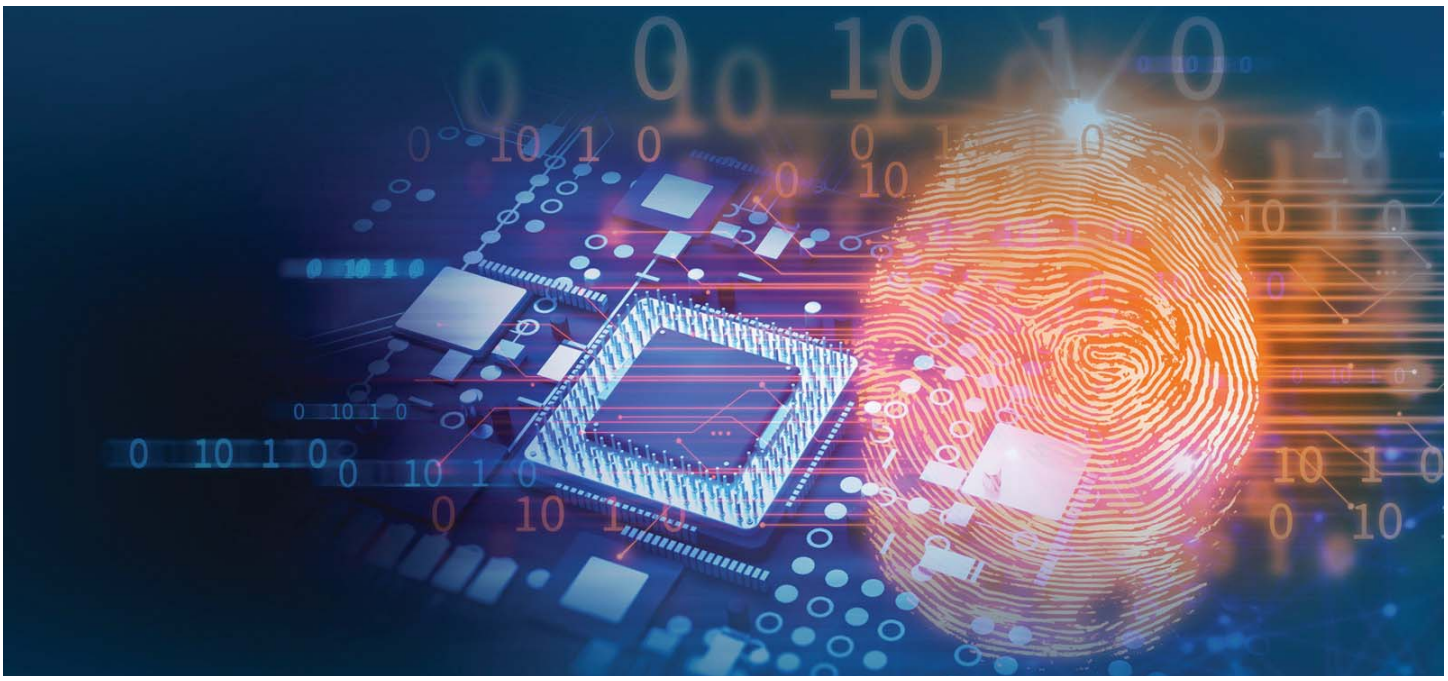
THE ILLINOIS
MANUFACTURER
SECOND QUARTER 2020

2020 MAKERS MADNESS:
"THE COOLEST THING MADE IN ILLINOIS"
CATERPILLAR'S 797F LARGE MINING TRUCK

BIOMETRIC INFORMATION PRIVACY LIABILITY: A HIGH AND RISING TIDE

VEDDER PRICE



The Spring 2018 issue of *The Illinois Manufacturer* featured an article ("What You Need to Know About Using Your Employee's Biometric Information") counseling that readers make it a high priority to comply with a 2008 Illinois law, the Biometric Information Privacy Act ("BIPA"), though BIPA had been largely ignored for much of the first decade of its life. Subsequent developments, including a flood of BIPA class actions, and Facebook's $550 million BIPA settlement, have underscored the soundness of that advice, and demonstrated the massive liability employers risk if they violate BIPA's mandates on how they collect, use, share and secure biometric information, such as the fingerprint scans widely used in modern time keeping systems. This article reviews BIPA's requirements, surveys the BIPA explosion, discusses court decisions that have detonated and sustained that explosion, and concludes with some practical action items.

