Employer Update

Weil

May 2019

Biometrics in the Workplace: Key Lessons from Emerging Case Law Under the Illinois BIPA

By David R. Singh, John Stratford, and Neeckaun Irani

In This Issue

In 2019, we can presume familiarity with the once-futuristic concept of identity authentication via biometric data. Our faces or fingerprints are scanned countless times each day when we unlock our smartphones,[1] and employers are increasingly taking advantage of the security and efficiency benefits of biometric authentication of employees. But the laws governing the collection of biometric data, and court interpretations of those laws, are still catching up. In 2008, the Illinois General Assembly passed the Biometric Information Privacy Act (BIPA)[2], making it the first state to regulate the collection of biometric data, which the BIPA defines to include fingerprints, eye scans, voiceprints, or scans of hand or face geometry. In general, the Act requires private companies to notify individuals and obtain consent for biometric data collection and issue related policies, obligates companies to employ measures to safeguard such information, and prohibits companies from disclosing that information except in specific circumstances. While the BIPA remains the only such law in the United States that provides for a private right of action, it has spawned significant litigation, including in the employment context, and diligent employers should review its provisions and analyze the case law interpreting BIPA to date in order to stay ahead of what is sure to be an expanding area of compliance and litigation risk.

Biometric Data

Biometric data generally refers to personal data relating to physical, physiological, or behavioral characteristics that may be used to identify an individual. Common statutory definitions include fingerprints, facial recognition scans relying on facial geometry, iris scans, voice recognition, and medical measurements like glucose levels or heart rhythms, while more familiar low-tech characteristics like written signatures, photographs, or physical descriptions like height, weight, hair color, or eye color may be excluded.[3] As the Illinois General Assembly highlighted in its legislative findings, biometrics are biologically unique to each individual and cannot be changed.[4] Thus, unlike the theft of social security numbers or security passcodes, for example, which can be changed if compromised, a one-time victim of biometric identity theft risks being forever compromised and left without recourse.[5] This concern, coupled with the fact that the "full ramifications of biometric technology are not fully known"[6] despite its increasing use, have caused legislators, regulators, courts, privacy advocates, and, increasingly, the plaintiffs' bar to focus on biometric issues.

Growth of Biometric Regulation and Litigation

Although no federal statute specifically governs the collection of biometric data currently, a growing number of state legislatures have recognized the increasing importance of biometric data issues. A number of states have expanded the definition of personal information under data breach statutes to include biometric information, for example.[7] A smaller number have followed in Illinois' footsteps and have enacted similar biometric-specific statutes as well.[8] In addition, as is often the case in the fast-moving privacy arena, various foreign jurisdictions have been early movers in enacting laws that implicate the collection and use of biometric data. The sweeping General Data Protection Regulation enacted in the European Union includes biometric data within its heightened classification of "sensitive personal information" which imposes more stringent data processing conditions in addition to the conditions already set forth for "personal information." Similarly, the recently-enacted Chinese Cybersecurity Law also categorizes biometric data as "sensitive personal information" and imposes more stringent requirements.

While other state biometric data statutes allow for enforcement by state attorneys general, the BIPA is unique in its allowance for a private right of action, and Illinois has become an early frontier for biometric litigation as a result, with both consumer and employee plaintiffs alleging that biometric data was improperly collected or used without consent.[9] Notably, the BIPA allows successful private plaintiffs to obtain the higher of actual damages or statutory damages of $1,000 per violation and $5,000 per intentional or reckless violation, in addition to attorneys' fees.[10]

Compounding this potential for significant damages where large numbers of individual violations may be at issue, early in 2019, the Supreme Court of Illinois held that plaintiffs are "aggrieved" and have standing to proceed under the BIPA by virtue of a defendant's violation of the act itself – even if plaintiffs have suffered no additional damage or adverse effect.[11] In *Rosenbach v. Six Flags Entm't Corp.*, Six Flags collected customer thumbprints to more quickly verify season pass ticket holders and to prevent fraudulent re-use of another customer's pass in its theme parks.[12] The mother of a child whose thumbprint was collected sued Six Flags for failing to follow the BIPA's procedures for obtaining consent.[13] After the trial court denied Six Flags' motion to dismiss, Six Flags appealed, arguing that the BIPA required some additional injury or adverse effect beyond mere violation of the statute. The appellate court agreed with Six Flags, but the Supreme Court reversed, holding that "when a private entity fails to comply with one of [the BIPA's consent] requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach."[14] Counsel experienced in defending privacy class actions in federal court may recognize the immediate contrast this decision draws with the "concrete and particularized" harm required to show Article III standing in federal court under *Spokeo v. Robins*, 136 S.Ct. 1540 (2016). Indeed, this distinction in standing requirements will require defendants to think carefully before asserting a *Spokeo* challenge to BIPA claims in federal court at the risk of being "trapped" in what may be perceived as more plaintiff-friendly state court jurisdictions if the motion is granted. In any event, it is clear that this early Illinois precedent, combined with the availability of per-violation statutory damages and the uncertainty created by a patchwork of new and underdeveloped areas of law, means that companies subject to BIPA must take seriously the risk of BIPA class actions and plan accordingly.

