This article has been published in
PLI Current: The Journal of PLI Press, Vol. 2, No. 2,
Spring 2018 (© 2018 Practising Law Institute),
www.pli.edu/PLICurrent.

PLI Current
The Journal of PLI Press
Vol. 2, No. 2, Spring 2018

The Cybersecurity-Biometric Privacy Tension and Evolving Litigation Defenses

Benjamin J. Byer
Davis Wright Tremaine LLP

With the rise in malicious hacking and data breaches, companies and government agencies are looking for ways to protect their data that offer more security than passwords. Because passwords are easily lost, stolen, guessed, and cracked by hackers, many companies are shifting to the use of biological characteristics that uniquely identify you, called biometric identifiers. For example, financial institutions and online retailers are developing ways to authenticate a purchase by requiring a user to take a selfie and smile, wink, or make some other gesture intended to confirm your actual presence. A stolen password could be easily reused, but faking a particular person's arbitrary facial expression is more complicated.

But along with the strength of biometric identifiers comes new risks. When hackers steal your password, you can change it. But when hackers acquire your

fingerprint or facial scan, you cannot change either. Indeed, biometric identifiers are often selected for their permanence. Many companies are investing in scanners that identify individuals based on the pattern of veins in their fingertips, rather than their fingerprints. A person's vascular identity is harder to forge than a fingerprint, and it changes less over time.

Some uses of biometric data may increase security and reduce the likelihood of data breaches, but other uses may interfere with an individual's right to privacy.

In addition to issues caused by the inability to change your biometrics, another new risk comes from the ability to collect biometric identifiers surreptitiously. When a website or company asks for your password, you actively decide whether or not to share it. But some biometric identifiers can be collected from cameras or microphones without your knowledge or consent. Thus, although some uses of biometric data may increase security and reduce the likelihood of data breaches, other uses may also interfere with an individual's right to privacy. More and more states are therefore regulating the use and collection of biometric data.

State Regulation of Biometric Identifiers

In 2008, Illinois enacted a biometric privacy law.[1] In 2009, Texas followed with its own.[2] And in 2017, Washington became the third state with an active biometric privacy law.[3]

Illinois's Biometric Information Privacy Act (BIPA) sits on one end of the spectrum by offering the greatest protection for a consumer's biometric information. BIPA governs the collection, storage, and use of biometric information, requiring notice and written consent before a person's biometric information is collected.[4] BIPA also prohibits private entities from selling biometric informa-

tion, restricts the disclosure thereof, and requires reasonable care be taken in storing or transmitting biometric identifiers/information. BIPA allows any "person aggrieved" by a statutory violation to sue for the greater of either actual damages or "liquidated damages" of $1,000 for a negligent violation or $5,000 for an intentional or reckless violation.[5]

In contrast, Washington's statute sits on the opposite end of the spectrum and is less restrictive. Under the Washington statute, a company (or individual) may not "enroll biometrics in a database for a commercial purpose without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of the biometrics for a commercial purpose." The statute requires either notice, consent, or a mechanism to prevent the subsequent use of the biometrics for a commercial purpose. The exact notice and type of consent required is context-dependent and need not be written. Unlike BIPA's required written consent, this provision of the Washington statute potentially allows a brick-and-mortar business to obtain your consent orally or over the phone.

To "enroll" means to capture a biometric identifier of an individual, convert it into a template, and store it in a database that matches the biometric identifier to a specific individual. If an entity does not enroll biometric information in exactly this way, the Washington statute does not impose its notice and consent requirements.

But, importantly, the Washington statute regulates commercial use of biometrics. Namely, it imposes its requirements on entities only when they enroll biometric identifiers in a "commercial database" and prevents the subsequent use of the biometrics for a "commercial purpose." The statute expressly allows entities to use biometric identifiers for security purposes. Indeed, the statute broadly defines these permitted security purposes to include preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value, including tangible and intangible goods, services, and other purposes in furtherance of protecting the security or integrity of software, accounts, applications, online services, or any person.

One of the key differences between BIPA and Washington's statute is the means of enforcement. The Washington statute lacks a private right of action, preventing aggrieved individuals from filing suit. Instead, it may be enforced solely by the attorney general. In contrast to the Washington and Texas statutes, the Illinois biometric privacy law allows consumer suits and has thus generated numerous class action lawsuits around the country.

The protections and restrictions of Washington's biometric privacy statute reflect a balancing of consumer privacy rights against the added security that using biometrics can provide. The statute attempts to strike this balance by preventing unwanted commercial use of biometric identifiers while allowing companies more freedom when using biometrics to secure data or transactions.

