LITIGATION UNDER ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT HIGHLIGHTS BIOMETRIC DATA RISKS

Date: 7 November 2017

U.S. Class Action Litigation Defense Alert

By: Carley Daye Andrews, Corey Bieber, Carl E Volz, Julia B. Jacobson, Molly K. McGinley

Since June 1, 2017, over thirty class actions have been filed in Illinois alleging claims under the Illinois Biometric Information Privacy Act ("Illinois BIPA"), which regulates the use and retention of biometric information.

Biometric information generally means data generated by analysis of an individual's biological characteristics, such as retina or iris scan, fingerprint, voiceprint, handprint, face geometry, or other unique biological patterns or characteristics that identify a specific individual.

Illinois BIPA was enacted in 2008 because major national corporations had selected Illinois as the test site for new applications of "biometric facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias."[1] Although Illinois BIPA has been on the books for almost a decade, it only recently has become a significant focus of the plaintiffs' bar. So why the uptick in litigation now?

Since 2008, use of facial recognition and other biometric information collection systems has been common in the public sector.[2] In the private sector, biometric information collection is equally prevalent, including use of fingerprint scans to lock and unlock smartphones, facial recognition-based tagging features in digital photo applications, to use by employers, and in security applications.

The vast repositories of biometric information collected through these myriad systems may be particularly attractive to hackers because biometric information does not change. As Senator Al Franken noted in his opening statement to the hearing of the Senate Judiciary Subcommittee on Privacy, Technology and the Law on how facial recognition technology affects privacy and civil liberties:

> "…biometric information is already among the most sensitive of our private information, mainly because it is both unique and permanent. You can change your password. You can get a new credit card. But you cannot change your fingerprint, and you cannot change your face—unless, I guess, you go to a great deal of trouble." [3]

With daily headlines stoking fears of large-scale data breaches and the immutable characteristics of biometric information, increasing public concern about the privacy and security of biometric information is no surprise.

As most cases brought in Illinois remain pending, the risk of liability is an open question, but defendants face the cost of defending class action lawsuits, potential statutory damages, potentially invasive discovery, and the possibility of requests for prospective relief to ensure future compliance with the Illinois BIPA.

Below, we discuss the history of biometric information laws, definitions of biometric information, scope and enforcement of existing laws, a brief overview of current litigation unfolding in Illinois, and recommendations to ensure compliance with existing biometrics laws.

A BRIEF HISTORY OF BIOMETRIC INFORMATION LAWS

When it was passed in 2008, Illinois BIPA was the first of its kind. Close on the heels of Illinois BIPA, Texas enacted its Capture or Use of Biometric Identifier statute ("Texas BIS") in 2009.[4] On July 23, 2017, Washington's Biometric Identifiers law ("Washington BI") went into effect.[5] Of these three biometric information laws, only Illinois BIPA provides for a private right of action, as discussed below.

Also this year, other states considered (but did not pass) laws governing the collection and use of biometric information, including Alaska (H.B. 72, 30th Leg., Reg. Sess. (Alaska 2017)), New Hampshire (H.B. 523, 2017 N.H. H.R., Reg. Session (N.H. 2017)), and Connecticut (H.B. 5522, 2017 Gen Assemb., Reg. Sess. (Conn. 2017)).

In several states, biometric information is included in the definition of personal information that is subject to data breach notification requirements, including Delaware, Illinois, Iowa, Maryland (effective January 1, 2018), Nebraska, New Mexico, North Carolina, Wisconsin, and Wyoming.[6] Among others, New York (2015) and California (2016) have considered (but did not pass) laws that included biometric information for data breach notification purposes.

In December 2011, the Federal Trade Commission (FTC) hosted a workshop exploring facial recognition technology and the privacy and security implications raised by its increasing use.[7] Shortly thereafter, the Senate Subcommittee on Privacy, Technology and the Law held its hearing on facial recognition technology. Not surprisingly, both the FTC's workshop and the Senate Subcommittee hearing had extensive participation from the private sector.

At the federal level, bills addressing biometric privacy have been proposed, but none has succeeded.[8] An existing law, Children's Online Privacy Protection Act (COPPA)[9], regulates collection of biometric information from children. Specifically, COPPA requires verifiable parental consent before photos, videos, and audio recordings that contain a child's image or voice are collected from children.[10] COPPA also permits a business to verify parental consent using facial recognition technology.[11] This past summer, the FTC, which is empowered to enforce COPPA, issued a policy statement indicating that the collection of an audio file with a child's voice solely as a replacement of written words is not subject to COPPA's restrictions if (among other requirements) the information collected via voice is not otherwise considered personal information, and no other use of the audio file is made before it is destroyed.