BIPA's Rationale and Requirements

Unlike other unique identifiers, such as social security or credit card numbers that can be changed, biometrics (for example, unique physical characteristics useful in identifying an individual, such as DNA, fingerprints, facial, hand or retinal features) are immutable. Because they do not change, biometrics are particularly useful in a variety of business settings. They can facilitate reliable, cost-effective time tracking for nonexempt workers, and virtually eliminate the time clock fraud of old (where Jones punches in for his tardy coworker Smith in Smith's absence). Biometrics can also promote security by reliably keeping unauthorized staff out of facilities, secure parts of physical plants, and information storage devices where confidential information or trade secrets are stored. (Look no further than your iPhone® home key's finger scanning feature.)

But the same unchangeable nature that makes biometrics useful arguably requires unique security measures to prevent their misuse. BIPA was intended to safeguard against the risk of identity theft created by the widespread use of biometric technology to facilitate financial transactions and security screenings. It imposes both detailed requirements on the management of information derived from biometric identifiers, and stiff penalties ("liquidated damages" in statutory parlance), for violations. BIPA requires private entities that use or possess biometric information and identifiers to maintain publicly available written policies that disclose their collection of biometric information, their purpose in collecting it, the use to which they will put it, and their retention schedule and guidelines for destroying biometric information and identifiers. BIPA also mandates that before any data is collected, written releases be provided by each individual from whom biometric data is to be obtained (such as manufacturing employees who will use finger-scan timekeeping technology). BIPA requires that biometric information users adhere to the "reasonable standard of care" for handling biometric information and identifiers in their relevant industry, and bars private entities from selling or disclosing biometric information and identifiers.

BIPA's Sanctions

BIPA has sharp teeth. Unlike other biometric privacy legislation to date, BIPA includes severe penalties and gives indi-

About the Author: Nicholas Anaclerio is a Shareholder at Vedder Price and can be reached at nanaclerio@vedderprice.com, or (312) 609-7538.

viduals "aggrieved" by BIPA violations potentially crippling private causes of action. Negligent violations of BIPA carry a $1,000 per violation penalty, or liability for actual damages, whichever is greater, and intentional or reckless violations carry a per-violation toll of $5,000 or actual damages, whichever is greater. All violations entitle prevailing plaintiffs to recover their reasonable attorneys' fees, expert witness fees, and other litigation expenses. Consequently, BIPA defendants face not just the substantial financial burdens of paying their own defense counsel; if they lose, they also face liability for their opponents' attorneys' fees and other litigation expenses.

Consider hypothetically the potential multiplier effect of BIPA "liquidated damages." In January 2009, a small manufacturer implemented biometric timekeeping, but failed to have a publicly available, BIPA-compliant written policy. Throughout the subsequent year, each of its 300 employees used its timeclocks four times per shift (at shift start and end, and at break start and end) for each of five shifts per week for each of 50 workweeks. Assuming this manufacturer's violations are found merely negligent, plaintiffs' class counsel may argue that its BIPA liability for that year totals $300,000,000 plus class counsel's fees and costs. If the same manufacturer's violations are found "intentional" or "reckless," workers' class counsel may argue that its liability is $5,000 per violation for each of 300,000 violations, or $1,500,000,000 in fines, plus plaintiffs' class counsel's fees. Given these astronomical numbers, many plaintiffs adopt damages theories less aggressive than this four-violations-per-shift calculation, and our hypothetical manufacturer might well settle for a substantial discount. Still, the BIPA multiplier effect would give the plaintiffs' class counsel formidable leverage in negotiating that settlement.

