Published on *The National Law Review* https://natlawreview.com

An Overview of Why Class Action Privacy Lawsuits May Have Just Gotten Bigger – Yet Again

Article By:

Adam B. Korn

Sebastian A. Navarro

Todd Rosenbaum

The Illinois Biometric Information Privacy Act (BIPA), enacted in 2008, was one of the first state laws to address commercial collection of biometric data. Biometric data includes an iris scan, a fingerprint, a voiceprint, or a scan of hand or face geometry. Moreover, BIPA contains a comprehensive set of privacy protections, including requiring informed consent prior to collection of biometric data, a limited right to disclose biometric data, and most significantly, a private right of action for individuals aggrieved by BIPA violations. For such aggrieved individuals, BIPA provides statutory damages up to $1,000 for each negligent violation and up to $5,000 for each intentional or reckless violation.

The private cause of action permitted by BIPA was largely inconsequential for companies after the statute's enactment. But that changed in 2019 when the Illinois Supreme Court in Rosenbach v. Six Flags Entertainment Corp. held that a plaintiff can be considered an "aggrieved person" under BIPA and therefore entitled to statutory damages without alleging an actual injury. In other words, the Court held that a party does not need to have suffered a tangible or monetary injury in order to recover under BIPA; damages are presumed in the case of a BIPA violation. Unsurprisingly, this led to a significant uptick in BIPA lawsuits, including a class action lawsuit against Facebook in 2020 alleging the company collected biometric data without users' consent, in connection with which Facebook agreed to a $650 million settlement, one of the largest consumer privacy settlements in U.S. history. Similarly, in October 2022, the first-ever BIPA class action jury trial led to a $228 million dollar verdict.

There is no sign that these massive BIPA verdicts and settlements will slow down. In fact, in February 2023, the Illinois Supreme Court in Tims v. Black Horse Carriers, Inc. addressed the critical question of how long the statute of limitations for BIPA claims lasts. BIPA does not expressly provide a statute of limitations period; the plaintiffs argued that a five-year catchall limitation period provided in another Illinois statute should apply to all claims, whereas the defendants argued that a one-year limitation period for publication of private material should apply to all BIPA claims. The court held that BIPA claims other than those relating to publication are subject to a five-year statute of limitations in part due to the legislature's intent to greater regulate privacy consumer privacy. Moreover, the court

held that a longer statutory period also comports with public safety aims by allowing aggrieved individuals sufficient time to discover a violation and file an action.

In February 2023, the Illinois Supreme Court in Cothron v. White Castle System, Inc. further expanded actionable claims under BIPA by clarifying that BIPA claims accrue each time biometric data is unlawfully collected and disclosed. This has the potential to significantly increase damages due to BIPA's language permitting liquidated damages for "each violation" of the statute, although the Court noted that a trial court may exercise its discretion in fashioning an award to prevent damages that would result in "financial destruction of a business." See our Mintz Privacy blog post discussing *Cothron* in detail here.

Although Illinois is the only state that currently has enacted comprehensive biometric privacy laws, several other states, including California, have statutory privacy protections in place. The California Consumer Privacy Right Act (CCPA), enacted in 2018, was the first step in California's ramp-up of its privacy statutes. The CCPA created new protections for consumers, including the right to know about personal information collected by businesses and the right to opt out of such collection. In 2020, California voters approved the California Privacy Rights Act (CPRA), which expanded upon the protections in the CCPA, including the right to limit the use and disclosure of consumers' "personal information" collected by businesses, including biometric information. As of January 1, 2023, the CCPA, as amended by the CPRA, permits consumers to recover damages between $100 and $750 per incident involving a data breach or disclosure of personal information due to a business's failure to take reasonable measures to protect consumer data.

Also pursuant to the amended CCPA, California established a new regulatory agency, the California Privacy Protection Agency, to enforce California's privacy laws under the CCPA and CPRA. This is the first government agency in the United States dedicated to enforcing data privacy laws. Significantly, the agency is charged with creating new regulations to require businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to perform detailed annual cybersecurity audits. Further, the CPRA grants the Agency the power to assess administrative fines up to $7,500 for each violation of the CPRA. While not as comprehensive as BIPA, California's privacy statutes underscore the need for businesses to take privacy considerations seriously.

Nine other states, including New York, Massachusetts, and Maryland, have recently introduced biometric legislation. Nearly all of these states modeled their biometric legislation after BIPA, including providing a private right of action and allowing plaintiffs to recover of statutory damages. Several states have expanded upon the protections included in BIPA. Massachusetts' legislation, for example, provides larger damages awards in class actions by setting damages at "no less than $5,000 per violation." Maryland's legislation permits the state attorney general to impose civil penalties of up to $10,000 per violation in addition to a including a private right of action.

While it may take several more years for other states to adopt comprehensive biometric privacy laws such as BIPA, public demand for increased privacy regulations could make that day come sooner. The evolving legal landscape around data privacy should encourage data holders to regularly assess their practices concerning the use of consumer data.

National Law Review, Volume XIII, Number 60

Source URL:https://natlawreview.com/article/overview-why-class-action-privacy-lawsuits-may-have-just-gotten-bigger-yet-again