TESTIMONY OF

THE FEDERAL TRADE COMMISSION

ON

"WHAT FACIAL RECOGNITION TECHNOLOGY

MEANS FOR PRIVACY AND CIVIL LIBERTIES"

PRESENTED BY

MANEESHA MITHAL

ASSOCIATE DIRECTOR, DIVISION OF PRIVACY AND IDENTITY PROTECTION

SENATE COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW

July 18, 2012

I. Introduction

Chairman Franken, Ranking Member Coburn, and members of the Subcommittee, I am Maneesha Mithal, Associate Director of the Division of Privacy and Identity Protection at the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on facial recognition technologies.[1]

Facial recognition technologies currently operate across a spectrum, ranging from pure facial detection, which simply means detecting a face in an image, to biometric analysis of facial images, in which unique mathematical data are derived from a face in order to match it to another face.[2] In the latter example, if one of the faces is identified – *i.e.* the name of the individual is known – then in addition to being able to demonstrate a match between two faces, the technology can be used to identify previously anonymous faces. In between these two points are a range of possibilities that include determining the demographic characteristics of a face, such as age range and gender, and recognizing emotions from facial expressions.

Having overcome the high costs and poor accuracy that once stunted their growth, facial recognition technologies are quickly moving out of the realm of science fiction and into the commercial marketplace.[3] Today facial recognition technologies can be found in a wide array of

---

[1] This written statement represents the views of the Federal Trade Commission. My oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or of any Commissioner. Commissioner J. Thomas Rosch dissents to certain portions of the testimony. His views are explained in the attached separate statement.

[2] *See* Dr. Joseph J. Atick, International Biometrics & Identification Association, *Face Recognition in the Era of Cloud and Social Media: Is it Time to Hit the Panic Button?* (Dec. 2011), at 2, *available at* http://www.ibia.org/resources/.

[3] Throughout this testimony, the term "facial recognition" is used broadly to refer to technologies that are used to extract data from facial images. *See* Sony, Face Recognition Technology, http://www.sony.net/SonyInfo/technology/technology/theme/sface_01.html.

contexts, including digital signs, mobile applications, and social networks. While consumers may enjoy the benefits associated with advancements to these technologies – such as easier organization of online photos – there are also concerns that the technologies may increase the risks to consumer privacy. Recognizing that the commercial use of these technologies will likely continue to grow, the FTC has sought to understand how these technologies are being used, how they could be used, and how they will shape consumers' commercial experiences.

To examine these issues, the FTC hosted a workshop in December 2011 – "Face Facts: A Forum on Facial Recognition Technology" ("Face Facts workshop").[4] Researchers, academics, industry representatives, and consumer and privacy professionals all took part in a series of wide-ranging discussions. Major topics included the recent advances, current uses, and possible future uses of facial recognition technologies, as well as the privacy and security concerns those issues raise. Following the workshop, Commission staff requested public comments regarding a number of topics and questions.[5] Commenters were asked to provide input on, among other issues: the privacy and security concerns surrounding the commercial use of these technologies, best practices for providing consumers with notice and choice about the use of these technologies, and best practices for deploying these technologies in a way that protects consumer privacy. The FTC received eighty public comments from private citizens, industry representatives, trade groups, consumer and privacy advocates, think tanks, and members of

---

[4] FTC Workshop, *Face Facts: A Forum on Facial Recognition Technology* (Dec. 8, 2011), http://www.ftc.gov/bcp/workshops/facefacts/.

[5] *See* Press Release, FTC, FTC Seeks Public Comments on Facial Recognition Technology (Dec. 23, 2011), *available at* http://www.ftc.gov/opa/2011/12/facefacts.shtm.

Congress, reflecting a wide variety of viewpoints on these issues.[6] We are still reviewing these comments, and staff plans to use the information we have learned to date to release a report later this year setting forth recommended best practices for using facial recognition technologies in a manner that respects consumer privacy while still allowing consumers to receive the benefits these technologies may provide, such as convenience and more personalized service. The report would not serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.

