ABA Business Law Section business law today

Biometric Information – Permanent Personally Identifiable Information Risk

16 Min Read

By: Alan S. Wernick (/author/alanswernick/)

| January 28, 2019

IN BRIEF

- As the business use of biometric data becomes more prevalent, so has the statutory and judicial response concerning the use of biometrics and related privacy and contract law issues.
- Practitioners must proactively address the attendant legal risks with customers, employees, and third-party vendors.

One of the most famous scenes in the movie "Minority Report" features Tom Cruise's character Jon Anderton walking through a shopping mall as discrete scanners using iris recognition technology are hard at work, scanning his

(and other shoppers') irises. The scanners identify everyone individually to create a personalized shopping experience through targeted video screen advertisements that we can see change and move as Tom does. Far-fetched fictional technology? In the past 16 years the potential uses for biometric technology has grown (see, e.g., *"Minority Report" May Come to Real World with Iris Recognition*, Bloomberg Tech., Feb. 1, 2011) and today it is almost reality (see *Princeton Identity looks to make "Minority Report" tech a reality*, SecurityInfoWatch.com, Sept. 25, 2018).

This article briefly defines and describes some biometric applications presently in use, reviews one state's statutory response to biometrics, and looks at how some courts are handling lawsuits over the use of biometrics and related privacy law and contract law issues. The article concludes with some practical pointers for businesses and their professional advisers to consider when implementing biometric applications into the business process.

WHAT ARE BIOMETRICS?

Biometrics measure and analyze people's unique physical and behavioral characteristics. Biometrics' many uses include identification, access controls, testing, and numerous other rapidly evolving business applications. Like all technology, biometrics present both many beneficial applications for businesses and individuals, as well as legal risks.

Examples of biometrics include an individual's DNA, fingerprints, eyeballs/irises/retinas, voiceprints, handprints, and facial geometry, to name just a few. Some biometrics, like fingerprints and retinal blood vessel patterns, generally do not change over time. Others, like facial geometry, can change over time due to age, illness, or other factors, and thus may adversely impact the accuracy of the biometrics. The uniqueness and potential permanence of biometrics are advantageous from a security perspective to accurately identify and distinguish individuals, plus you do not have to worry about forgetting your biometric password.

HOW ARE BIOMETRICS USED IN BUSINESS TODAY?

Businesses presently use, and will continue to use, biometrics (and related technologies) in a wide variety of applications to improve their business processes and their customer and employee interactions, conveniences, and trustworthiness. Some examples include:

- **Workforce management**. Consider a modern update to the time clock for employees logging in and out of work. Instead of workers having to wait in line to retrieve a time card, punch the card into a time-stamping machine, and then replace the time card into its slot, biometric readers allow workers to simply tap their fingerprints onto a biometric fingerprint scanner. This can prevent buddy time-punching and time theft, and increase accountability and security. See the *Dixon* case discussed below.
- **Hospitals**. Although credit-card data breaches make for major headline news, medical identity theft events plus mistakes caused by hospital physicians and staff mixing up patients' files are increasingly common, costly, and potentially life-threatening. Biometric technologies can help hospitals and other medical providers avoid these risks.
- **Banking**. The banking industry has been looking into and adopting biometric technologies to help reduce identity theft and improve efficiencies and customer experience in the banking process.
- **Retail.** Tanning salons, health clubs, or similar member-model-based businesses allow their customers to easily enter and use the business facility by using a fingerprint scanner at any of the businesses' locations for customer identification. See the *Sekura* case discussed below.
- **Automotive**. Biometrics can be used instead of key fobs to enter and operate an automobile, or to recognize whether the driver is becoming impaired (e.g., tired or texting), which could put the occupant(s) of the vehicle and other people and vehicles around it at risk.

However, if compromised, the same characteristics and advantages of biometrics present a potential threat to the individual owner of the biometric markers and risks to the businesses that use, and are the stewards of, biometric data.

> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions. (740 ILCS 14/5(c)).

BIOMETRIC INFORMATION PRIVACY STATUTES

Biometric Information Privacy ("BIP") is permanently ingrained into the privacy legal risk matrix confronting businesses and individuals, and is under review by state and federal legislators and regulators in the United States and other governments and regulators in the international community. October 2018 marked the 10th anniversary of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq.*, a comprehensive BIP statute that has given rise to a number of class-action lawsuits against businesses.