Biometric Data in the Employment Context

Given the now-widespread use of biometrics in the workplace, employers should pay special attention to the general trends above, and the increase in BIPA litigation in particular. A 2018 survey of IT professionals in North America and Europe, for example, showed that 62% of companies were currently utilizing biometric authentication, and an additional 24% planned on using it by 2020.[15]

The scope of employee lawsuits under the BIPA has matched the myriad uses that employers make of biometric data. One common alleged BIPA violation stems from employers' use of fingerprint scans for timekeeping in lieu of classic clock-punching.[16] Employers using such technologies have been subject to dozens of class-action lawsuits where plaintiff employees allege failure to comply with the BIPA,[17] with some resulting in significant settlements.[18] The alleged violations in these suits may include an employer's failure to notify or obtain consent for fingerprint collection, failure to issue a policy on biometric data collection, and, to the extent third-party vendors are used to administer the system, a failure to obtain consent for disclosure of the information.[19] Importantly – and perhaps of particular interest given recent U.S. Supreme Court jurisprudence upholding the use of class-action waivers in arbitration agreements under the NLRA[20] – courts have held that employee arbitration agreements may not cover BIPA claims where such claims are not specifically enumerated in the agreement.[21]

In recognition of these trends, the Illinois state legislature has proposed legislation to restrain the litigation stemming from the Act, albeit in the face of resistance by privacy advocates.[22] One recent proposal excludes from the private right of action collection "by an employer for employment, human resources, fraud prevention, or security purposes" and instead provides for enforcement by the Department of Labor.[23] Although passage of this or similar amendments in Illinois could soften the impact of the BIPA on employers, the increased scrutiny of biometric data collection makes it unlikely that a meaningful reversal of the trend will take place in the near future, and indeed there are already signs that more state legislatures will follow Illinois in allowing for a private right of action.[24]

Takeaways

Given the rise of employers utilizing biometric data and ever-increasing litigation in this unsettled area of law, companies potentially subject to the BIPA and similar laws must proactively work to comply and reduce litigation risks. While the nature of actions a company must take will necessarily scale with the size of the enterprise and the scope of its data collection, at a high level, companies should at least consider the following steps:

- Take stock of biometric data collection practices at the company; determine what is being collected, from whom, and for what purposes.
- Assess the company's practical and technological measures for safeguarding biometric data and ensure at a minimum compliance with industry standards.
- Immediately draft policies that cover the collection and use of biometric data under the guidelines set forth in the BIPA or review existing policies to ensure compliance.
- Review the company's policies and practices on obtaining consent from employees, and implement an appropriate system for tracking consent.
- Draft employment agreements and arbitration clauses with biometric data laws in mind.
- Continue to monitor trends in state and federal legislation, as well as the rapidly developing case law interpreting the BIPA.

---

[1] One 2017 study found that Americans check their smartphones an average of eighty times per day, or once every twelve minutes. *See* SWNS, *Americans check their phones 80 times a day: study*, New York Post (Nov. 8, 2017), *available at* https://nypost.com/2017/11/08/americans-check-their-phones-80-times-a-day-study/.

[2] 740 Ill. Comp. Stat. Ann. 14/15.

[3] *See, e.g.,* 740 Ill. Comp. Stat. Ann. 14/10.

[4] 14/5. Legislative findings; intent, IL ST CH 740 § 14/5.

[5] *Id.*

[6] *See id.*

[7] Wis. Stat. Ann. § 134.98 (West); Iowa Code Ann. § 715C.1 (West); Neb. Rev. Stat. Ann. § 87-802 (West).

