CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 160 years

WEDNESDAY, OCTOBER 21, 2015

Chicago Daily Law Bulletin®

Volume 161, No. 206

Illinois finds itself at forefront of facial-recognition litigation

Illinois is leading the way in regulating facial-recognition technology — it is one of only two states (the other Texas) that has passed laws covering the collection and use of biometric information. Illinois also is currently the only state where litigation over facial recognition technology has been filed.

Five lawsuits are pending in Illinois courts — one against Shutterfly Inc., the photo storage and publishing site, and four against social media platform Facebook. All of the cases allege that the companies are violating the state's Biometric Information Privacy Act.

While the number of laws — and the number of lawsuits — likely will increase, the outcomes of these groundbreaking cases may signal where the state and the country may be headed in regulating the collection, storage and use of biometric information

Biometric technologies, including facial-recognition technology, "identify people using their faces, fingerprints, hands, eye retinas and irises, voice and gait among other things," according to the U.S. Government Accountability Office's July 2015 report titled "Facial Recognition Technology: Commercial Uses, Privacy Issues and Applicable Federal Law."

According to the report, unlike conventional identification methods, such as the use of a card to access a building or a password to log onto a computer system, "biometric technologies measure things that are generally distinct to each person and cannot easily be changed."

The GAO report notes that a facial recognition technology system usually includes four components: a camera; an algorithm to create a "face print" or a facial template; a database of stored images; and an algorithm to compare the captured image to the database of images.

To consumers, the best-known use of facial-recognition technology is the photograph identification or "tagging" in social networking applications.

Illinois enacted the Biometric Information Privacy Act in 2008 in response to a number of companies testing new applications of finger-scan technologies for in-store purchases and other financial transactions. The act prohibits collecting, capturing or otherwise obtaining a person's biometric information unless the company first informs the subject in writing that the information is being collected, why the information is being collected and how long it will be used and stored.

The act also requires receiving the subject's written consent prior to collecting biometric information. The act also requires private entities possessing biometric information to have a written policy available to the public that establishes a schedule for retaining and permanently destroying the biometric information.

For the moment, Illinois seems to be the epicenter of the facial-recognition controversy.

Illinois resident Brian Norberg alleges that Shutterfly has done none of these things. Norberg filed a putative class action against Shutterfly, a widely used electronic- and print-based photo storage and sharing service, and its wholly owned subsidiary, ThisLife LLC. Filed in federal court in June, the complaint alleges that Shutterfly and ThisLife use facial-recognition technology to identify people appearing in the 20 billion photos stored in its database using "photo-ranking algorithms" and "advanced image analysis."

According to the complaint, Norberg does not have a Shutterfly account but was identified by Shutterfly's system when a friend uploaded photos that included him.

At Shutterfly's prompting, the friend tagged Norberg's face with his name. Shutterfly then associated Norberg's "face template" with his name and stored it in its database.

The complaint asserts: "Defendants create these templates using sophisticated facial recognition technology that extracts and analyzes data from the points and contours of faces appearing in photos uploaded by their users. Each face template is unique to a particular individual, in the same way that a fingerprint or voiceprint uniquely identifies one and only one person."

Shutterfly not only collects and uses individuals' unique biometric information to identify them by name but also allegedly to identify them by gender, age, race and location.

In a Sept. 16 motion to dismiss, Shutterfly argued that the BIPA does not apply to photographs and the information derived from them. In fact, Shutterfly contends the state legislature specifically excluded photographs from the statutory language.

Facebook, another business that relies on users uploading photos, has been hit with at least four proposed class actions in five months. All of the lawsuits allege the social network giant is illegally collecting and storing users' biometric data.

Carlos Licata in April filed suit in state court, alleging that Facebook shows "a brazen disregard" for users' privacy rights and violates the BIPA by not disclosing that its tag suggestion feature uses facial-recognition software to scan uploaded photos and extract unique biometric information to identify individuals. Licata further claims Facebook launched its tag suggestion feature in 2010 and automatically enrolled users in the facial-recognition system without obtaining their informed, written consent.

Three other lawsuits asserting nearly identical claims were filed against Facebook in federal court. All four actions seek class certification and statutory damages of $5,000 for every intentional and reckless violation of the BIPA or, alternatively, statutory damages of $1,000 for every violation deemed negligent.

PRIVACY, TECHNOLOGY AND LAW

NERISSA COYLE MCGINN

Nerissa Coyle McGinn is a Chicago-based partner at Loeb & Loeb LLP. Her practice focuses on matters involving the convergence of advertising and promotions, emerging media, technology, and privacy law, as well as intellectual property law, focusing on trademark clearance and counseling. She can be reached at nmcginn@loeb.com.

Given the sheer number of users and photos involved, statutory damages for each violation could have a severe financial impact on both Facebook and Shutterfly.

No federal laws specifically regulate the use of biometric data, but the GAO and Federal Trade Commission have studied the privacy issues involved in facial recognition technology. As the statutory history of the BIPA recognizes, use of biometric data poses potentially serious privacy challenges, in large part because biometric identifiers are unlike other personal identifiers: "For example, Social Security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."

While the GAO report to Sen. Al Franken, D-Minn., the ranking member on the Senate Judiciary Committee's Subcommittee on Privacy, Technology and the Law, makes no recommendations, it recognizes that federal privacy law must adapt to address new technologies and reiterates a "2013 suggestion that Congress strengthen the current consumer privacy framework to reflect the effects of changes in technology and the marketplace."

In 2012, the Federal Trade Commission addressed the emerging privacy issues posed by facial recognition technology in its publication of "Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies." The FTC urged companies to maintain reasonable data security protections for consumers' images and biometric information collected from those images as well as appropriate retention and disposal practices of that data. The agency also recommends notifying consumers when facial-recognition technologies are used.

In particular, the FTC advised that social networks using a facial-recognition feature "should provide users with a clear notice — outside of a privacy policy — about how the feature works, what data it collects and how it will use the data." In addition, consumers should be given "(1) an easy to find, meaningful choice not to have their biometric data collected and used for facial recognition; and (2) the ability to turn off the feature at any time and delete any biometric data previously collected from their tagged photos."

Finally, the FTC recommended that facial-recognition technology should not be used to identify images of a consumer to someone who could not otherwise identify him or her, without obtaining the consumer's affirmative express consent.

For the moment, Illinois seems to be the epicenter of the facial-recognition controversy. Texas may have passed its law regulating biometric data before Illinois, but no lawsuits have yet been filed asserting violations of that law. While federal regulation of the collection and use of biometric data has been on the radar for a few years, much like other privacy issues, it does not seem to be gaining traction in Congress.

And it seems unclear whether the FTC will take its regulatory and enforcement eyes off of its efforts in the area of data security to focus on the narrower issue of biometric data.