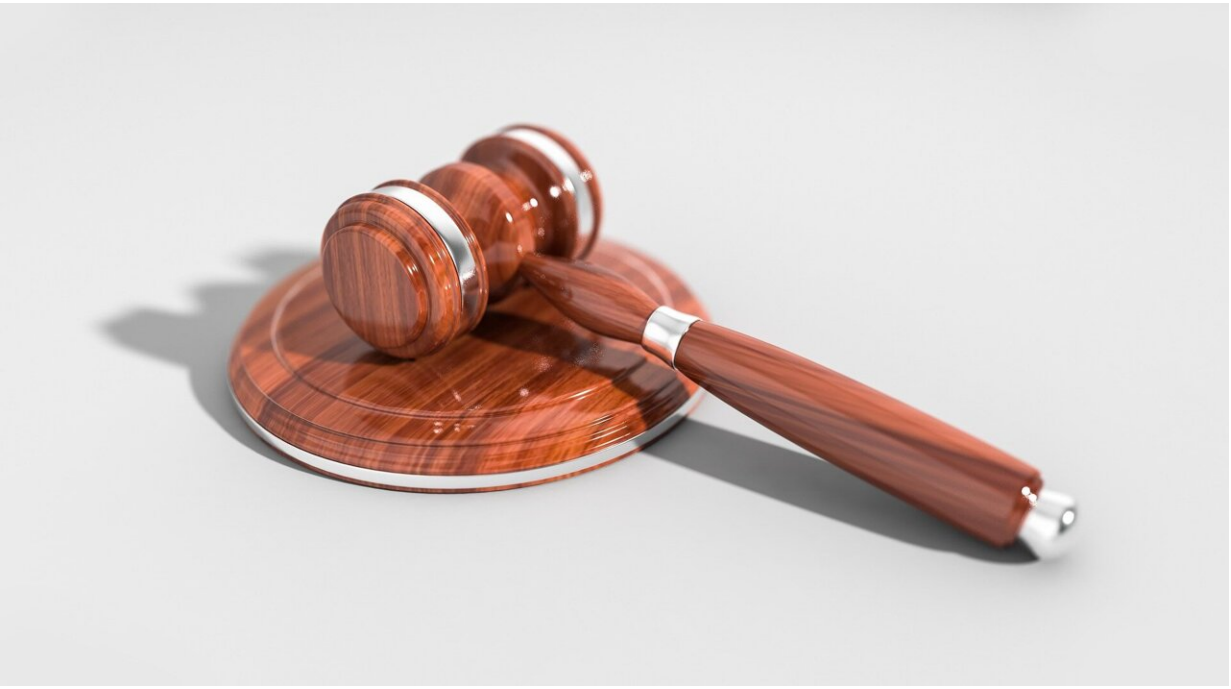
Illinois Supreme Court allows massive damages in biometric privacy cases but says lawmakers should weigh in

February 21 2023, by Talia Soglin



Credit: Pixabay/CC0 Public Domain

The Illinois Supreme Court issued a much-anticipated opinion on the state's biometric privacy law Friday, leaving the door open for massive damages when companies are found to violate residents' privacy rights but suggesting lawmakers revisit the issue.

The case involves Ohio-based fast-food company White Castle. Latrina Cothron, a Chicago-based White Castle manager, alleged she was required to use a fingerprint scan in order to access her paystubs at White Castle without prior consent in violation of the law.

Privacy attorneys and experts have closely watched for the Supreme Court's decision in the Cothron case because of the potential for a ruling that could allow damages to accrue each and every time Cothron and other White Castle employees scanned their fingerprints over the course of their employment.

On Friday, the Supreme Court ruled biometric privacy claims accrue under state law every time a person provides their biometric information without prior informed consent. The court acknowledged this interpretation of the law could leave the door open to massive damages—in White Castle's case, more than $17 billion, but said "the statutory language clearly supports plaintiff's position."

But the court also suggested damages should not be so large as to bankrupt businesses, as White Castle has argued could occur.

In a split opinion, the majority wrote Friday that while the legislature did intend to use "substantial potential liability" to protect residents' biometric information, "there is no language in the Act suggesting legislative intent to authorize a damages award that would result in the financial destruction of a business."

"Ultimately, however, we continue to believe that policy-based concerns about potentially excessive damage awards under the Act are best addressed by the legislature," Justice Elizabeth Rochford wrote in the opinion, which was joined by Justices P. Scott Neville, Joy Cunningham and Mary O'Brien. "We respectfully suggest that the legislature review these policy concerns and make clear its intent regarding the assessment

of damages under the Act."

In a statement, White Castle said it was "deeply disappointed with the court's decision and the significant business disruption that will be caused to Illinois businesses, which now face potentially huge damages."

The company said it was reviewing its options for further judicial review, pointing to the dissent in the ruling. White Castle did not answer questions about its current biometric privacy practices in the workplace.

James Zouras, an attorney for Cothron, said in a statement he was "extremely gratified" by the ruling.

"Hopefully, today's decision will encourage employers and other biometric data collectors to finally start taking the law seriously and ensure such biometric data is properly safeguarded," Zouras said.

