Published on *The National Law Review* https://natlawreview.com

Facial Recognition Technology: Social Media and Beyond, an Emerging Concern

Article By:

Jeffrey D. Neuburger

This week, a major self-regulatory initiative intended to address privacy concerns associated with facial recognition technology hit a significant stumbling block. Nine consumer advocacy groups withdrew from the ***National Telecommunications and Information Administration*** (NTIA)-initiative due to a lack of consensus on a minimum standard of consent. The NTIA initiative had been ongoing since early 2014. Consumer advocacy and civil liberties groups were participating with industry trade groups in NTIA-sponsored meetings intended to create guidelines on the fair commercial use of facial recognition technology. Advocates and industry groups were attempting to develop a voluntary, enforceable code of conduct for the use of facial recognition technology and generally define the contours of transparency and informed consent.

The deadlock in discussions and withdrawal of key participants in those discussions highlights how difficult the resolution of those issues will be.

Facial recognition technology is a powerful tool with many potential uses. Some are relatively well-known, particularly those which identify people in online social networks and photo storage services. For example, Facebook and others have for years employed “tag suggestion” tools that scan uploaded photos and identify network friends and suggest that the member “tag” them. How does the technology work? Facebook explains: “We currently use facial recognition software…to calculate a unique number (“template”) based on someone’s facial features, like the distance between the eyes, nose and ears. This template is based on your profile pictures and photos you’ve been tagged in on Facebook. We use these templates to help you tag photos by suggesting tags of your friends.”

Taking it a step further, earlier this month Facebook introduced “Moments,” a new app that syncs photos stored on a user’s phone based, in part, on which friends are depicted in the photos.

Other uses of the technology are not as familiar. Facial recognition technology and “faceprints” have been used, for example, in retailer anti-fraud programs, for in-store analytics to determine an individual’s age range and gender to deliver targeted advertising, to assess viewers’ engagement in a videogame or movie or interest in a retail store display, to facilitate online images searches, and to develop virtual eyeglass fitting or cosmetics tools. While these capabilities may be quite useful, many users consider the technology to be uncomfortably creepy.

The technology has been the focus of privacy concerns for quite a while. In October, 2012, the Federal Trade Commission (the "FTC") issued a report, "Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies." The FTC staff made a number of specific recommendations with respect to the use of the technology, including, without limitation, providing clear notice about collection and use, giving users opt-out rights, and obtaining express consent before using a consumer's image in a materially different manner than originally collected.

Individual states have also legislated in this area. For example, Texas and Illinois have existing biometric privacy statutes that may apply to the collection of facial templates for online photo tagging functions. Illinois's "Biometric Information Privacy Act," ("BIPA") 740 ILCS 14/1, enacted in 2008, provides, among other things, that a company cannot "collect, capture, purchase, receive through trade, or otherwise obtain a person's… biometric information, unless it first: (1) informs the subject … in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject … in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information." 740 ILCS 14/15(b). The Texas statute, Tex. Bus. & Com. Code Ann. §503.001(c), enacted in 2007, offers similar protections.

Neither statute has been interpreted by a court with respect to modern facial recognition tools, but that may change in the coming months. In April of this year, a putative class action complaint was filed in Illinois state court against Facebook over a tagging feature that rolled out in 2010 and has been used to create, what the plaintiffs term, "the world's largest privately held database of consumer biometrics data." ***Licata v. Facebook, Inc.***, No. 2015CH05427 (Ill. Cir. Ct. Cook Cty. filed Apr. 1, 2015). The plaintiffs brought claims against Facebook for allegedly collecting and storing biometric data without adequate notice and consent and failing to provide a retention schedule and guidelines for permanent deletion, or otherwise comply with BIPA with respect to Illinois users. The complaint seeks an injunction and statutory damages for each violation (note: BIPA provides for $1,000 in statutory damages for each negligent violation, and $5,000 for intentional violations, plus attorney's fees). Facebook counters that users can turn off tag suggestion, which deletes a facial recognition template.

A month later, a similar suit alleging violations of BIPA was filed against Facebook. (***Patel v. Facebook, Inc.***, No. 15-04265 (N.D. Ill. filed May 14, 2015)). Moreover, last week, a putative class action suit was brought against the photo storage service Shutterfly in Illinois federal court alleging violations of the BIPA for collecting faceprints from user-upload photos in conjunction with a tag suggestion feature. (***Norberg v. Shutterfly, Inc***., No. 15-05351 (N.D. Ill. filed June 17, 2015)).

Based on the NTIA discussions, the FTC report, and the issues raised in the Illinois litigations, it is clear that there are numerous considerations for companies to think about before rolling out facial recognition features, including:

- How should the concepts of transparency and consent apply to the use of facial recognition tools?
- What level of control should individuals have over when and how a faceprint is stored and used?
- Should companies obtain prior affirmative consent before collecting such data, as most apps do before collecting geolocation data?
- Does facial recognition technology clash with a consumer's rights in a way that "manual" tagging of photographs by social media users would not?
- How should a company's policy regarding facial recognition deal with non-members of a

service or anonymous members of the public captured in a photo?
- What level of transparency is appropriate when a company combines facial profiles with third-party data for analytics or secondary uses?
- How should a company address retention periods for faceprints?
- What should happen to the faceprint of a user who unsubscribes from a service?
- Should faceprint data be the subject of heightened data security (e.g. encryption)?
- Should additional restrictions be placed on the use of commercial facial recognition technology by teens?
- Would a standard electronic contracting process, whereby a user consents to a service’s terms of service and privacy policy via a clickwrap agreement, constitute appropriate notice and consent for the use of facial recognition? Or must there be a distinct, written notice and consent process for facial recognition data collection practices as well as a formal, posted facial recognition policy?

These questions and more are yet to be answered. Companies that are planning on using facial recognition technology – whether in mobile apps, online, or even in offline applications – should be aware of the emerging legal landscape in this area. More litigation in this area is likely.

National Law Review, Volume V, Number 174

Source URL:https://natlawreview.com/article/facial-recognition-technology-social-media-and-beyond-emerging-concern