In addition to the Illinois BIPA, other state and federal legislators have considered, or are considering, legislation concerning biometric information privacy. A couple of states (e.g., Texas, 2009; Washington, 2017) have passed biometric information privacy statutes. Other states have considered, or currently are or will be considering, comprehensive legislation regarding biometric information privacy, or currently mention some biometric information (e.g., fingerprints) in their existing statutes. New legislation concerning BIP is under consideration as the legislative and judicial branches of state and federal governments try to understand the impact BIP has on individuals and businesses

today, and whether and how biometric information should be regulated. The Illinois BIPA states: "The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g). This fundamental concept is applicable to and should be considered in all BIP legislation, and viewed in light of the unique permanence of biometric data.

BIPA (740 ILCS 14/20) provides that for each negligent violation of the act, a prevailing plaintiff may recover liquidated damages of $1,000 or actual damages, whichever is greater, in addition to obtaining other relief such as an injunction. For each intentional or reckless violation of the act, the plaintiff may recover the greater of liquidated damages of $5,000 or actual damages. In addition, the plaintiff may recover reasonable attorney's fees and costs, including expert witness fees and other litigation expenses, plus other relief, including an injunction, as the state or federal court may deem appropriate.

In February 2018, SB 3053 was introduced in the Illinois legislature to narrow the application of the Illinois BIPA. The present version of SB 3053 would add language to the Illinois BIPA narrowing it as follows:

> (f) Nothing in this Act shall be deemed to apply to an entity collecting, storing, or transmitting biometric information if: (i) the biometric information is used exclusively for employment, human resources, fraud prevention, security purposes; (ii) the private entity does not sell, lease, trade, or similarly profit from the biometric identifier or biometric information collected; or (iii) the private entity stores, transmits, and protects the biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

The proposed SB 3053 amendments to Illinois BIPA may appear to help certain businesses avoid legal liability as described in the proposed amendment, but at the end of the day it does not change the fact that biometric data, if compromised, will potentially increase the risks to the individual represented by the biometric data. Further, such a change in the statute may not lessen the legal risks of those businesses collecting and using employee and/or customer biometric data, or improve the business's appearance of trustworthiness in the minds of the employees and/or customers (particularly after that individual's biometric information has been compromised). In addition, a further consideration is how this proposed amendment impacts and furthers BIPA's stated legislative findings and intent (740 ILCS 14/5). As of this writing, the SB 3053 proposed amendment to the Illinois BIPA has not been passed into law.

BIP presents complex business, legal, and technology issues for legislators to consider. Thus, careful, critical thinking and thoughtful drafting is required in crafting legislation addressing BIP. Congress, state legislators, government regulators, and legislative bodies and regulators in other countries, as well as drafters of international treaties, have been considering, and will continue to consider, legislation regarding BIP. Like most legislation dealing with technologies, BIP legislation will continue to evolve as the law and legislation tries to catch up to rapidly evolving technologies and to the impact of these technologies on society in our global community.

RECENT BIPA COURT DECISIONS

Several court decisions regarding BIPA have found that simply alleging a violation of BIPA's notice and consent provisions alone are not sufficient to support standing to bring the lawsuit. However, other court decisions have found standing when the allegations went beyond merely alleging a failure of notice and consent.

A recent example of one of these BIPA lawsuits is a September 2018 class-action lawsuit filed in the Circuit Court of Cook County against Wendy's International LLC (the fast food restaurant). Other businesses that have found themselves defending against BIPA lawsuits include Facebook, Lowes Chicago Hotel Inc., Omnicell Inc., Southwest Airlines, and United Airlines. BIPA lawsuits are industry independent and may occur in any industry acquiring and using biometric data. The ultimate outcomes of these and other recently filed BIPA cases is yet to be determined.