The FTC is also considering how the three core principles articulated in the Commission's March 2012 report on consumer privacy ("Privacy Report") – privacy by design, simplified consumer choice, and transparency – can be applied to the use of facial recognition technologies.[7] These principles call upon companies handling consumer data to implement privacy by design by building in privacy protections at every stage in the development of their products and services, provide consumers with simplified choices about the collection and use of their information, and increase transparency by providing clearer, shorter and more standardized privacy notices.

This testimony addresses solely commercial uses and does not address the use of facial recognition technologies for security purposes or by law enforcement or government actors. It describes the current facial recognition landscape, including: (1) recent advances in facial

---

[6] *See* FTC, # 402; FTC Seeks Public Comments on Facial Recognition Technology; Project Number P115406, http://www.ftc.gov/os/comments/facialrecognitiontechnology/index.shtm.

[7] FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, *Recommendations for Businesses and Policymakers,* (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

recognition technologies, (2) current commercial uses of facial recognition technologies, and (3) possible future commercial uses of facial recognition technologies. The testimony concludes by setting forth some privacy considerations the Commission is examining as staff prepares its facial recognition report and weighs next steps in this area.[8]

II. Current Facial Recognition Landscape

A. Recent advances in facial recognition technologies

Until recently, because of high costs and limited accuracy, facial recognition technologies were not widely used on a commercial basis. However, recent years have brought steady improvements in these technologies. Several developments have contributed to the increased accuracy in facial recognition systems. For example, better quality digital cameras and lenses create higher quality images, from which biometric data can be more easily extracted. In addition, the goal of some facial recognition technologies is to match an image of an unknown face to an identified "reference photo," where the name of the individual is known. Until recently, it was difficult to match two images if the photos were taken from different angles. With current technologies, companies can generate 3D face images to help reconcile pose variations in different images.

These recent technological advances have been accompanied by rapid growth in the availability of identified photos online. Previously, most of the images available online were of celebrities, but today there are many sources of identified images of private citizens online. One

[8] This hearing, and therefore this testimony, focuses specifically on facial recognition technology. However, the Commission is aware that there have also been recent advances in other forms of biometric technologies, such as voice recognition, which may raise similar privacy concerns. Accordingly, the Commission is working to better understand the privacy implications of all forms of biometric technology that commercial entities are using.

explanation for this is the rise in popularity of social networking sites. For example, approximately 2.5 billion photos are uploaded to Facebook each month.[9] This multitude of identified images online can eliminate the need to purchase proprietary sets of identified images, thereby lowering costs and making facial recognition technologies commercially viable for a broader spectrum of commercial entities.[10]

B. Current commercial uses of facial recognition technologies

As noted, facial recognition technologies currently operate across a spectrum ranging from the ability to determine that a photo has a face in it ("pure facial detection") to the ability to identify demographic characteristics of a face, to the ability to match different images of the same face and possibly identify an unknown face. In many cases, the privacy risks associated with commercial uses of facial recognition increase along with the sophistication of the technology at use. For example, the privacy risks associated with companies using facial recognition to identify an unknown face are generally much greater than the risks raised by a company using pure facial detection to locate a face in an image.

Current uses of pure facial detection include, among others, refining search engine results to include only those results that contain a face, locating faces in images in order to blur or de-identify them, or ensuring that the frame for a video chat feed actually includes a face. Pure facial detection is also used in virtual eyeglass fitting systems and virtual makeover tools that

---

[9] *See* Chris Putnam, *Faster Simpler Photo Uploads*, THE FACEBOOK BLOG (Feb. 5, 2010), http://blog.facebook.com/blog.php?post=206178097130.

[10] *See* Center for Democracy & Technology, *Seeing is ID'ing: Facial Recognition & Privacy*, Center for Democracy & Technology (Jan. 22, 2012) at 3, *available at* https://www.cdt.org/files/pdfs/Facial_Recognition_and_Privacy-Center_for_Democracy_and_Technology-January_2012.pdf.

allow consumers to "try on" a pair of glasses or a new hairstyle online. In these systems, after the consumer has uploaded a photo of herself to the website, that photo is scanned, basic facial features are picked out and – using the detected facial features as reference points – the eyewear or hairstyle is superimposed on the consumer's face.

