WINSTON & STRAWN LLP

IN THE MEDIA

Use of Biometric Information as a Basis for Civil Liability

MAY 20, 2015

Chicago-based partner Derek Sarafa and associate Thomas Weber co-authored the article "Use of Biometric Information as a Basis for Civil Liability" published in *Law360* on May 20, 2015. The article focuses on the key components of complying with Illinois' Biometric Information Privacy Act (BIPA), damages under the Act, and the potential expansion of civil liability for the use of biometric information.

Biometric information refers to specific biological characteristics that can be used to automatically recognize a person, such as fingerprints, retina scans, and facial recognition scans. The growing use of such technology by businesses such as Apple (fingerprint authentication to unlock phone) and Facebook (the "Photo Tag Suggest" function) creates potential legal liability for any alleged misuse of that information.

However, as the article explains, there are very few state statutes and no federal statutes that create civil remedies based on the capture and disclosure of biometric data by private businesses. Therefore, enterprising plaintiffs lawyers are attempting to leverage the existing statutes to create a new sphere of liability, and Illinois' BIPA is front and center in this effort, particularly because it allows for a private right of action.

While there are no published opinions interpreting the BIPA, language in the statute suggests that potential civil liability is narrow. But on April 1, 2015, a class action was filed against Facebook in the Circuit Court of Cook County, Illinois, seeking to extend the BIPA's reach.

The article describes the four distinct categories of compliance under the BIPA that businesses should adhere to in avoidance of potential liability:

1. The collection and disclosure of biometric recognition technologies is acceptable, but certain protections must be in place, most important of which is consent from individuals.
2. Any business in possession of biometric information must have a publicly available policy establishing guidelines for retaining and ultimately destroying the biometric information in its possession.
3. A business cannot profit from an individual's biometric information.
4. Businesses in possession of biometric information must store the information by taking the same precautions that would be taken for "other confidential and sensitive information."

1 Min Read

Related Locations

Chicago

Related Topics

Law360 | Data Privacy | Consumer Privacy | Biometric Information

Related Capabilities

Privacy & Data Security | Technology, Media & Telecommunications | Professional Services

Related Professionals

Thomas Weber

© 2024 Winston & Strawn LLP.