In a recent court decision, an Illinois appellate court in *Sekura v. Krishna Schaumburg Tan, Inc.,* 2018 Ill. App. (1st) 180175 (Ill. App. Sept. 28, 2018), had occasion to review BIPA. The plaintiff, Sekura, alleged, among other things:

- Defendant, a franchisee of L.A. Tan Enterprises, Inc. ("L.A. Tan"), required customers enrolling in L.A. Tan's national membership database to have their fingerprints scanned (to allow the customer to use their membership at any of L.A. Tan's locations). Every time the plaintiff visited an L.A. Tan location, plaintiff was required to scan her fingerprints before using the services.
- Plaintiff alleged she had never been:
  - informed of the specific purposes or length of time for which defendant collected, stored, or used her fingerprints;
  - informed of any biometric data retention policy developed by defendant or whether defendant will ever permanently delete her fingerprint data;
  - provided with nor signed a written release allowing defendant to collect or store her fingerprints; and
  - provided with nor signed a written release allowing defendant to disclose her biometric data to SunLync (the third-party vendor receiving the L.A. Tan biometric data) or to any other third party.
- In addition, plaintiff alleged that "in 2013, more than 65% of L.A. Tan's salons were in foreclosure and that defendant's customers have not been advised what would happen to their biometric data if defendant's salon went out of business" and that plaintiff "becomes

> emotionally upset and suffers from mental anguish when she thinks about what would happen to her biometric data if defendant went bankrupt or out of business or if defendant's franchisor, L.A. Tan, went bankrupt or out of business, or if defendant shares her biometric data with others."

The only issue before the appellate court was "whether a harm or injury, in addition

to the violation of the Act itself, is required in order to have standing to sue under the Act." In its statutory interpretation of BIPA, the court carefully parsed the words of BIPA and examined the available legislative intent. The court concluded that the plaintiff did have standing, reversed the trial court's dismissal, and remanded the case back to the trial court for further proceedings.

In its analysis, the court distinguished another Illinois Appellate court decision concerning BIPA, *Rosenbach v Six Flags Entertainment Corporation*, 2017 IL App (2d) 170317 (2017), concluding

> ...even if *Rosenbach* was correctly decided and an additional "injury or adverse effect" is required, *Rosenbach* is distinguishable from this case, in the following two ways. *Rosenbach*, 2017 IL App (2d) 170317, ¶ 28 (requiring an "injury or adverse effect," in addition to violation of the Act). First, as the federal district court similarly found, disclosure to an out-of-state third-party vendor constitutes an injury or adverse effect, and plaintiff in the instant case alleged such a disclosure, while the *Rosenbach* plaintiff did not. *Dixon*, 2018 WL 2445292 *12. Second, the mental anguish that plaintiff alleges in her complaint also constitutes an injury or adverse effect. *E.g.*, *Chand*, 335 Ill. App. 3d at 823, 269 Ill.Dec. 543, 781 N.E.2d 340 (Kuehn, J., concurring in part and dissenting in part) (actual damages may include "mental anguish"). For these reasons, we must reverse and remand.

The Illinois Appellate Court for the 2nd District decision in *Rosenbach* was appealed to the Illinois Supreme Court and reversed. In *Rosenbach v Six Flags Entertainment Corporation* (http://www.illinoiscourts.gov/Opinions/SupremeCourt/2019/123186.pdf), 2019 IL 123186 (January 25, 2019) the Illinois Supreme Court held "...an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act [BIPA], in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act."

In reversing the appellate court, the Illinois Supreme Court stated: "While the appellate court in this case found defendants' argument persuasive, a different district of the appellate court subsequently rejected the identical argument in *Sekura v. Krishna Schaumburg Tan, Inc.*, 2018 IL App (1st) 180175. We reject it as well, as a recent federal district court decision correctly reasoned we might do. *In re Facebook Biometric Information Privacy Litigation*, 326 F.R.D. 535, 545-47 (N.D. Cal. 2018)."