More sophisticated technologies that do not merely distinguish a face from surrounding objects, but also assess various characteristics of that face, can be used commercially in a variety of ways. For instance, companies can use technologies that identify moods or emotions from facial expressions to determine a player's engagement with a video game or a viewer's excitement during a movie.

Companies are also using technologies that determine demographic characteristics to deliver targeted advertisements in real-time in retail spaces.[11] These companies place cameras – which assess the age range and gender of the consumer standing in front of the screen – into digital signs or kiosks. They then display an advertisement based on that consumer's assessed demographic characteristics. For example, a 30 year-old male might be shown an advertisement for shaving cream, while a 50 year-old female may be shown an advertisement for perfume. As currently implemented, companies do not appear to be storing images processed by digital signs for future use.

Digital signage is an area where industry trade groups have proactively issued guidance and "best practices" for their members. For example, Point of Purchase Advertising International's Digital Signage Group ("POPAI") has developed a code of conduct containing

---

[11] Shan Li and David Sarno, *Advertisers start using facial recognition to tailor pitches*, LA TIMES, Aug. 21, 2011, *available at* http://articles.latimes.com/2011/aug/21/business/la-fi-facial-recognition-20110821.

recommendations for marketers to follow in order to maintain ethical data collection practices in retail settings.[12] Similarly, the Digital Signage Federation worked with the Center for Democracy and Technology to craft a voluntary set of privacy guidelines for their members, which include advertisers and digital sign operators.[13] Both of these self-regulatory codes address the use of facial recognition technologies in digital signs.

One company has leveraged this ability to determine age range and gender in order to obtain aggregated demographic data about the clientele of bars and nightclubs via cameras placed at the entrance to these venues. This company only stores the aggregated demographic data, and not images of the venues' customers. Both the operators of the venue and third parties – such as liquor distributors – can use this data to understand the demographics of a particular venue's customers at certain times, and possibly tailor their specials or promotions accordingly. This company also makes the aggregate information it collects available through a mobile app that consumers can use to make decisions about which venues to patronize.[14]

Facial recognition technologies that are used to actually identify individuals, rather than simply to detect a face or demographic characteristics, work by deriving unique biometric data from facial images. This biometric data is the unique mathematical characteristics that are extracted from the image in order to capture the individual identity (e.g., distance between eyes,

---

[12] POPAI, Digital Signage Group, *Best Practices: Recommended Code of Conduct for Consumer Tracking Research* (Feb 2010) *available at* http://www.popai.com/docs/DS/2010_dscc.pdf.

[13] *See* Digital Signage Federation, *Digital Signage Privacy Standards* (Feb. 2011) *available at* http://www.digitalsignagefederation.org/Resources/Documents/Articles%20and%20Whitepapers/DSF%20Digital%20Signage%20Privacy%20Standards%2002-2011%20%283%29.pdf.

[14] *See* SceneTap, http://www.scenetap.com/.

ears, size of features, etc.). Those unique mathematical characteristics can then be compared to the characteristics extracted from other facial images to determine if there is a match.[15]

This type of technology has been implemented in a variety of manners. For example, a mobile phone user can authenticate herself by using her face, rather than a password, to unlock her phone. One of the most prevalent current uses of this technology is to enable semi-automated photo tagging or photo organization on social networks and in photo management applications. On social networks these features typically work by scanning new photos a user uploads against existing "tagged" photos. The social network then identifies the user's "friends"[16] in the new photos so the user can tag them. As currently implemented, these features on social networks suggest "tags" only of people that the user already knows, either through a "friend" relationship or other contacts that suggest the two individuals know each other.

C. Possible future commercial uses of facial recognition technologies

Future uses of facial recognition technologies may provide new and exciting products and services that consumers want. They may also provide privacy and security benefits. For example, as noted above facial recognition technology can be used to authenticate users on mobile devices. In the future, we can foresee broader use of these technologies for authentication purposes which can enhance privacy and security for consumers.

At the same time, there may be privacy and security concerns. For example, will it become feasible to use facial recognition to identify previously anonymous individuals in public

---

[15] *See* Dr. Joseph J. Atick, International Biometrics & Identification Association, *Face Recognition in the Era of Cloud and Social Media: Is it Time to Hit the Panic Button?* (Dec. 2011), at 2, *available at* http://www.ibia.org/resources/.

