CLIENT ALERTS & INSIGHTS

Biometrics: The Wave of the Future Sparks a Current Wave of Class Action Litigation

OCTOBER 6, 2017

Authors: Mark S. Eisen

Brought about by an obscure state law passed nearly a decade ago-the Illinois Biometric Information Protection Act (740 ILCS 14/1)-the next wave of privacy class action litigation is here and in full-swing. While an Illinois law, the BIPA is appearing in cases nationwide regarding the collection, storage and use of biometric information. The BIPA, in short, regulates the collection and use of biometric information (*i.e.,* iris scans, fingerprints, voiceprints and facial geometry). The BIPA was enacted in 2008, and flew largely under the radar until an initial trickling of class actions, beginning with the first class action filed against Facebook in 2015, and followed shortly thereafter by lawsuits against Google, Shutterfly and Snapchat.

Over the last year, this initial trickling has turned into a flash flood. Plaintiffs' attorneys' emphasis has moved from tech companies to the everyday workplace. This year alone, over two dozen BIPA class actions have been filed by former employees against their employers over the use of fingerprint scanning as a means of clocking in and out. Where there were once time cards, employers are turning to fingerprint scanning for a number of reasons (efficiency, expediency, accuracy, avoidance of fraud, etc.). Plaintiffs' attorneys, however, are scanning the State of Illinois for this practice and filing suit in droves.

Like many privacy statutes, the BIPA provides for highly detailed, discrete requirements and potentially ruinous statutory damages for even the most hyper-technical violation. Under the BIPA, entities possessing or collecting biometric data must:

- Develop a written policy, available to the public, establishing a retention schedule and guidelines for destruction;
- Destroy biometric data when the initial purpose for obtaining/collecting such data has been fulfilled, or within three years of the person's last interaction with the entity, whichever is sooner;
- Obtain prior express written consent prior to the collection or receipt of biometric data based on a disclosure to the individual that biometric data is being collected and the length of time for which the data is collected;
- Store biometric information using a reasonable standard of care for the entity's industry, and in a manner that is the same or exceeds the standards used to protect other confidential information.

The BIPA likewise heavily regulates the sale and disclosure of biometric data. A violation of any one of the BIPA's intricate requirements could result in the imposition of statutory damages ranging from **$1,000 to $5,000** per violation.

Given the statutory damages at issue-and the numerous hyper-technical statutory provisions-it is easy to see why this statute has been viewed predominantly as a boon to the plaintiffs' bar. Indeed, each of the recently-filed BIPA cases shares a similar and very simple refrain: (i) Plaintiff used to work for Defendant; (ii) Defendant uses a fingerprint scanner to clock employees in and out; and (iii) Plaintiff was not provided a disclosure regarding the use/storage of her biometric information. Conspicuously absent are any allegations of ***actual damages*** (*i.e.*, identity theft) or the even the potential for actual damages. Plaintiffs are proceeding on the basis of statutory damages alone.

These lawsuits are simply the next in a long line of opportunistic pseudo-privacy class actions, following the well-worn footpath of statutes like the Telephone Consumer Protection Act and Fair Credit Reporting Act. Like TCPA and FCRA cases, plaintiffs' lawyers are undoubtedly on the hunt for cases to file. It is thus crucial to ensure, prior to the implementation of any form of biometric-based clocking procedure (or even the use of biometrics to access secure/confidential information), that proper employee-consent has been obtained. To the extent biometric information is already obtained/being used, it is essential to take steps to curtail the risk of possible lawsuits *(i.e.,* obtaining retroactive releases of possible claims and/or implementing proper disclosures and written consent procedures). With cases being filed every day, employers must be proactive here; this is not a problem that is likely to go away on its own.

Finally, it is important to keep in mind that there are defenses available to these cases. Whether BIPA cases (which require a plaintiff be "aggrieved by" a violation) can be pursued in the absence of actual damages is an issue of intense debate before federal and state courts. Further, whether arbitration clauses in the employment context (an issue currently before the Supreme Court) will enable employers to avoid BIPA class actions will soon be known. Constitutional challenges are likewise being levied against the BIPA, as employers operating in multiple states challenge the validity of an Illinois statute that effectively forces companies to change their conduct nationwide.

Although there are defenses, litigation is, by its nature, expensive and uncertain; companies are well-advised to audit their privacy practices and-if they are collecting biometric information-consider whether their practices are BIPA-compliant.

For more information about this topic, please contact:

David Almeida at dalmeida@beneschlaw.com or 312.212.4954
Partner
Chair, Class Actions Practice Group
Chair, Retail, Hospitality & Consumer Package Goods Industry Team

Mark E. Eisen at meisen@beneschlaw.com or 312.212.4956
Associate
Litigation Practice Group
Retail, Hospitality & Consumer Package Goods Industry Team

Courtney C. Booth at cbooth@beneschlaw.com or 312.212.4946
Associate
Litigation Practice Group
Retail, Hospitality & Consumer Package Goods Industry Team