The Texas statute sits somewhere in the middle. It includes strict procedural rules that more closely track Illinois's BIPA, but lacks a private right of action, much like Washington's statute.

Biometric Privacy Litigation

The private right of action BIPA provides has created a recent wave of class action lawsuits. Plaintiffs have focused on alleged failures to comply with BIPA's notice and consent procedures. Because neither the Washington nor the Texas statute provides a private right of action, these statutes remain largely untested.

The BIPA class action plaintiffs have brought lawsuits primarily addressing the use of two technologies: (1) alleged improper use of facial recognition technology in photographs uploaded to a website, and (2) alleged improper collection and use of fingerprints. Suits alleging improper use of facial recognition software have focused on social media and photo-sharing websites. For example, multiple lawsuits in the U.S. District Court for the Northern District of California target Facebook's facial recognition software that tags people in photos.[6] Those plaintiffs claim they are entitled to compensation because Facebook did not receive informed consent from everyone in the photos users uploaded. These suits have raised issues for photos of users who have agreed to Facebook's end user agreement and for photos of individuals who have not joined Facebook. Shutterfly and Snapchat have also been accused of similar violations.[7]

Many complaints have also alleged that companies failed to obtain informed written consent before collecting an individual's fingerprints. These complaints often center on employers using fingerprint scanners to control when employees clock in and clock out, or to control admission such as for members of a gym.[8] For example, United Airlines and McDonalds have both been accused by employees claiming that their fingerprint-based timekeeping and employee-tracking systems collected their biometric data without the required notice and consent.[9] For larger employers, the available damages may be staggering. Even if plaintiffs

cannot demonstrate intentional violations of BIPA (which would raise the penalty from $1,000 per violation to $5,000) and the company committed only one "violation" with respect to each individual, the exposure builds quickly.

Defenses to Biometric Privacy Litigation

Biometric privacy litigation is a rapidly changing landscape. As plaintiffs have brought more cases, courts have addressed the potential defenses and changed the playing field. Two principal defenses have emerged to a lawsuit alleging a BIPA violation: the plaintiff lacks standing and the plaintiff is not sufficiently aggrieved.

First, BIPA defendants may argue that the "harm" suffered by the plaintiffs is too abstract or immaterial to give rise to Article III standing under the Supreme Court's ruling in *Spokeo v. Robins*.[10] Spokeo was a website operator that compiled consumer data to build individual consumer profiles containing details about a person's life. Spokeo sold this information to businesses seeking to learn about prospective employees. Thomas Robins accused Spokeo of violating the Fair Credit Reporting Act for distributing inaccurate information. Like BIPA, the FCRA provided a private right of action and generated lawsuits alleging procedural violations.

Initially, the district court held that the lawsuit should be dismissed because a violation of the statute is not sufficient harm; Robins needed to have an actual injury. The Ninth Circuit reversed, holding that Robins suffered an actual injury when Spokeo violated his statutory rights. The Supreme Court weighed in and held that "a bare procedural violation [of a federal statute], divorced from any concrete harm," does not suffice to "satisfy the injury-in-fact requirement of Article III."

Although *Spokeo* did not involve biometrics, it raised an important question: Does an individual need to show actual harm to bring a lawsuit for failing to comply with the procedures described in a biometric privacy law? Courts have since begun applying *Spokeo* to biometric privacy litigation. For example, *McCollough v. Smarte Carte, Inc.*[11] addressed Smarte Carte's operation of fingerprint-keyed lockers at Chicago's Union Station. The plaintiff alleged the locker provider did not first obtain written consent. The defendant moved to dismiss the claim, arguing plaintiff had failed to allege an actual and specific injury. The court agreed,

holding that a procedural violation of BIPA was insufficient to grant standing without a showing of an actual injury.

But not all courts have dismissed BIPA lawsuits that did not allege specific adverse effects. For example, *Monroy v. Shutterfly, Inc.* found that "[a]lthough the question is a close one, the court ultimately is not persuaded."[12] The court instead held that "nothing in BIPA makes recovery dependent upon a showing of 'adverse effects.'" The court concluded that "collecting, storing, and using [the plaintiff's] biometric identifiers and biometric information . . . violated the right of [plaintiff] to privacy in their biometric identifiers and biometric information."[13] *Shutterfly* distinguished cases like *Smarte Carte* by noting that the harm alleged in those cases was the defendants' failure to provide certain disclosures, while the harm Monroy alleged was that "he had no idea that Shutterfly had obtained his biometric data in the first place."[14]

Similarly, *Patel v. Facebook*[15] recently addressed plaintiffs' claims that Facebook's use of facial recognition software to recommend people to tag in uploaded photos violated BIPA because Facebook did not first obtain consent. The U.S. District Court for the Northern District of California found that the BIPA statute itself "leave[s] little question that the Illinois legislature codified a right of privacy in personal biometric information" and determined "that a violation of BIPA's procedures would cause actual and concrete harm." As a result, a violation of "BIPA necessarily amounts to a concrete injury." Like *Shutterfly*, *Facebook* distinguishes cases finding a lack of concrete injury because in those cases "the plaintiffs indisputably knew that their biometric data would be collected before they accepted the services offered by the businesses involved."

