TESTIMONY OF

THE FEDERAL TRADE COMMISSION

ON

THE USE OF FACIAL RECOGNITION TECHNOLOGY

BY GOVERNMENTS AND THE PRIVATE SECTOR

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

[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*

contexts, including digital signs, mobile applications, and social networks. While consumers may enjoy the benefits associated with advan.66z9.3 T0osc 0 Tw -ene

[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.

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 use of hig

[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.

[11] Shan Li and David Sarno, *Advertisers start using facial recognition to tailor pitches*, LA TIMES

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/2010dscc.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/.

See Dr. Joseph J. Atick, International Biometrics & Identifica 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.

IV.