Legal Matters®

Business
spring 2019

Landmark decision allows suits against companies for collecting biometric data

In a ruling that's expected to have widespread implications, the Illinois Supreme Court has held that consumers can sue companies for collecting biometric data, including facial scans or fingerprints, if the companies fail to disclose how the information will be used.

The court unanimously said companies that gather people's data improperly could be held liable for damages, even without concrete injury to the consumers.

The ruling paves the way for lawsuits against Facebook, Google and other businesses that have been fighting challenges on this and related issues.

In the Illinois case, a teenager's fingerprints were collected in 2014 when he bought a pass for a Six Flags amusement park. His family sued Six Flags, claiming that the collection without their consent violated a state law called the Biometric Information Privacy Act (BIPA).

BIPA is known as the strictest biometric data law in the country. It requires companies to obtain a written release, from either the person whose data is collected or their legally authorized representative, and to provide a written explanation detailing the reason for collecting it and the length of time it will be stored.

The Illinois law allows individuals to sue for damages of $1,000, or up to $5,000 if a court rules that the violation of the law was deliberate or reckless.

Other state privacy laws typically only allow attorneys general to sue companies.

©SergeyNivens

Six Flags argued that because the family didn't have evidence that taking their son's fingerprints caused any harm to him, it shouldn't pay damages.

The court disagreed, saying that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act" in order to sue.

As a result, the court said the family could sue Six Flags. Ultimately, the

continued on page 3

ALLRED, BACON, HALFHILL & YOUNG, PC

11350 Random Hills Road, Suite 700 | Fairfax, VA 22030
(703) 352-1300 | admin@abhylaw.com | www.abhylaw.com

OSHA revises electronic recordkeeping rule; Labor groups file suit

The Occupational Safety and Health Administration (OSHA) has eliminated the requirement that employers electronically submit Forms 300 (Log of Work-Related Injuries and Illnesses) and 301 (Injury and Illness Incident Report).

OSHA published the revised rules in the Federal Register at the end of January.

The rule still requires certain employers to submit Form 300A electronically every year. This requirement applies to (1) establishments with 250 or more employees; and (2) establishments with 20 to 249 employees in certain designated industries. Those employers must also submit their Employer Identification Numbers.

Employers that are required to submit a Form 300A for 2018 must do so electronically by March 2, 2019.

OSHA said that this rule change was necessary to protect the privacy of workers by preventing "routine government collection of information that may be quite sensitive, including descriptions of workers' injuries and the body parts affected, and thereby avoid … the risk that such information might be publicly disclosed under the Freedom of Information Act (FOIA) or through the Injury Tracking Application."

OSHA also commented that the benefit of collecting data from Forms 300 and 301 is uncertain. The agency said it was not able to ensure that personal identifying information would be redacted from employer injury data due to the amount of data it would receive. OSHA said that although it could use software to remove the personal identifying information, such technology isn't completely effective.

For years, the debate over illness and injury report-

continued on page 3

Legal pitfalls of crowdfunding campaigns

You have the next big idea and need some cash to make it happen.

©AndreyPopov

Crowdfunding campaigns, such as Kickstarter and IndieGogGo, can be effective ways to get a boost, offering contributors a reward in exchange for a financial contribution to the future of your business.

Before you jump in, it's important to be aware that these campaigns aren't without risk.

The first thing to pay attention to is the language you use to explain and present your product or project.

When you make an agreement to receive funding in exchange for a reward to your supporters, it amounts to a contract. That means you need to be clear about what you are, and aren't, going to provide.

You must make good on whatever you've promised. If you agree to give them a product and don't deliver it, or don't deliver it at the quality you promised, you could be on the hook for a breach of contract claim. An individual can bring a claim, or it could become a class action on behalf of many or all of your backers.

On many crowdfunding sites, the terms of service state that you must return any money raised if you don't deliver whatever you promised.

One of the best ways to protect yourself is to communicate regularly with your donors, informing them about the status of the campaign and the delivery of the product.

Another way to protect yourself is to form an LLC or other corporate entity. These business arrangements protect your personal assets if you ever had to pay a legal judgment against you.

Crowdfunding sites typically have provisions to protect themselves from liability, but do not protect the entrepreneur using their service.

In addition to breach of contract claims, your campaign can open you up to consumer protection or fraud claims if you don't deliver what you promise. Government agencies can also sue to enforce such laws.

Protect yourself by looking at your description as if you were a potential funder, and make sure what you are promising is clear.

For most typical, rewards-based crowdfunding campaigns, you should state clearly in your description that your supporters will not obtain any equity in your company or any share of your profits. To be safe, you should be sure that the words "invest," "investor," and "investment" do not appear anywhere.

Also, remember that any income from your crowdfunding campaign is taxable. It can get complicated if the related expenses will be incurred in future years or if you need to capitalize the expenses.

A business attorney can help you minimize your risk and help prepare you for a legally sound crowdfunding campaign.

Landmark decision allows suits against companies for collecting biometric data

continued from page 1

court found that Six Flags had violated the Illinois law and would have to pay damages to the family.

