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 Eyes Privacy Limits For Facial Recognition Rules

By **Allison Grande**

Law360, New York (February 03, 2012, 8:00 PM ET) -- In developing a strategy for policing facial recognition technology, the Federal Trade Commission will need to decide when it is being used in a seemingly reasonable way and when it goes beyond consumers' reasonable expectation of privacy, attorneys say.

Having held a workshop and having sought public comment on the issue in recent months, the FTC must now consider what uses of this technology, which relies on images collected from the public sector, violate consumers' privacy in crafting any regulation, a determination that could potentially clarify what constitutes a reasonable use of a broad range of technologies in the privacy realm.

"Some uses of personal information are so trivial and harmless that neither notice nor express consent is needed," Reed Smith LLP partner Paul Bond said. “But if you want to use personal information in an unexpected way … you may often do so by providing good notice and getting valid consent.”

Facial recognition technology "turns both intuitions on their head," Bond said.

The Electronic Privacy Information Center has called for a ban on facial recognition technology until adequate safeguards and privacy standards can be established.

In detailed comments to the FTC on Tuesday, the group urged the agency to take "affirmative steps" to ensure the protection of consumers’ right to safeguard their identity, saying it should impose a moratorium on the commercial deployment of the technology in the absence of formal guidelines and legal standards.

Seven members of a bipartisan congressional privacy caucus have also asked the FTC to establish clear policies guiding the implementation, operation and maintenance of this new technology. Such policies are essential, the caucus said in a letter to the agency Tuesday.

Consumers should have the choice to affirmatively opt-in to being the subject of facial recognition, the caucus said.

The caucus' letter applauded the FTC for paying attention to privacy and security concerns by holding a public workshop on the topic in early December, during which the agency vowed to take a hard-line on companies that violate consumers' privacy using this technology and by soliciting public comment on the topic through Jan. 24.

Unlike online behavioral advertising and other purported privacy intrusions that regulators and lawmakers are seeking to curb, facial recognition technology relies on the relatively unremarkable occurrence of someone posting and tagging a picture of a person online.

But that posting allows information available by name to be linked and cross-linked with information about a person by sight, a process that the individual only indirectly consented to by willing to be photographed.

The information can then be used for tasks that individuals may find reasonable, such as comparing photographs in a missing children's database to photos from a public place or protecting the security of a store membership card, or in ways that consumers could view as above their expectations, such as being served a targeted ad or to link unwanted information to an individual.

"The FTC is concerned about where to draw the line between a helpful algorithm that gets inappropriate images off of Facebook and the invasive facial recognition manifestations of the same technology," said Andrew B. Serwin, the founding chair of Foley & Lardner LLP's privacy, security and information management practice. “It’s hard to predict where it will draw that line, especially considering that this technology doesn’t involve someone’s purely private behavior being collected and exposed.”

In making these determinations, the FTC is likely to try its best to strike a balance between the benefits that this innovation brings and the significant privacy concerns raised by its existence, according to Sheppard Mullin Richter & Hampton LLP partner Craig Cardon.

“The question facing the FTC will be how do we allow this new technology to grow and emerge without cutting it off before it happens by burdening it with new rules, while still protecting consumers’ interests,” he said.

While Facebook’s facial recognition feature is the most notable example of this technology, the “more dispersed and less regulated” area of mobile app developers may pose as many issues as social media sites, according to Bond.

“The temptation in the startup phase [that some mobile app developers are in] is to collect and use information now and ask for forgiveness later,” Bond said.

Regulators should also be mindful of the differences between facial detection, which detects the characteristics of a person but does not specifically identify the individual, and facial recognition, which matches an image to a person’s identity.

“Detection doesn’t do anything more than what a person standing in public could do if they walked up to another person, while facial recognition puts a name to something that had been anonymous,” Cardon said. “Each process raises different questions about how much needs to be disclosed to consumers and what kind of consent needs to be obtained.”

Instead of proposing stringent regulations on the industry, the FTC could allow companies to come up with their own approach for dealing with facial recognition technology, and then use its authority under Section 5 of the FTC Act to pursue bad actors who violate the protections laid out in their privacy policies, Cardon noted.

Consumer education could also prove beneficial to supplement this self-regulation, Bond added.

“Showing how the technology has been evolving and educating the public about the consequences of sharing information about themselves can help consumers understand that there may be the prospect of surveillance in certain situations that didn’t exist before,” Bond said.

The FTC is likely to take a different approach than international regulators because the U.S. doesn’t have the same stringent privacy protection framework that qualifies this information as personal data as in other countries, according to attorneys. For example, Germany's data protection regulator in August ordered Facebook to remove its facial recognition feature or face fines.

Private civil actions challenging this technology are likely to fail due to the difficulty of proving actual harm or financial loss, leaving consumers to rely on the FTC and lawmakers to decide how to best protect their privacy.

“Unless people can identify an invasion of their expectation of privacy that caused them harm, there is not much potential for private consumer lawsuits to act as a way to regulate this issue,” Cardon said.

No matter what approach the FTC and lawmakers take with the information collected from the public on this topic, the growing stock of personal information online will only fuel this privacy debate in the future.

“Computers can process so much information that is cropping up that consumers want out there, but they don’t want that information to be skewed,” Serwin said. “Everyone agrees that it’s important to try to balance innovation and consumer protection, but reasonable minds differ on how exactly to do that.”

--Editing by Andrew Park.