How Should Facial-Recognition Technology Be Regulated? Part One

Part 1 of 3

With new technologies, the timeline from “that’s freaky!” to “ho-hum” is rapidly getting compressed. That’s certainly proving true of facial-recognition technology.

In the film “Minority Report,” released in 2002, Director Steven Spielberg envisioned a world (set in 2054) in which every individual would be instantly recognized (and marketed to) in public spaces, such as shopping malls. At the time, it was truly science fiction. Today, the Chinese government has embarked on a project to match faces to its database of 1.3 billion ID photos in seconds, with a target of achieving 90 percent accuracy. And many of us are routinely using Apple’s Face ID (made available in 2017 with the release of the iPhone X) to unlock our phones, or Facebook’s “tag suggestions” feature to identify our friends in photos.

The privacy concerns with facial-recognition technology are obvious: Nothing is more “personal” than one’s face. So how is the processing of facial data regulated, whether such data is collected by a government agency as in China or by a private entity like Apple or Facebook? And as facial-recognition technology use becomes more pervasive (as widely predicted), what restrictions are appropriate in the future?

In this three-part blog post, we first look at what current data protection laws have to say about the use of facial-recognition technology, with a specific focus on U.S. and EU law. We then consider the future of facial-recognition technology regulation.

US Law

U.S. law addressing facial-recognition technology is a patchwork — and a small patchwork, at that.

No federal law regulates the collection of biometric data, including facial-recognition data. At the state-law level, three states (Illinois, Washington and Texas) have passed biometric legislation, but the Washington statute doesn’t specifically encompass facial-recognition technology. The Illinois Biometric Information Privacy Act, which alone includes a private right of action, is “the gold standard for biometric privacy protection nationwide” in the view of the Electronic Frontier Foundation.

BIPA defines a “biometric identifier” to include a scan of “face geometry,” but specifically excludes photographs. An ancillary defined term under BIPA is “biometric information,” which is information “based on an individual’s biometric identifier used to identify an individual.”

Unlike the EU's data protection laws (discussed in part two), BIPA doesn't begin from a position of prohibiting the use of biometric data but rather puts guardrails around how it's used. Specifically:

Private entities collecting biometric identifiers or biometric information must have a written policy, made publicly available, that sets a retention schedule for destroying such information when the initial purpose of collection has been satisfied or within three years of the individual's last interaction with the private entity, whichever occurs first.

When an individual's biometric identifier or biometric information is first collected, the individual must: be informed that the biometric data is being collected, be told of the "purpose and length of term" of the biometric data collection, and provide a written release.

Biometric data can't be sold, and it can't be disclosed unless the individual concerned consents to the disclosure (or certain other exceptional circumstances apply – e.g., required by law).

No surprise that BIPA, with its private right of action, has been the subject of numerous lawsuits, including several focused on facial-recognition technology. Most notably on the facial-recognition technology litigation front, a class-action lawsuit against Facebook for BIPA violations regarding Facebook's "faceprint" feature is pending in the Northern District of California. Google recently managed to fend off (on standing grounds) a similar lawsuit under BIPA in the Northern District of Illinois concerning its face template application.

A pending Illinois bill (SB 3053) would provide a carve-out from BIPA for use of biometric data "exclusively for employment, human resources, fraud prevention, or security purposes," if certain safeguards are in place; but Illinois's new attorney general has announced his opposition to any weakening of the law. Meanwhile, California's sweeping new privacy law, the California Consumer Privacy Act, scheduled to become effective in January 2020, will explicitly cover biometric data.

Our next post will discuss EU law.