Rosenbach Opens the Floodgates

On January 25, 2019, the Illinois Supreme Court decided *Rosenbach v. Six Flags Entertainment Corp.*, in which the plaintiff alleged that the theme park took her minor son's thumbprint when issuing his season pass, and committed technical BIPA violations, though she did not claim any actual harm (such as misuse of the boy's biometric data). Rejecting Six Flags' contention that Ms. Rosenbach's son could not be "aggrieved by a violation" of BIPA sufficient to warrant the suit without pleading and proving actual harm, the Illinois Supreme Court held that no allegation of actual harm was necessary for the plaintiff to seek relief. It remains controversial whether BIPA liquidated damages are available to plaintiffs who have suffered no actual damages. Notwithstanding, plaintiffs' class counsel (and some judges) maintain that *Rosenbach* indeed decided that no actual damages are necessary for plaintiffs to recover BIPA liquidated damages.

The Flood that Followed and the Facebook Settlement

Predictably, after *Rosenbach*, plaintiffs' class counsel fell in love with BIPA. Relieved of any obligation to plead that a defendant's technical noncompliance with BIPA actually hurt anyone, they have prosecuted class actions with a zeal that shows no signs of relenting. The ease with which employers and others can unintentionally violate BIPA has fueled the ascendency of BIPA class actions.

Suit filing reports for the Circuit Court of Cook County, Illinois, reflect the filing of 72 BIPA class actions in calendar 2018, and 20 BIPA class actions in the final calendar quarter of 2018 (October through December 2018). During the first calendar quarter of 2019 alone (just 2/3 of which post-dated the *Rosenbach* decision), 80 BIPA class actions (four times the total number for the preceding calendar quarter, indeed more than the total number for all of 2018) were filed in the Circuit Court of Cook County. For calendar year 2019, 279 BIPA class actions were filed in the Circuit Court of Cook County, nearly four times as many as were filed in 2018 (the last full year before *Rosenbach*).

Following *Rosenbach*, the federal Ninth Circuit Court of Appeals in *Patel v. Facebook, Inc.* rejected Facebook's contention that a massive putative class of users who claimed BIPA violations arising from Facebook's facial recognition software lacked standing to sue because they did not allege actual "real world" harm. (Facebook's facial recognition software enabled it to analyze newly uploaded photos and suggest that users "tag" friends in the photos.) In December 2019, Facebook petitioned the U.S. Supreme Court to decide whether constitutionally required standing (harm sufficient to entitle one to bring suit) could exist based solely on the risk that a plaintiff's personal information might be misused in the future. The Supreme Court refused to consider Facebook's appeal on January 21, 2020, however, subjecting the tech mammoth to the risk of a trial that it averted days later with a $550 million settlement.

While sophisticated tech giants including Facebook, Google, and Vimeo have been caught in the BIPA web, many far smaller employers have also been forced to defend BIPA class actions brought by plaintiffs who can sue without claiming they have sustained any actual harm from the technical violations they allege.

Action Items

If your business uses biometrics as simple as finger scan timekeeping systems, it is at risk, and should, either independently or with qualified counsel:

(1) audit, for the duration of its use of biometrics, whether it has complied fully with BIPA's policy-making and publication, notice, consent, security and other requirements;

(2) identify, quantify and mitigate its risks of BIPA liability by correcting any areas of noncompliance;

(3) consult vendors used to facilitate biometric data collection, storage, use, and deletion, to assess their BIPA compliance;

(4) evaluate vendor agreements that allocate liability risks, including BIPA liability, through indemnification and insurance procurement provisions;

(5) review insurance programs to assess whether BIPA liability is or is not covered (whether BIPA liabilities fall within standard insurance coverage is itself a complex and disputed question);

(6) consider BIPA liability in the insurance renewal process; and

(7) monitor, and consider supporting legislative and judicial initiatives aimed at moderating the BIPA burden that employers in Illinois and elsewhere now face. ◆