Illinois' biometric privacy law is considered the strictest in the U.S., in part because it allows individuals to sue companies over alleged violations. It requires consent before companies can collect and store biometric data, such as fingerprints or retina scans.

Since its passage in 2008, the Biometric Information Privacy Act has sparked upward of 1,600 lawsuits in state and federal courts, White Castle's attorneys said in their Supreme Court brief. Recently, a number of big tech companies have agreed to settle biometric privacy cases for millions of dollars, though companies generally don't admit wrongdoing in those settlements.

Google and Snapchat parent Snap Inc. both reached class-action settlements in biometric privacy lawsuits in Illinois last year, agreeing to pay out $100 million and $35 million, respectively. Also last year, Facebook paid out a $650 million settlement involving its facial tagging

feature.

Under the law, plaintiffs can be awarded $1,000 for violations deemed negligent and $5,000 for "intentional" or "reckless" violations.

Individual payouts in high-profile biometric privacy settlements have been much lower—Facebook doled out checks of $397 per person, for instance—but they are still higher than amounts in other types of consumer settlements because of the potential for high damages.

On Friday, privacy law experts offered varied opinions as to whether the Supreme Court's ruling will significantly affect the size of biometric privacy settlements. Many such cases had been stayed pending a ruling in the White Castle case.

Lior Strahilevitz, a professor at the University of Chicago Law School, said he expected the size of damages and settlements in biometric privacy cases to increase as a result of the opinion.

"Plaintiffs and people who've had their biometric information used without authorizing it are in a much stronger position today than they were yesterday," Strahilevitz said.

Matthew Kugler, a professor at Northwestern University's Pritzker School of Law, said the language in the opinion nevertheless sends a clear signal to lower courts that companies should not be required to pay exponential damages for each and every scan or data transmission.

"The court was trying to preserve the status quo," Kugler said. "We will continue to see large damages awards, but the court is signaling to the lower courts that those awards should not be larger than they were previously."

Three justices dissented from Friday's ruling, arguing that a claim under the biometric privacy law accrues only upon the first scan or transmission of biometric data.

"There is only one loss of control or privacy, and this happens when the information is first obtained," Justice David Overstreet wrote in the dissent, adding that the majority's ruling could lead to "annihilative liability" for companies.

"Imposing punitive, crippling liability on businesses could not have been a goal of the Act," said the dissent, which was joined by Justices Mary Jane Theis and Lisa Holder White.

Jody Kahn Mason, an attorney in the Chicago office of law firm Jackson Lewis, which represents employers in biometric privacy litigation, said it is too early to tell how the Cothron ruling will affect the size of privacy settlements. But all members of the court, she said, seemed to support the idea that privacy litigation should not put companies out of business.

"They were clearly grappling with this issue," she said. "Both the majority opinion and the dissent affirm and say, damages should not be ruinous and they should be discretionary."

Jackson Lewis did not represent parties in the White Castle case but submitted an amicus brief on behalf of trade organizations.

A number of major business groups signed onto amicus briefs in support of White Castle, including the National Retail Federation, the Chicagoland Chamber of Commerce, the Illinois Chamber of Commerce and the U.S. Chamber of Commerce.

Many companies staunchly oppose the Biometric Information Privacy Act, which could make it difficult for lawmakers to amend despite the

Supreme Court's suggestion that they clarify questions around damages, Kugler said.

"Given that many companies would like to burn it to the ground, it's hard to do only a tweak," Kugler said.

Strahilevitz said change could also be inhibited for another reason: biometric privacy litigation has generated lots of cash for plaintiffs' attorneys in Illinois, a group that happens to be "a very important constituency for fundraising for Democratic politicians."

"It's possible that the business community prevails in Springfield," by limiting the damages plaintiffs are entitled to under the law, Strahilevitz said, "but I wouldn't expect to see it."

It's also difficult to say whether the legislature intended to allow for such damages, Strahilevitz said. At the time the law was written, he said, legislators had a limited understanding of how far modern usage of biometric data could go and were not likely contemplating the possibility of judgments in the billions of dollars.

"It's kind of like asking what the Founding Fathers would have thought about NASA," Strahilevitz said.

The Illinois Supreme Court has previously issued plaintiff-friendly rulings interpreting the law.

In 2019, the court upheld citizens' rights to sue companies for collecting their biometric data, including fingerprint scans, in a case against Six Flags. And earlier this month, the court issued another plaintiff-friendly ruling in a case involving logistics company Black Horse Carriers. In that case, Tims v. Black Horse Carriers, the court upheld a five-year statute of limitations for claims, rather than a narrower one-year time period.

The Cothron lawsuit was first filed in Cook County state court in 2018 and later moved to federal court, which ruled in Cothron's favor. White Castle appealed the decision to the U.S. Court of Appeals for the 7th Circuit, which sent the case to the Illinois Supreme Court to interpret the issues under state law.

The case will now return to federal trial court, which will address early-stage litigation issues such as whether or not to certify the case as a class-action lawsuit. Cothron has asked the court for permission to bring claims on behalf of up to 9,500 current and former White Castle workers.