How Should Facial-Recognition Technology Be Regulated? Part Two

Part 2 of 3 – EU Law

In this three-part blog post, we 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.

EU Law

The former EU Data Protection Directive (Directive 95/46/EC) made no mention of biometric data. With the advent last May of the EU General Data Protection Regulation, biometric data is front and center. Under GDPR Article 9, biometric data (when used for the purpose of uniquely identifying a natural person) is among the "special categories" of personal data that is prohibited from being processed at all unless certain exceptional circumstances apply, and the definition of biometric data specifically refers to "facial images."

Like Illinois's BIPA, the GDPR makes an important distinction between facial-recognition data and photographs. Recital 51 of the GDPR states the distinction as follows: "The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person."

Although the GDPR doesn't mention video images — such as those collected by a security camera — presumably the same principle will apply. Any images collected, whether via photos or videos, will only constitute biometric data if "specific technical means" are used to uniquely identify or authenticate an individual.

If facial-recognition technology is used for purposes that fall within the GDPR's definition of biometric data, the only exception likely to be practical for many commercial applications of facial-recognition technology is where "the data subject has given explicit consent." This requirement would appear to impose a nearly insurmountable hurdle in many common facial-recognition technology use scenarios, including where facial-recognition technology is used for marketing or security purposes. Any kind of

passive consent — e.g., an individual proceeding into an environment where facial-recognition technology is active after passing prominent signs indicating that facial-recognition technology is being employed — won't pass muster under the GDPR.

Notably, however, Article 9(4) of the GDPR permits each EU member country to introduce certain derogations with respect to restrictions on processing biometric data ("member states may maintain or introduce further conditions, including limitations"). The Netherlands, for instance, has provided a carve-out for biometric data if necessary for authentication or security purposes, and Croatia's new data protection law exempts surveillance security systems. It'll be interesting to see if other EU members follow suit.

Our next post will discuss the future of facial-recognition technology regulation.