Legal Backgrounder

Vol. 34 No. 4 April 5, 2019

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

The Coming Litigation Tsunami?: Why Private-Right-of-Action Enforcement Undermines Privacy and Data Security

by Al Saikali

What impact would a private right of action have if it were included in a federal data-privacy law? This question is being asked as Congress considers such a law. Thus far, Congress has not included private rights of action in federal privacy laws like the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act. A private right of action in the context of a data-privacy law appears to benefit plaintiffs' lawyers the most, imposes a significant burden on judicial resources, and creates a disincentive for companies to be more forthcoming about privacy incidents, which is antithetical to the purpose of these laws and harmful to consumers.

BIPA—A Case Study

The Illinois Biometric Information Privacy Act (BIPA) is perhaps the most prominent example of an existing privacy law that contains a private right of action. The law, which went into effect over ten years ago, requires companies that collect biometric information (*e.g.*, fingerprints, facial scans, hand scans, and retinal scans) to first provide notice and obtain a written release from the data subjects. BIPA also prohibits companies from sharing biometric information with third parties without first obtaining the data subject's consent. Security safeguards must also be implemented in an effort to protect the biometric information. Most pertinent to this article, individuals who are "aggrieved by" a violation of the law are entitled to sue for an amount of $1,000 to $5,000 per violation depending on the level of negligence or intentional misconduct involved.

BIPA's adoption was motivated by fear that biometric information, which cannot be replaced if stolen, might be compromised and misused in some way. The fear never became a reality. Since late 2017, however, over 200 class-action lawsuits have been filed against companies whose employees punch in and out of work using a finger scan. The lawsuits contend that the defendants never gave employees notice that their biometric information was being collected, nor were they asked to sign a release as required by BIPA. Companies that employ as few as 1,000 people are now facing a minimum of $1,000,000 in liability under these lawsuits.

Finger scanning technology minimizes fraudulent conduct known as "buddy punching." The technology does not collect a library of the users' fingerprints. Instead, it measures ridges or minutiae points on the individual's finger, applies a mathematical algorithm to the measurements, creates a numerical representation of the fingerprint (which cannot be reverse-engineered to create a fingerprint), and that representation is then encrypted.

Al Saikali is a Partner in the Miami office of Shook, Hardy & Bacon, LLP, where he chairs the Privacy and Data Security Practice. Shook, Hardy & Bacon, LLP represents more companies in BIPA class action lawsuits than any other defense firm in the country.

Imagine opening a door to a safe and finding another safe, which you then open to find a piece of paper with letters and numbers on it, which can't be used to do anything useful. This fingerprint technology is the most secure form of authentication available to companies seeking to minimize fraud while protecting their workers' sensitive information. None of the 200 BIPA class action lawsuits allege that the plaintiff's information was actually breached, compromised, or otherwise misused.

In their defense, the companies argued that BIPA's "aggrieved by" requirement demands more than a technical violation of the law; plaintiffs had to demonstrate actual harm. In January, the Illinois Supreme Court held in *Rosenbach v. Six Flags* that a mere lack of notice and failure to obtain a release was, alone, enough to meet the "aggrieved by" requirement under BIPA.

Emboldened by *Rosenbach*, the plaintiffs' bar is now filing between three and five new lawsuits a day. They have also moved to a new strategy: arguing that a BIPA violation occurs every time their client placed their finger on the scanner to punch in/out of work. So, for example, a single employee could punch in/out of work over 500 times per year (maybe hundreds more times if you count punching in and out for rest breaks). Multiply the 500 by the number of years that employee is with the company. Multiply that by the number of provisions of BIPA that were allegedly violated (*e.g.*, failure to give notice, failure to get a release, failure to adopt security safeguards, and storing information with a cloud service provider). Multiply that by the number of employees affected. Then multiply all of that by 1,000. That's the minimum amount of damages plaintiffs are seeking in each of these lawsuits. It totals hundreds of millions, or billions, of dollars.

The sheer number of lawsuits essentially guarantees that we will see conflicting decisions by Illinois courts on various issues as they address the merits of BIPA claims. These mixed results will only increase the lifecycle of the litigation and the costs to businesses (and their insurers) defending it.

Who Will Follow Illinois on Biometrics?

Not surprisingly, given the plaintiffs' bar's success with BIPA in Illinois, two other states, Florida and New York, are now considering similar versions of BIPA enforceable by private rights of action. The Florida bill is unlikely to become law because of the political composition of the legislative and executive branches, but the future of the New York law is less certain.

At the federal level, Congress may take a more measured approach. It is considering a biometric privacy law, supported by some affected companies, that does not contain a private right of action. The Commercial Facial Recognition Privacy Act would, among other things, prohibit certain entities from using facial recognition technology to identify or track an end user without obtaining the affirmative consent of the end user. That law, like HIPAA, would be enforced by the Federal Trade Commission and state Attorneys General, but it does not create a private right of action. Nor does it preempt private rights of action under state laws like the Illinois BIPA.

What's The Next Wave of Privacy Litigation?

A privacy class action tsunami even larger than the Illinois BIPA tidal wave is looming in the distance under the California Consumer Privacy Act (CCPA). The CCPA, which goes into effect next year, creates certain privacy rights for California residents (*e.g.*, right to know about how their personal information is collected and sold, right to opt out of the sale of their information, right to delete personal information, and a right to obtain a copy of information a business collects about them).

