What is the Future of Facial-Recognition Technology Regulation? Part Three

Part 3 of 3

In this three-part blog post, we have looked 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 will now consider the future of facial-recognition technology regulation.

The acknowledgment that biometric data, including facial-recognition data, constitutes personal information is certainly overdue. What's still being worked out is what precautions (including notice and consent) are appropriate before facial-recognition data can be collected and used, and what exceptions may be warranted for security and fraud prevention purposes, among others.

Let's face it (pun intended): Facial-recognition technology can be used in ways that actually improve privacy and security through more accurate authentication. Imagine faster check-in and passport control at airports, as well as heightened security; speedier and more accurate patient care at hospitals; and more efficient payment confirmations, whether online or at retail establishments. Apple says that the probability a random stranger could unlock your iPhone using Face ID is one in a million — which makes it 20 times more secure than Touch ID.

So the challenge becomes: How do we encourage legitimate uses of facial-recognition technology to flourish and reap the technology's undeniable benefits, while preventing misuse and ensuring respect for privacy rights?

There would appear to be two divergent paths forward:

1. The path of strict regulation, as illustrated by the GDPR (although even the GDPR allows EU member countries some flexibility to implement derogations).
2. The more flexible path promoted by the U.S. Federal Trade Commission, as described in its October 2012 report "Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies" (an approach also endorsed in its 2015 report on the internet of things). The FTC has recommended certain best practices in deploying facial-recognition technology, including building in privacy by design, implementing reasonable security protections, and providing consumer choice on a context-sensitive basis. But the FTC stopped short of endorsing

regulation.

Or perhaps there's a middle path. Microsoft President Brad Smith recently weighed in on the facial-recognition technology debate with a provocative proposal. While Smith is an advocate of market forces, he believes that new laws are required to prevent a facial-recognition technology "commercial race to the bottom" that results in the abuse of personal data. In particular, he recommends legislation that requires transparency (including documentation explaining the capabilities and limitations of the technology), enables testing for accuracy and unfair bias, and provides appropriate notice and consent. Simultaneously, Microsoft has adopted facial-recognition technology principles concerning fairness, transparency and the like that can serve as industry best practices. Given the current stage of facial-recognition technology development, Microsoft's "incremental approach" seems eminently sensible.