[16] We use the term "friend" to refer to an individual user that another user has a mutual connection with on the social network.

places, such as streets or retail stores, or in previously unidentified photos online? While it does not seem that it is currently possible for commercial entities to accomplish this on a wide scale, recent studies suggest that in the near future, it may be possible. For example in a 2011 study, Carnegie Mellon researchers were able to identify individuals in previously unidentified photos from a dating site, by using facial recognition technology to match them to their Facebook profile photos.[17]

Some have surmised that advances in facial recognition technologies may end the ability of individuals to remain anonymous in public. If these predictions come to fruition, companies could employ facial recognition technologies in a number of ways that raise significant privacy concerns. For example, companies could match images from digital signs with other information to identify customers by name and target highly-personalized ads to them based on past purchases, or other personal information available about them online. Further, a mobile app that could, in real-time, identify previously anonymous individuals on the street or in a bar could cause serious privacy and physical safety concerns, although such an app might have benefits for some consumers.

III. Questions and Next Steps

In its March 2012 Privacy Report the Commission articulated three core principles for companies to consider in protecting consumer privacy:

(1) **Privacy by Design**: The Commission called on companies to build in privacy at every

---

[17] *See Face Recognition Study - FAQ*, http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/. This study used a limited geographic area, and therefore a limited number of photos and subjects; thus, the results cannot necessarily be duplicated on larger scale. *See Face Facts Workshop, Remarks of Prof. Alessandro Acquisti, Carnegie Mellon University*, at 130-131 and 138-139.

stage of product development. Such protections include providing reasonable security for consumer data, collecting only the data that is consistent with the context of a particular transaction or the consumer's relationship with the business, retaining data only as long as necessary to fulfill the purpose for which it was collected, safely disposing of data no longer being used, and implementing reasonable procedures to promote data accuracy. The Commission also called on companies to implement and enforce procedurally sound privacy practices throughout their organizations, including, for instance, assigning personnel to oversee privacy issues, training employees on privacy issues, and conducting privacy reviews when developing new products and services.

(2) **Simplified Consumer Choice**: The Commission noted that, for practices that are not consistent with the context of a transaction or a consumer's relationship with a business, companies should provide consumers with choices at a relevant time and context. In addition, companies should obtain affirmative consent before (1) collecting sensitive data or (2) using consumer data in a materially different manner than claimed when the data was collected.

(3) **Transparency**: The Commission called on companies to increase the transparency of their data practices so that interested parties can compare data practices and choices across companies. The Commission also suggested that companies – particularly those that do not interact with consumers directly, such as data brokers – provide consumers with reasonable access to the data that the companies maintain about them.

The Commission intends to release a report this year laying out recommended best practices for the use of facial recognition technologies that build on comments by workshop

panelists, written submissions, and these three core principles. In developing the report, the Commission is considering the following questions.

First, the Commission is considering ways in which companies using facial recognition technologies can implement "privacy by design." For example, how can companies establish and maintain sound retention and disposal practices for the consumer images and biometric data that they collect? For instance, should digital signs using demographic detection ever store consumers' images? Are there certain sensitive areas where companies should not place digital signs? Are there ways that the use of facial recognition technologies may increase consumer information privacy and security?

Second, the Commission is examining how companies that use these technologies can provide consumers with simplified choices about the collection and use of their data. How should companies using facial recognition technology provide choices? Under what circumstances should companies seek consumers' affirmative express consent before engaging in facial recognition?

Finally, the Commission is considering how companies using facial recognition technologies can increase the transparency of their data practices. For example, are consumers aware that digital signs using demographic detection are being used in retail environments? How can they be made aware? Similarly, how many consumers know that social networks have begun implementing facial recognition for photo "tagging"? How and when should these social networks disclose their practices to consumers? The Commission is currently evaluating these and other questions as it develops a final report on the use of facial recognition technologies in commercial environments.

IV. Conclusion

Thank you for the opportunity to provide the Commission's views on the topic of facial recognition. We look forward to continuing to work with Congress and this Subcommittee on this important issue.