Outside the United States, a new privacy law coming into effect in the EU also covers biometric information and includes the potential for significant fines for noncompliance.

WHAT IS BIOMETRIC INFORMATION?

Each of Illinois, Texas, and Washington provides a slightly varying definition of biometric information:

- Illinois BIPA defines "biometric identifiers" as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." Among other exclusions, Illinois BIPA expressly excludes writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, physical descriptions (such as height, weight, hair color, and eye color), information captured from a patient in a health care setting and other types of information.[12]
- The Washington BI defines biometric information as "data generated by automatic measurements of an individual's biological characteristics" and provides some examples[13], but restricts only biometric information that has been "enrolled" or reduced to another irreversible form in a database. Like Illinois BIPA, Washington BI excludes photographs and information collected in connection with health care treatment and also expressly excludes data generated from photographs, an area that has become the focus of some recent Illinois lawsuits as described below.
- The Texas BIS uses a narrower definition: "biometric identifiers" means "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[14]

In the EU, the new privacy law known as the General Data Protection Regulation (GDPR), which takes effect on May 28, 2018, includes a broad definition of biometric data as "resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[15] Since GDPR introduces extra territorial scope -- it applies to any business that offers goods or services to the EU or monitors behavior of an individual in the EU -- US businesses subject to Illinois BIPA, Texas BIS, or the Washington BI also could be subject to GDPR.

HOW IS BIOMETRIC INFORMATION REGULATED?

Illinois BIPA, Texas BIS, and the Washington BI share some common characteristics. Each of them:

- applies to private entities but not state or local government agencies;
- requires notice before biometric information is collected;
- limits the sale and disclosure of biometric information;
- requires reasonable care to safeguard biometric information;
- limits retention of biometric information to only the purpose for which it was collected; and
- requires destruction of biometric information when it is no longer needed.

Of the three laws, Illinois BIPA has the most rigorous notice and consent requirements as a private entity can collect biometric information only after: (1) informing the subject in writing that biometric information is being collected or stored and stating the specific purpose and length of term for which the information is being collected,

stored, and used; and (2) receiving a signed, written release.[16] Texas BIS also requires notice and consent, but not necessarily written consent, before biometric information is collected.[17]

The Washington BI is a bit more opaque on the topic of notice and consent. Specifically, it requires consideration of context when determining the appropriateness of notice before the "enrollment" of biometric information. To 'enroll' a biometric identifier means to "capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual."[18] The Washington law also offers the pre-enrollment alternatives of "obtaining consent" or "providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose."[19]

All three states prohibit the sale or other disclosure of biometric information collected from an individual, unless: (1) the individual consents to the disclosure; (2) the disclosure completes an authorized financial transaction; (3) the disclosure is required by state or federal law or municipal ordinance; or (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction. The Washington law permits disclosure of biometric information without consent whenever doing so is "necessary to provide a product or service subscribed to, requested, or expressly authorized by the individual" or subject to contractual requirements that are consistent with the scope of the consent. Moreover, Washington law does not require notice and consent "to collect, capture, or enroll a biometric identifier and store it in a biometric system, or otherwise, in furtherance of a security purpose."[20]

Illinois' BIPA also requires that a business in possession of biometric identifiers have a publicly available written policy, and to establish a retention schedule and guidelines for the destruction of biometric information. The policy must require the destruction of biometric information whenever the initial purpose for its collection has been satisfied, or within three years, whichever occurs first. Texas BIS has a one-year destruction period instead of three-year period, but does not require a publicly-available written policy.

Biometric information collected from patients in the health care context under the federal Health Insurance Portability and Accountability Act ("HIPAA") is excluded from regulation under the Illinois and Washington laws.

The EU GDPR law prohibits the collection and use of biometric data unless the purpose for the collection and use fits within one of the limited exceptions, which include circumstances when the collection and use are necessary for compliance with law, or to protect the vital interests of the person to whom the biometric information relates (the "data subject") if that individual is physically or legally incapable of giving consent, or if the data subject makes the biometric information manifestly available, or gives written, unambiguous, specific and freely given consent.[21]

HOW ARE BIOMETRIC INFORMATION LAWS ENFORCED?