Facial recognition under attack

In addition to penalizing Six Flags, the ruling shoots down an argument that's been made by other corporate defendants, including Facebook and Google.

For example, a class action lawsuit pending against Facebook alleges violations of the Illinois law due to the platform's use of facial recognition to tag photos. If Facebook loses the case, the fines could total billions of dollars.

In a case filed against Google, the plaintiffs claim that the company didn't obtain users' consent to use facial recognition technology in Google Photos.

Numerous other cases currently are pending under the same Illinois law. Both Texas and Washington State also have laws that regulate facial recognition.

If you're a business outside of Illinois, could this case affect you? At the moment, it's unclear how widespread the effect will be. The federal appeals courts are split on the question of whether consumers can sue companies after a data breach without proving concrete harm, and the U.S. Supreme Court has refused to decide the issue.

©SergeyNivens

In the federal cases, the focus has been on whether a data breach amounts to a sufficient risk of future harm to allow a plaintiff to sue.

One federal appeals court addressed this question under the BIPA law in 2017 and decided there was no injury. However, the Illinois Supreme Court avoided this question in the current case, instead saying that a straight violation of the law was enough.

Regardless of your location, the decision demonstrates how important it is to speak with a business attorney to ensure that your company is making proper disclosures to consumers if you collect biometric data.

OSHA revises electronic recordkeeping rule; Labor groups file suit

continued from page 2

ing has continued among employers, unions, the administration and OSHA.

Prior to 2017, OSHA required employers to maintain detailed illness and injury logs, but they didn't have to submit them annually. At that time, the only immediate reports required were those that involved serious injuries and death. For example, a third-degree burn that led to emergency treatment would not be included under the guidelines.

Then, the Obama administration issued its final electronic reporting rule in 2016, mandating that employers send detailed reports annually, beginning in 2017. Unions had been pushing for years for these requirements.

Soon after, a group of manufacturing, steel and construction companies filed suit again the Department of Labor, arguing that the rule was "arbitrary" and "capricious." That lawsuit is still pending in federal court in Texas.

The White House Office of Management and Budget (OMB) pushed the latest rule change through quickly during the government shutdown, taking six weeks to go through the process instead of the usual three months. The timing came as a surprise to both union leaders and public health researchers.

After hearing that the rule was moving through quickly, a group of unions requested a meeting with the OMB, which is responsible for reviewing regulations prior to publishing them, to discuss the rule before it was finalized. The unions, which have been fighting for increased reporting for years, allegedly never received a reply.

As soon as the rule was finalized, a group of public health organizations filed suit against the Labor Department, claiming that the rule violates the federal Administrative Procedure Act, which regulates the rule-making process.

The suit argues that OSHA didn't properly explain the reason for the change and didn't sufficiently consider the flood of comments that opposed the change.

One of the plaintiffs in the case, the nonprofit Public Citizen, is seeking more detailed injury reporting to help prevent work-related injuries and death.

We welcome your referrals.

We value all of our clients. While we are a busy firm, we welcome your referrals. We promise to provide first-class service to anyone that you refer to our firm. If you have already referred clients to our firm, thank you!

ALLRED, BACON,
HALFHILL & YOUNG, PC
11350 Random Hills Road, Suite 700 | Fairfax, VA 22030
(703) 352-1300 | admin@abhylaw.com | www.abhylaw.com


©welcomia

Report: Companies must be prepared for cybersecurity regulations

A new report indicates that companies need to prepare for a flood of cybersecurity regulations nationwide.

The 2019 Compliance Landscape Report by Edgile, a cyber risk and regulatory compliance partner to Fortune 500 companies, reviewed state bills, resolutions and laws across the country.

The report states that in 2018, at least 35 states reviewed more than 265 cybersecurity-related bills and resolutions. Fifty of them became law. This trend is expected to gain momentum as states address privacy risks and global rules that affect business, such as the European Union's GDPR privacy rules.

These are just a few examples of laws that went into effect in 2018:

• **California:** The state passed the first "Internet of Things" law, requiring the manufacturer of a "connected device" to "equip the device with a reasonable security feature or features designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure."

• **Ohio:** Ohio passed a law that gives businesses a legal incentive to adopt and maintain written cybersecurity programs. It's the first state law of this kind.

• **South Carolina:** The state passed the first insurance cybersecurity law under the NAIC Insurance Data Security Model Law. The law requires insurers, agents and other licensed entities to maintain an information security program based on ongoing risk assessment, oversee third-party service providers, investigate data breaches, and notify authorities of such breaches.

• **Vermont:** The state was the first to pass a data broker law, requiring businesses defined as "data brokers" to register annually with the secretary of state, notify authorities of security breaches, and adhere to standard security measures when dealing with personally identifiable information. A "data broker" is defined as a business that knowingly collects and sells or licenses to third parties the personal information of a consumer with whom that business doesn't have a direct relationship.

Consult a business attorney in your state to learn about what regulations apply to your company.