available via an online web portal, but may also choose to provide their privacy policy as part of owners' manuals, on paper or electronic registration forms and user agreements, or in other ways.

Contextual and just-in-time notices of the use of facial recognition technology will also be needed in a range of circumstances. For example, they can bolster privacy policies that may only speak more generally to collection, use, and disclosure of personal information and do not mention recognizing people's faces, particularly where facial recognition is merely a feature of a broader product or service or is not readily apparent to the consumer.[54]

When collection, use, and sharing practices 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.

Notice that Facial Recognition is in Use

The use of facial recognition technology may not always be readily apparent to consumers, and consumers may not know which company's privacy policy they should review. To facilitate transparency in these cases, companies should take reasonable steps to disclose that facial recognition technology is in use.

---

54 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.")

This notice (like related privacy policies) should be provided in clear language that consumers can readily understand.

Reasonable steps to facilitate transparency compliance by third-party companies using a participating company's facial recognition technology could include:

1. including reasonable limitations on use in contract language,

2. providing companies with model language for physical location signage or inclusion in their privacy notices,

3. requiring signage if the facial recognition technology will be deployed in public places; and

4. using other reasonable efforts to promote provision of clear, meaningful notice to consumers.

Principle 3: Data Security

Implement reasonable measures to protect facial recognition data and image reference sets against loss and unauthorized access or use during collection, transmission, and storage. Maintain reasonable retention and disposal practices for facial recognition data.

Reasonable data security should evolve over time and in reaction to evolving threats and identified vulnerabilities. Data security should be 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 factors. Companies should provide reasonable data security to facial recognition data when at rest and in transit.[55]

Companies may choose security technologies and procedures that best fit the scale and scope of the facial recognition data they collect and maintain, subject to their obligations under applicable data security statutes and commitments to consumers and other stakeholders. Companies should take steps to guard against unauthorized access to or uses of photos and facial recognition data.

Companies should also set reasonable retention and disposal practices for facial recognition data. Facial recognition template data that can be used to personally identify an individual, as opposed to aggregate information or simple detection or classification data, should be retained no longer than necessary for legitimate business purposes, and deleted or destroyed in a secure manner.

Principle 4: Privacy by Design

Build in reasonable privacy and security controls at every stage of product development and throughout your organization.

---

55 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.

Companies following the Privacy by Design principle should promote consumer privacy and data security throughout their organizations and proactively incorporate privacy and security into facial recognition products and services at every stage of product development and deployment. Companies can implement the Privacy by Design principle in a variety of ways, including:

- Taking a proactive approach to privacy by anticipating and preventing privacy-invasive events before they happen.

- Embedding privacy 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 privacy 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 made available to consumers or deployed.

Companies should also implement privacy by design into their organizational practices, including, for instance, assigning personnel to oversee privacy issues, training employees on privacy, and conducting privacy reviews when developing or modifying facial recognition products and services.

Principle 5: Integrity & Access

Implement reasonable measures to maintain the accuracy of facial recognition data. Offer individuals reasonable access to review or request deletion of facial recognition data.

The Integrity & Access principle recognizes that use of inaccurate facial recognition template data has the potential to harm consumers. The risk of such harms, in addition to the scale, scope, and sensitivity of facial recognition data retained by a company, may help to determine what levels of access, correction, and redress may be reasonable in a given context.

Companies should take steps to help ensure that the facial recognition data they collect is accurate, particularly if the use of such data is focused more on individually identifying users. Care should be taken to be sensitive to concerns about the mislabeling of persons, particularly with regard to demographic variances in race, age and gender.

Principle 6: Accountability

Take reasonable steps to ensure that use of facial recognition technology and data by your organization and third party service providers or business partners adheres to these Principles.

Companies should implement reasonable policies, procedures, and practices to help ensure that these Principles underlie their use of facial recognition technologies. Companies may implement training programs for employees and other personnel that handle facial recognition data. Companies may also consider creating internal privacy review boards to evaluate and approve new technologies and services involving facial recognition data. Reporting mechanisms for consumers to report concerns should be readily available. Companies should also 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.