Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FTC And Facial ID Tech: What Businesses Should Know


Kurt Wimmer

Law360, New York (November 08, 2012) -- Facial recognition technology is no longer the stuff of sci-fi movies. From online photo tagging tools to digital signs that target ads based on the age and gender of passersby, commercial uses of facial recognition are increasingly common. The growing use of facial recognition in the private sector caught the eye of the Federal Trade Commission in late 2011. In December of that year, the FTC held a workshop on the privacy implications of facial recognition, and then sought comments on the issues raised at the workshop.

Building on the workshop and the comments, the FTC recently released a staff report urging companies to adopt best practices for commercial uses of facial recognition. The report, "Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies," discusses how the core privacy principles set forth in the FTC's March 2012 report on consumer privacy[1] — privacy by design, simplified choice and transparency — should inform the use of facial recognition technologies.

Below, we provide an overview of the staff report's guidance on how each of these principles should be applied by companies that employ facial recognition in their products and services.

Privacy by Design

The principle of privacy by design holds that companies should consider privacy throughout their organizations, at every stage of product development, and during the entire lifecycle of the data that they collect (from initial acquisition to disposal). In the facial recognition context, this broad principle means three things:

Provide reasonable security not only for the biometric data extracted from images but also for the underlying images themselves.

The report endorses the use of encryption for stored biometric data, suggesting that encryption diminishes the likelihood that such data could be used by a wrongdoer who acquires the data without authorization. More notably, however, the report also suggests that companies that make identified photos available for public viewing take steps to prevent the unauthorized "scraping" of these photos. The staff's concern with scraping is that the scraped photo could be used as a reference against which an unidentified photo could be compared, potentially resulting in the identification of the person in the unidentified photo.

Establish and maintain appropriate retention and disposal practices.

The report's guidance on retention and disposal largely echoes the guidance the FTC provided in its March 2012 privacy report: Consumer data should be retained only for as long as necessary to carry out the purpose for which it was collected. So, for example, when an eyeglass company allows consumers to upload their images to the company's website in order to enable consumers to virtually "try on" different pairs of glasses, the company should only retain those images for as long as is necessary to provide that service.

Although the report suggests it would be permissible to allow the consumer to save his or her image for use across different sessions, the report also states that the consumer should be given the opportunity to have the image deleted. Similarly, in the photo tagging context, where companies store biometric data derived from previously uploaded photos in order to suggest tags for new photos, the report says that those companies should delete that biometric data if the user decides to turn off the photo-tagging feature.

Finally, and perhaps most notably, the report explains that "in all cases, the company should ... inform consumers of: (1) the length of time images are stored, (2) who will have access to the stored images, and (3) consumers' rights regarding deletion of the stored images."

Consider the sensitivity of information when using facial recognition technologies.

The FTC's March 2012 report suggested that companies consider the sensitivity of the data they maintain in developing their data management practices, noting, for example, that sensitive data (e.g., geolocation data) generally should be retained for less time than other data. The facial recognition report's discussion of the relative sensitivity of facial recognition data focuses less on the kind of facial recognition data that a company collects (e.g., data that can be used to uniquely identify an individual vs. data that can be used to assess age or gender) than it does on the place where facial recognition data is collected.

For example, the report suggests that digital signage companies be "vigilant regarding the locations of signs" that employ facial recognition technology and should not place them in "sensitive areas, such as bathrooms, locker rooms, health care facilities, and areas where children congregate." Also, the report highlights as a key concern the prospect that facial recognition technology could be used to identify otherwise anonymous people in public places.

Simplified Choice

The FTC's March 2012 report advised that companies should provide choice before collecting and using consumer data for practices that are not "consistent with the context of the transaction or the company's relationship with the consumer."

Although that report suggested that the ability to opt out of a practice for which choice is required generally is sufficient, it also discussed several practices that required the "affirmative express consent" of the consumer. Facing Facts invokes the same general standard for when choice is required with respect to the collection and use of data for facial recognition, and also notes certain practices for which affirmative express consent should be obtained.

Clear notice to users — provided outside of a privacy policy — will be sufficient for most current uses of facial recognition technology.

Where a use of facial recognition is inconsistent with the context in which the consumer interacts with the technology, Facing Facts suggests that the ability to "opt out" usually will be sufficient. For example, the report notes that notifying consumers of the presence of digital signs that use facial recognition technology before the consumers come into contact with these signs is sufficient because it gives consumers the opportunity to exercise "walk away choice."

Similarly, providers of photo tagging tools should provide upfront notice of how their tool works (including the data it collects and how the data will be used), and permit consumers to turn off the feature and have any previously collected biometric data deleted.

For certain practices, however, affirmative express consent should be obtained.

As a general matter, the report states that companies must obtain affirmative express (i.e., opt-in) consent before using previously collected images or biometric data in a materially different way than was promised when the images or data were collected. This principle will be familiar from previous FTC pronouncements about companies' obligations in the event of a material change to their data practices.

The report also provides guidance with respect to specific practices that require an opt-in. These include situations in which a digital sign operator individually identifies consumers through its signs and situations in which a social networking service identifies users of its service to other users who are not their "friends."

Transparency

Throughout Facing Facts, the FTC staff emphasizes the importance not only of providing clear notice to consumers who may interact with a technology that uses facial recognition, but also of general consumer education about these technologies — and about sharing photos online. The report notes that education about the implications of sharing photos "has particular relevance for teens, who often impulsively post photos and other content without an understanding that the photos could be used for unintended, secondary purposes."

It is important to note in closing that Facing Facts is properly understood as a statement of suggested best practices. The staff makes clear that the report is not intended to have the force of law or to serve as authoritative guidance from the FTC. Still, considering the undeveloped legal terrain surrounding facial recognition (and other technologies that use biometric data), the report provides much-needed guideposts for businesses looking to make use of this promising technology.

--By Kurt Wimmer and Stephen Satterfield, Covington & Burling LLP

Kurt Wimmer is a partner in Covington & Burling's Washington, D.C., office. He is co-chairman of the firm's global privacy and data security practice group. Stephen Satterfield is an associate in Covington's Washington office and a member of the global privacy and data security practice group.

[1] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012).