dri™ The Voice of the Defense Bar

The Business Suit

The newsletter of the Commercial Litigation Committee

8/24/2018

Volume 22, Issue 4

The Future Is in the Palm of Your Hand and in the Details of Your Eyes, Face, and Fingerprints as Businesses Handling Biometric Data Face a New Wave of Class-Action Litigation

By Emily Knight

Biometric data is quickly gaining popularity among businesses and the public alike. Businesses are increasingly integrating biometrics into security systems, while individuals are interested now more than ever in the handling of their biometric information, especially after California's law enforcement recently used DNA and genealogical tracing to identify and arrest the Golden State Killer. But, as more states begin to regulate the collection and handling of this ultra-personal data, businesses may find themselves exposed to new forms of liability. Given the evolving regulatory landscape surrounding biometric data, companies incorporating this new technology should proceed with prudence to protect themselves from future litigation.

What Is Biometric Data and Why Use It?

Biometric identifiers are the distinctive, measureable characteristics used to recognize an individual—*i.e.* DNA, fingerprints, voiceprints, and iris or retina scans. Biometric data is the information derived from these identifiers, usually reduced to algorithms or equations, and is the information a business digitally stores and uses. Businesses favor biometric data for security purposes because of its increased reliability, efficiency, and security. But unlike knowledge-based, personal information (social security numbers, passwords, etc.), biometric data cannot be replaced. As a result, the collection and use of this data may be far more damaging once compromised.

The Current Regulatory Landscape

Illinois, Texas, Washington, and Colorado have all enacted biometric data statutes. Illinois's Biometric Information Privacy Act ("BIPA") is the most onerous and, therefore, has been the focus of recent litigation.

Brief Overview of the BIPA

The BIPA generally protects any information based on an individual's biometric identifier and is used to identify a person. Under the BIPA, private companies collecting this type of data:

- Must provide notice and obtain consent prior to collecting biometric identifiers. The notice must be written, explain the purpose for collection, and identify the retention period;
- Must implement a written retention policy;
- Cannot sell or profit from an individual's biometric data;
- Cannot disclose data to a third party unless an enumerated exception applies; and
- Must protect biometric data in at least the same manner it protects other sensitive and confidential information.

A business's failure to adhere to these standards may subject it to a private cause of action, with recovery of statutory damages and attorney's fees. For negligent violations, plaintiffs may receive the greater of $1,000 or actual damages for each violation. For intentional or reckless violations, plaintiffs may receive the greater of $5,000 or actual damages for each violation. The BIPA is currently the only statute that creates a private cause of action for violations. The Texas, Washington, and Colorado statutes are enforced by the state attorney general.

Currently, no federal law regulating biometric data exists. However, the FTC maintains broad authority to initiate an unfair or deceptive trade practice action if a company promises a certain level of security but fails to keep this promise. Businesses should also keep in mind the EU's General Data Protection Regulation (GDPR), which broadly

prohibits processing biometric data of any EU citizen unless it fits into one of the GDPR's explicitly enumerated bases.

The First Wave of Class-Action Litigation

In the first wave of BIPA class-action litigation, two types of fact patterns have emerged: (1) improper use of facial recognition technology (*i.e.*, social media); and (2) improper collection and use of fingerprints, primarily in the employment context. In both instances, plaintiffs are alleging that the company failed to provide proper notice and/or obtain consent before collecting their biometric identifiers. In other words, plaintiffs are relying on technical violations. But before addressing the validity of these claims, courts have been forced to wrestle with the issue of standing.

Standing Under BIPA

Under the BIPA, only a "person aggrieved" can initiate an action. Companies defending these claims are frequently challenging class standing on the grounds that a cognizable injury does not exist. Yet, the courts' willingness to accept this challenge has been mixed. *See McCollough v. Smarte Carte, Inc.*, No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016) (dismissing the case because plaintiff failed to satisfy standing requirements); *But see Patel v. Facebook Inc.*, 290 F. Supp. 3d 948 (N.D. Cal. 2018) (explaining that a violation of the BIPA's notice and consent procedures infringe upon the very privacy rights the legislature sought to protect by enacting the statute).

Steps Businesses Can Take Now to Avoid Liability Later

As biometric data gains popularity, it is almost certain that more states will enact legislation; therefore, companies should begin updating their data security policies and procedures now to avoid headaches later.

Businesses that intend to collect and use biometric data should always provide written notice and obtain informed consent. The notice should explain the purpose of collecting, how the data will be used, the company's retention policy, and whether any outside vendors will have access to it. Since almost all biometric data actions right now hinge on notice and consent, it is vital that businesses sufficiently address this step. Companies must also protect biometric data at least in the same manner as other confidential information. This means encryption, limited access, and retention and disposal policies. Additionally, such safeguards will help to protect against liability when a breach occurs, even in the absence of a state statute. In these instances, many states will default to a common law standard of reasonableness.

Despite the recent uptick in class-action litigation, commercial use of biometric data is not going anywhere any time soon. As of now, this area of law remains largely untouched. But a prudent business will begin addressing its biometric data privacy policies and procedures now to avoid potential exposure to class-action litigation later.

Emily Knight is an associate in the Trial Department at Tucker Ellis LLP, practicing in the Cleveland office. She can be reached at 216.696.4893 or emily.knight@tuckerellis.com.