But even if a plaintiff has standing, a defendant may also argue that the plaintiff is not "aggrieved by a violation of" BIPA. Recently, an Illinois state court of appeals found that a "plaintiff who alleges only a technical violation of the statute without alleging *some* injury or adverse effect is not an aggrieved person under . . . the Act."[16] That injury or adverse effect, however, "need not be pecuniary" to create an aggrieved party. Unlike the plaintiffs in *Facebook* and *Shutterfly*, where the courts found an Article III injury to privacy rights, the plaintiff in *Six Flags* knew his biometric information was being collected. *Six Flags*, therefore, did not address whether a violation of one's right to privacy—inherently—also creates a

party "aggrieved" by a violation of BIPA. Until courts directly address this question, the extent to which *Six Flags* and the definition of "aggrieved" create an additional hurdle for a plaintiff remains unclear.

Conclusion

Although just one state has a biometric privacy statute enabling consumer lawsuits, courts across the country have been enforcing BIPA. This rapidly developing area of law therefore requires all companies intending to collect and use biometric identifiers to proceed carefully. To minimize the likelihood of a lawsuit, companies with nationwide activities should ensure that they comply with BIPA. They should obtain user consent, allow users to request their information be removed, and proceed cautiously before sharing biometric information with third parties.

But companies should not treat all uses of biometric identifiers equally. Some commercial uses of biometrics create delicate consumer privacy issues, while other uses may ultimately help secure a consumer's privacy. Rather than reflexively shying away from any use of biometrics and the added security they can provide, companies should be proactive in recognizing the regulatory risk and the security benefits. Assessing the use of biometric information and implementing internal rules governing its use allow a company to reap the security rewards while minimizing litigation risk.

Benjamin J. Byer is a partner at Davis Wright Tremaine LLP, where his practice focuses on litigation involving patent infringement claims and cybersecurity, including biometric privacy, the Computer Fraud and Abuse Act, and related trade secret misappropriation and copyright infringement claims. He litigates before trial and appellate courts nationwide and has a diverse technical background that includes electrical engineering, computer architecture, and atomic physics research. Mr. Byer is on the faculty of PLI's Nineteenth Annual Institute on Privacy and Data Security Law. A version of this article is published in the course handbook for that program.

NOTES

1. 740 Ill. Comp. Stat. 14/1 *et seq.*
2. Tex. Bus. & Com. Code Ann. § 503.001.
3. H.B. 1493 (Wash. 2017).
4. 740 Ill. Comp. Stat. 14/15(a), (b).
5. *Id.* 14/20.
6. Licata v. Facebook, Inc., Nos. 3:15-cv-03748, 3:15-cv-03749, and 3:15-cv-03747 (N.D. Cal. 2015).
7. *See* Class Action Complaint, Norberg v. Shutterfly, Inc., No. 1:15-cv-5351 (N.D. Ill. June 17, 2015); Martinez v. Snapchat Inc., No. 2:16-cv-05182 (C.D. Cal.).
8. Knobloch v. Chicago Fit Ventures LLC, No. 2017-CH-12266 (Ill. Cir. Ct. Sept. 8, 2017); Howe v. Speedway LLC, No. 2017-CH-11992 (Ill. Cir. Ct. Sept. 1, 2017); Fields v. ABRA Auto Body & Glass LP, No. 2017-CH-12271 (Ill. Cir. Ct. Sept. 8, 2017).
9. *See, e.g.*, McDonald's Biometric Information Lawsuit, www.mcdonaldslawsuit.com (last visited Apr. 9, 2018).
10. Spokeo v. Robins, 136 S. Ct. 1540 (2016).
11. McCollough v. Smarte Carte, Inc., 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016).
12. Monroy v. Shutterfly, Inc., 2017 WL 4099846, at *8 (N.D. Ill. Sept. 15, 2017).
13. *Id.* at *9.
14. *Id.* at *8 n.5.
15. Patel v. Facebook, 2018 WL 1050154 (N.D. Cal. Feb. 26, 2018).
16. Rosenbach v. Six Flags Entm't Corp., 2017 WL 6523910, at *4 (Ill. App. Ct. Dec. 21, 2017).