[8] Other states, like Texas and Washington, have also enacted statutes focusing on biometric data collection and use. Tex. Bus. & Com. Code Ann. § 503.001 (West); Wash. Rev. Code Ann. § 19.375.020 (West).

[9] *See, for example, U.S. Equal Employment Opportunity Commission v. Consol Energy, Inc*., 860 F.3d 131, 140 (C.A.4 (W.Va.), 2017) (upholding over $400,000 jury award where employer failed to accommodate based on employee Christian Evangelicals' religious belief that biometric hand scanners are associated with the Antichrist's Mark of the Beast).

[10] 740 Ill. Comp. Stat. Ann. 14/20.

[11] *See Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, at *8.

[12] *Id.* at *1.

[13] *Id*. at *5.

[14] *Id.* at *6.

[15] Spiceworks, Inc, Data Snapshot: Biometrics in the workplace commonplace, but are they secure? The Spiceworks Community, https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure (last visited May 5, 2019).

[16] Charles N. Insler, Understanding the Biometric Information Privacy Act Litigation Explosion, 106 Ill. B.J. 34, 36 (2018).

[17] *See, e.g., Grabowska v. Millard Maintenance Company, LLC*, No. 2017-CH-13730 (Ill.Cir.Ct. filed Oct. 12, 2017); *Henderson v. Signature Healthcare Services, LLC*, No. 2017-CH-12686 (Ill.Cir.Ct. filed Sept. 19, 2017).

[18] Becky Yerak, Mariano's, Kimpton Hotels Sued Over Alleged Collection of Biometric Data, Chicago Tribune (July 21, 2017) (Cook County Judge approved a $1.5 million dollar settlement).

[19] *See, e.g., Miller v. Southwest Airlines Co.*, 2018 WL 4030590 (N.D. Ill. Aug. 23, 2018).

[20] *See Epic Systems Corp. v. Lewis*, 138 S.Ct. 1612 (2018).

[21] *Liu v. Four Seasons Hotel, Ltd.*, 2019 IL App (1st) 182645, ¶ 28, 2019 WL 1560416, at *4 (Ill.App. 1 Dist., 2019) (holding arbitration clause did not apply to BIPA violation because timekeeping did not relate to arbitration covered wage and hour violations which typically involve wrongfully withholding wages, or complying with work regulations, rather than privacy rights.).

[22] Ross Todd, Illinois Biometric Privacy Law-and Effort to Carve Out Exceptions-Gets Moment in Spotlight at Facebook Hearing The Recorder (2018), https://www.law.com/therecorder/2018/04/10/illinois-biometric-privacy-law-and-effort-to-carve-out-exceptions-gets-moment-in-spotlight-at-facebook-hearing/ (last visited May 5, 2019); 2019 Illinois Senate Bill No. 2134, Illinois One Hundred First General Assembly - First Regular Session, 2019 Illinois Senate Bill No. 2134, Illinois One Hundred First General Assembly - First Regular Session.

[23] *See id.*

[24] *See, e.g.*, Fla. H.B. 1153 (2019) (proposed Florida Biometric Information Privacy Act, providing for a private right of action for aggrieved plaintiffs).

Employer Update is published by the Employment Litigation and the Executive Compensation & Benefits practice groups of Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

If you have questions concerning the contents of this issue, or would like more information about Weil's Employment Litigation and Executive Compensation & Benefits practices, please speak to your regular contact at Weil, or to the practice group members listed below.

Practice Group Members:

Jeffrey S. Klein
Practice Group Leader
New York
+1 212 310 8790
jeffrey.klein@weil.com

Frankfurt
Stephan Grauke
+49 69 21659 651
stephan.grauke@weil.com

London
Ivor Gwilliams
+44 20 7903 1423
ivor.gwilliams@weil.com

Miami
Edward Soto
+1 305 577 3177
edward.soto@weil.com

New York
Sarah Downie
+1 212 310 8030
sarah.downie@weil.com

Gary D. Friedman
+1 212 310 8963
gary.friedman@weil.com

Steven M. Margolis
+1 212 310 8124
steven.margolis@weil.com

Michael Nissan
+1 212 310 8169
michael.nissan@weil.com

Nicholas J. Pappas
+1 212 310 8669
nicholas.pappas@weil.com

Amy M. Rubin
+1 212 310 8691
amy.rubin@weil.com

Paul J. Wessel
+1 212 310 8720
paul.wessel@weil.com

Silicon Valley
David Singh
+1 650 802 3010
david.singh@weil.com