More relevant for the purpose of this article, the CCPA creates a private right of action for California residents if their unencrypted personal information is subject to an unauthorized access and exfiltration, theft,

or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. In other words, a California resident need only show that a data breach affected their information *and* that the breach was a result of the company's failure to implement and maintain reasonable security procedures and practices. The CCPA entitles plaintiffs who meet these requirements to recover damages between $100 and $750 per consumer per incident, or actual damages, whichever is greater.

The law contains a "right to cure" pursuant to which a consumer, before initiating their lawsuit, must provide the business 30 days written notice identifying the specific provisions of the CCPA the consumer alleges have been or are being violated. In the event a cure is possible, and if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business.

CCPA supporters have argued that the CCPA will not increase litigation significantly because the law does not create a private right of action for *all* breaches, only those that were a result of the company's failure to implement and maintain reasonable security procedures and practices. Such a requirement is meaningless, however, because a plaintiff will simply allege the lack of procedures and practices, creating an issue of fact that will require a company to stay in the litigation until the trier of fact makes an ultimate determination. Plaintiffs' lawyers will simply find expert witnesses who will testify that one of the reasons why the company suffered a data breach was the lack of a specific administrative, technical, or physical safeguard.

CCPA supporters also argue that the law's right to cure provision will prevent many class action lawsuits from being filed. This is highly unlikely. The right to cure is meaningless in the data-breach context. If a company suffers a breach that impacts an individual's personal information, it is almost impossible to put that cat back in the proverbial bag. California is now considering an amendment to the CCPA what would broaden the private right of action to apply to *any* violation of the law (including the privacy protections), not just data breaches.

If it is still unclear how the CCPA could lead to an enormous amount of litigation against companies doing business in California, imagine the following scenario. A company collects a significant amount of personal information from tens of thousands of customers and employees in California. It spends millions of dollars adopting safeguards to build its cyber defense, but as any information security expert will tell you, safe haven from a cyber attack cannot be guaranteed. A hacker then uses zero-day malware (malware for which no safeguard has yet been designed to protect against) to attack the company. Let's make the scenario even simpler—an employee mistakenly sends a file containing the personal information of thousands of individuals to the wrong recipient and is unable to retract the email or contact the recipient.

In both of those situations, most companies would provide notice to the affected individuals. Once the CCPA goes into effect, those companies could face tens of millions of dollars in liability from class action lawsuits. As a result, those companies will face two options: (1) provide notice and almost assuredly be hit with a class action seeking tens of millions of dollars; or (2) say nothing about the incident and hope that nobody finds out about it. You see where this dilemma leads a company—they will be *less* likely to provide notice of a data breach as a result of the CCPA. This result, which hurts California residents, is the complete opposite of what the CCPA was intended to do.

Think, as well, of the impact to insurance companies whose cyber coverage might have otherwise applied in that scenario. What impact will the potentially massive liability have on coverage for data breaches? One possibility is that the cost of cyber-liability coverage will skyrocket for everyone, so only

ISBN 1056 3059

the largest companies will be able to afford it. Another possibility is that large exclusions will be written, making the coverage meaningless. A third possibility is that insurers will not offer cyber-liability coverage to companies doing business in California. How are any of these outcomes good for Californians?

Be Prepared for a New Cottage Industry

With these new privacy laws, we can expect a cottage industry of professional plaintiffs to test whether companies are in compliance. A similar phenomenon is taking place in the European Union with respect to the General Data Protection Regulation. Professional plaintiffs will know before they make the request for their information what information the company has about them. They'll simply want to test whether they receive back everything they know the company has. If they don't, a civil lawsuit (perhaps even a class action) will be filed.

Is the Risk of Class Actions Really that Significant?

A common argument made by the plaintiffs' bar is that companies already face class action lawsuits for data breaches. Companies have in fact been hit with class action lawsuits based on common-law theories of liability such as negligence, breach of implied contract, or even fraud, and statutory theories of liability like violations of state consumer protection laws. Those lawsuits, however, require plaintiffs to demonstrate some actual harm in order to establish standing to sue. This can be difficult because the individuals rarely suffer any financial harm as a result of the breaches, and to the extent they do and can demonstrate it was a result of the subject incident, they are typically reimbursed (*e.g.*, fraudulent charges on credit cards).

While some courts have lowered the bar for plaintiffs' showing of actual harm to include a mere risk of harm, businesses still have a fighting chance when moving to dismiss data-breach suits for lack of standing. According to plaintiffs, however, a private right of action to pursue statutory damages would significantly improve their odds of overcoming what has been the highest obstacle to their recovery in privacy and data-security litigation (the need to demonstrate actual harm as a result of an incident).

A Path Forward

A new privacy law making its way through the Washington legislature (Senate Bill 5376) may be a middle ground for the path forward. That law provides many of the same privacy rights as California and Massachusetts (which is considering a law similar to California's). Unlike California and Massachusetts, however, the law does not create a private right of action. Instead, it would be enforced by the state attorney general.

To be sure, this is not a perfect solution. State attorneys general are limited by their resources and will have to prioritize which cases to enforce, but strong enforcement in a limited number of cases will send a message that compliance is a serious matter. The alternative, a private right of action, would lead to abuse by the plaintiffs' bar and even create incentives that are contrary to the purposes of the laws themselves.

As Congress considers a national data-privacy law, businesses should pay close attention to whether the law will include a private right of action, and whether the law will preempt existing state privacy laws that already provide a private right of action. The cost of implementing systems and processes to comply with data-privacy laws is significant. If Congress were to add a bonanza for the plaintiffs' bar, the impact on U.S. companies and judicial systems would be enormous.

  ISBN 1056 3059