In *Dixon v Washington and Lee Smith Community-Beverly, et al.*, 2018 WL 2445292 (USDC IL ND, 20180531), the Illinois district court was presented with the plaintiff-employee alleging, among other things, that her employer, the defendants, had violated BIPA by requiring employees to clock in and out of work by scanning their fingerprints onto a biometric timekeeping device provided by a third-party vendor, and failed to disclose to plaintiff that her fingerprint data was disclosed to or otherwise obtained by a third party. Defendants argued, in part, that plaintiff lacked standing on the ground that the procedural injuries plaintiff alleged are insufficient to support a cause of action under BIPA or a negligence claim. Plaintiff argued that although defendants' argument is ostensibly aimed at the meaning of "aggrieved" in BIPA, it directly questions whether plaintiff alleged a cognizable injury sufficient to meet Article III standing necessary for federal jurisdiction. "The Court concludes that this alleged violation of the right to privacy

in and control over one's biometric data, despite being an intangible injury, is sufficiently concrete to constitute an injury in fact that supports Article III standing."

Another recent BIPA related development concerns insurance coverage in BIPA lawsuits. As a result of a lawsuit, *Mazya v. Northwestern Lake Forest Hospital, et al.*, 2018-CH-07161 (June 6, 2018), in the Circuit Court, Cook County, Illinois, one of the defendants, Omnicell Inc., tendered the suit to Zurich American Insurance Co., its insurance company, to defend and indemnify Omnicell in that lawsuit. Zurich responded by filing on August 30, 2018, a lawsuit in the U.S. District Court for the Northern District of California alleging that Omnicell's general liability policy expressly excludes coverage for alleged violations of state or federal laws that prohibit collection of personal information. The final outcomes of the *Mazya* case and other BIPA cases discussed in this article are yet to be determined as the courts further explore the facts and the applicable law, and further define the BIP legal landscape.

PRACTICE POINTERS

Although not exhaustive, here are some practical pointers for consideration by businesses and their professional advisers regarding the use of biometric applications in business processes:

1. Develop written policies addressing how the business will collect, use, distribute, and destroy biometric data.
2. Follow those written policies. It does not look good to a judge, arbitrator, or a government regulator (or to employees and customers) when a business's written policies say one thing, but the facts show they are actually doing something else. If you need an economic perspective on this, consider the enhanced statutory penalties found in some statutes when a business is found to have intentionally or recklessly violated the statute.
3. Inform and disclose. Clearly, concisely, and consistent with statutory obligations, notify your employees and customers how you are handling their biometric data.

For instance,

a. How long will the business keep the biometric data?

b. When (and how) will the biometric data be destroyed?

c. Will the biometric data be shared with (e.g., processed by) a third-party vendor?

d. How will the biometric data be handled if the business is sold, closes, or enters bankruptcy?

4. Secure with encryption the biometric data at rest and in transit.
5. Limit the access to the biometric data. If you must distribute the biometric data to a third-party vendor, carefully and concisely craft the contract with that third-party vendor to clearly express the parameters surrounding the biometric data.
6. Consider storing less than 100 percent of the entire biometric dataset for an individual (i.e., only enough of the dataset to confirm an accurate match between the individual and the individual's biometric dataset to satisfy the business's need to use the biometric information).
7. Consider, when practical, having employees and customers use two-factor authentication in conjunction with biometric information. Use the nonbiometric (second factor) data to randomize the biometric information that is authenticated only when both the biometric information and the second factor are present.
8. If plaintiffs are alleging BIPA violations, courts will look for allegations that go beyond merely alleging a failure to provide notice or obtain consent and will look for specific factual allegations that constitute an actual and concrete injury as contemplated by the applicable statute(s).
9. Appropriately address your legal, statutory, obligations regarding biometric data in all of your contracts with your customers, contracts with your vendors accessing or handling biometric data for which you are the steward of that biometric data, and your employee policies/handbooks.
10. Consider the business's general commercial liability insurance coverage and whether it provides adequate coverage for BIPA risks, and how (or if) the insurance

carrier helps insureds in understanding and managing these risks.

The application of these practical pointers may vary depending on the business and applicable laws, and are not exhaustive of all the considerations regarding the use of biometric applications in business processes.

CONCLUSION

Biometric data and devices and applications that collect, process, and analyze biometric data are now, and will become even more, ubiquitous. An increasing number of businesses in a variety of industries will increasingly confront BIP issues in their business processes as they begin to realize and recognize the return on investment biometric technologies can provide to the business. The bottom line is that these businesses and their professional advisers must understand and proactively address the legal risks attendant to biometric information and the use thereof with customers, employees, and third-party vendors.