Illinois BIPA has garnered the most attention from the plaintiffs' bar because, unlike Texas BIS and Washington BI, Illinois BIPA has an express private right of action with significant statutory damages of $1,000 or actual damages (whichever is greater) for each negligent violation of the act, and $5,000 or actual damages (whichever is greater) for each intentional or reckless violation of the act.[22] Thus, plaintiffs seek damages for each violation--for example, each instance when a putative class member scanned his or her finger into the defendant's timekeeping device, or each photo uploaded to a website where facial recognition technology is automatically applied. Significantly, Illinois BIPA also includes an attorney's fee provision, including expert witness fees and

other expenses, and allows plaintiffs to seek injunctive relief. The plaintiffs' bar has seized on this opportunity, filing class actions under Illinois BIPA not only in Illinois, but also in other states as well.[23] Damages under Illinois BIPA may be crippling in class action litigation where the number of potential violations could proliferate into the seven or eight figure range.

The Texas BIS has left enforcement to the attorney general, with civil penalties of not more than $25,000 per violation. The Washington BI does not include its own private right of action but a violation of it is deemed a violation of Washington's Unfair Business Practices-Consumer Protection Act[24], which may be enforced solely by the attorney general.

Under the EU's GDPR, fines for non-compliance are up to the greater of 4% of annual global revenue, or €20m. The GDPR also provides for private rights of action and class actions in certain instances.

WHAT IS THE LITIGATION LANDSCAPE UNDER ILLINOIS BIPA?

Despite years of inactivity under Illinois BIPA, seven cases were filed in 2015; plaintiffs then filed seven more putative class actions in 2016. The cases filed in 2015 and 2016 generally targeted retailers and online service providers, alleging that they improperly collected and stored photographs. In 2016, plaintiffs also began focusing on businesses that collect fingerprint data, with several lawsuits filed against companies that were scanning customers' fingerprints while receiving services. So far in 2017, there has been an explosion of lawsuits under Illinois BIPA, with more than 30 new class action lawsuits filed in the past four months alone and new filings on a near daily basis. Plaintiffs have increasingly directed their attention toward technologies that use biometric information to clock-in employees or monitor employee activities.

While the majority of lawsuits filed under Illinois BIPA in 2015 and 2016 were brought in federal court, almost all of the 2017 Illinois BIPA class actions have been filed in Illinois state court. The trend is, however, to remove these Illinois BIPA state court proceedings to federal court under the Class Action Fairness Act.[25]

Defendants in most Illinois BIPA cases have moved to dismiss the claims, arguing improper extraterritorial application of Illinois law, violation of the U.S. Constitution's Dormant Commerce Clause, lack of personal jurisdiction, failure to allege injury sufficient to confer Article III standing, and failure to allege a violation of Illinois BIPA. The U.S. Supreme Court case of *Spokeo Inc. v. Robbins*[26] appeared to support dismissal of some claims on Article III standing grounds, but the Northern District of Illinois recently rejected that argument[27], finding that the plaintiff had alleged a violation of privacy sufficient to confer standing. Even where courts have denied motions to dismiss, they have emphasized the importance of early discovery on the issue of Article III standing.[28] If an Illinois BIPA class action survives dismissal at an early stage, defendants could face significant discovery, including discovery into the use of the biometric information that has been collected.

RECOMMENDATIONS TO ENSURE COMPLIANCE WITH BIOMETRIC INFORMATION LAWS

While some of these cases have settled or been dismissed[29], the vast majority of cases remain pending. Accordingly, the level of the risk associated with liability under Illinois BIPA is an open question. Nevertheless, in

light of the heavy burden of defending class action litigation, any business that collects biometric information should take steps to reduce the risk of litigation and regulatory fines in this area. Best practices include:

- Identify whether biometric information is collected and for what purpose.
- Determine whether notice and consent requirements apply and whether existing processes satisfy those obligations. Complying with Illinois BIPA's notice and consent requirements for biometric information generally will ensure compliance with the other two states' notice and consent requirements if the notice is sufficiently explicit about intended uses of the biometric information.
- Apply administrative, logical, and/or physical restrictions to restrict the sale or other transfers-for-profit of biometric information. For example, ensure that biometric information stored in a database is accessible only to authorized individuals who are trained in biometric information laws.
- Confirm that the company's security incident response policy addresses biometric information for those states in which biometric information is subject to data breach notification requirements.
- Verify that existing data retention and destruction policies include provisions that meet the requirements of Illinois BIPA and the Texas BIS.
- Check that current information security policies specifically consider the sensitivity of biometric information to ensure that the biometric information laws' requirement of "reasonable care" is met. Examples of reasonable care with respect to the security of biometric information are context-specific, but could include encryption, firewalls, intrusion detection systems and anti-malware software.
- When biometric information is collected from employees, ensure that adequate notice and consent processes are in place. As noted above, the use of fingerprint identification for workplace clock-in and clock-out procedures has become the subject of recent litigation.[30] Consider asking employees to agree to the use of their biometric information at the time of hire, or prior to introducing biometric technology in the workplace.

* * * *

In light of the recent flurry of new statutes and the increase of litigation in this area, businesses collecting data that could be considered biometric information should evaluate their current policies to confirm they comply with the varying requirements of these state laws.

This alert provides some high-level information on biometric privacy laws. Please join us at our upcoming Webinar, where these issues will be discussed in greater depth.

Notes:

1 740 ILCS 14/5(b).
2 For example, the Department of Homeland Security's Office of Biometric Identity Management (OBIM) operates and maintains the Automated Biometric Identification System or IDENT. See https://www.dhs.gov/biometrics (last visited Nov. 2, 2017).
3 *What Facial Recognition Technology Means for Privacy and Civil Liberties*, 115 Cong. 1 (2012) (Statement of Sen. Al. Franken), *available at* https://www.gpo.gov/fdsys/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf.

4 Tex. Bus & Com. Code Ann. §503.001 (West).
5 Wash. Rev. Code Ann. §19.375.010 et seq. (West).
6 Massachusetts also considered (but did not pass) an amendment to its data breach notification law. H.B. 1985, 190th Gen. Court, Reg. Sess. (Mass. 2017), *available at* https://malegislature.gov/Bills/190/H1985.
7 *See* Face Facts: A Forum on Facial Recognition Technology, FEDERAL TRADE COMMISSION ROUNDTABLE (2011).
8 *See* Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (Sen. Rockefeller); Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (Sen. Leahy); Personal Data Protection and Breach Accountability Act of 2014, S. 1995, 113th Cong. (Sen. Blumenthal); Personal Data Notification and Protection Act of 2015, H.R.1704, 114th Cong. (Rep. Langevin).
9 15 U.S.C. §§ 6501-6506.
10 Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business, FEDERAL TRADE COMMISSION (2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.
11 *See* Letter from Donald S. Clark, Secretary, Federal Trade Commission, to Jest* Limited (Trading as Riyo), c/o Allison Fitzpatrick (Nov. 15, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/881633/151119riyocoppaletter.pdf (describing a two-step process combining photo verification identification with facial recognition technology to allow parents to provide consent via web and mobile devices to collect personal information about children).
12 740 ILCS 14/10
13 H.B. 1493, 65 Leg., Reg. Sess. (Wash. 2017).
14 Tex. Bus & Com. Code Ann. §503.001(a) (West).
15 Council Regulation 2016/679/EC on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L119/34 (hereinafter "Council Regulation").
16 740 ILCS 14/5(b)(1)-(3) (West).
17 Wash. Rev. Code Ann. §19.375.020(1) (West).
18 *Id.*
19 *Id.*
20 *Id.* at subsection (7).
21 Council Regulation at L119/37.
22 740 ILCS 14/20 (West).
23 Complaints asserting claims under Illinois BIPA have been filed in California, New York, and Hawaii. See *Martinez v. Snapchat, Inc.*, Case No. 2:16-cv-5182 (C.D. Cal. Jul. 14, 2016); *Santana v. Take-Two Interactive Software, Inc.*, Case No. 1:15-cv-8211 (S.D.N.Y. Oct. 19. 2015); *Bralich v. Sullivan*, Case No. 1:17-cv-00203 (D. Haw. May 04, 2017).
24 Wash. Rev. Code Ann. §19.86 (West).
25 28 U.S.C. §1332(d)(2).
26 578 U.S. __, 136 S. Ct. 1540 (2016).
27 Case No. 16-cv-10984 (N.D. Ill. Sept. 15, 2017).
28 *Rivera, et al. v. Google, Inc.*, Case No. 16-cv-02714, Dkt. No. 94, Minute entry before the Honorable Edmond E. Chang: Status hearing held on the bifurcation issue (N.D. Ill. Aug. 10, 2017) ("Among other things, the Court

also urged the parties to prioritize Article III standing discovery, to the extent discovery is needed, to allow fulsome briefing on that issue sooner rather than later.").
29 One recent case settled on a class basis for $1.5 million, with $600,000 (or 40%) going to settlement class counsel for attorneys fees.
30 See *Howe v. Speedway LLC*, Case No. 2017-CH-11992 (C.O.O.C.C. Sept. 1, 2017).

KEY CONTACTS

CARLEY DAYE ANDREWS
PARTNER

SEATTLE
+1.206.370.7661
CARLEY.ANDREWS@KLGATES.COM

COREY BIEBER
PARTNER

CHICAGO
+1.312.807.4390
COREY.BIEBER@KLGATES.COM

