Sensitive to the Touch

The Evolution of U.S. Biometric Privacy Law

By Niya T. McCray, CIPP/US

Although the legislative horizon still remains murky in some states, others have taken up the helm and pioneered the cause for effecting comprehensive biometric-data privacy legislation.

Biometric technology is a gold mine, but for whom? With biometric legislation in flux and class action plaintiffs in a mad dash toward the courthouse, the contours of biometric data are still yet to be decided. Meanwhile, commercial entities, preparing for the uncertain, are battling policy providers for clear determinations of whether their current commercial general liability (CGL) policies will provide coverage in the event of liabilities arising from cyber-related incidents. Biometrics is the wave of the future… and the source of present confusion.

(Eye)Scan, uScan

By now you have no doubt seen countless articles, blog posts, and commentaries—admittedly, some that I have authored—speaking to the flood of legislation and litigation arising due to growing concerns over biometric privacy. An increasing number of vendors, employers, and businesses—both large and small—are incorporating biometric data into their daily operations as mechanisms to streamline their systems, to prevent timekeeping fraud, and to bolster the strength and integrity of their operational security. However, in their quests to become more efficient and to gain a greater competitive edge, these entities have failed in one regard: understanding the larger implications that biometric technology will undoubtedly have in litigation, legislation, and daily life.

Biometric data, for those of us unversed in cyber talk, is the measurable physical and behavioral characteristics that allow the establishment and verification of a person's identity. Some of the most common biometrics used are fingerprints, retinal scans, facial recognition (think of your iPhone X), and voice recognition. This list is in no way exhaustive, but it gives you a sneak peek into just how invasive biometrics can be. Because this data is so unique and intrinsically linked to each individual, companies have begun to appreciate it for its immense value. Companies collect it, extract data points from individually submitted samples, and from that point forward, compare every future scan with the original scan to make sure that their employees and customers are who the data says that they are.

■ Niya T. McCray, CIPP/US is an attorney in Bradley Arant Boult Cummings LLP's Birmingham, Alabama, office. She is an ANSI-certified Information Privacy Professional-United States private sector law and is currently an associate in the Business Litigation and Cybersecurity & Privacy Practice Groups. Ms. McCray serves on the 2018 DRI Cybersecurity Seminar Planning Committee as the manuscript chair. She is also a member of the International Association of Privacy Professionals and TechBirmingham.

At first glance, biometrics seems like a win: there's only one you, and unless someone is a modern-day 007 and can somehow perfectly duplicate every ridge, every contour, every detail on your finger, a fingerprint scan is truly a quick and painless way of proving your identity. But what happens, however, when biometric data is breached by malicious sources? If a hacker steals your credit card information, your credit card company will immediately send you a new card, close the compromised one, and work with you to restore any losses that you suffered. In contrast, if a hacker steals your fingerprint scan or your facial recognition data, who do you ask for a new face, a new fingerprint, a different voice pattern? These unanswerable questions are but a few of the driving factors behind the legislation and litigation springing forth from the biometric data surge.

In efforts to keep pace with this runaway train, a handful of states have already jumped onto the tracks, proposing or passing laws that attempt to define acceptable collection, retention, and destruction practices for biometric data. Nevertheless, as legislators, consumers, and businesses are discovering, the implementation of biometric technologies has far overtaken comprehension of them. While the legislative horizon still remains murky for some states, there are only a select few—Illinois, Washington, and Texas—that have courageously (depending on who you ask) taken up the helm and pioneered the cause for effecting comprehensive biometric-data privacy legislation.

Big Law on the "Prairie": Illinois' BIPA

Who would have guessed that the first state to ban traveling elephant acts would also be the first state to tackle the untamable circus of biometric privacy? *See* Senate Bill 1342; 740 Ill. Comp. Stat. 14/1. In 2008, Illinois became the first state to enact a law: the Biometric Information Privacy Act (BIPA). The act set forth a comprehensive system of rules aimed at better controlling the commercial entities that chose to collect consumer biometric data. Specifically, lawmakers touted BIPA as a means of regulating the "collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 Ill. Comp. Stat. 14/5(g).

It would appear that consumer secrets—or at least consumers' biometrics—are safe with BIPA. Notably, BIPA prohibits private entities from collecting biometric data without first providing notice to the individual *and* obtaining informed consent via a written release. 740 Ill. Comp. Stat. 14/15(b). The Illinois law also safeguards biometric data by explicitly prohibiting commercial profiteering from the information—selling, leasing, or trading it. 740 Ill. Comp. Stat. 14/15(c)-(d). Moreover, BIPA mandates that collecting entities adhere to strict guidelines for both protecting and storing biometric information, namely that biometrics be stored in at least the same manner as other confidential information and that entities develop clear, articulated policies to address the retention and destruction of biometrics. 740 Ill. Comp. Stat. 14/15(a), (e). The best part of BIPA, from the consumer's view, is that it offers a private right of action for those alleging biometric data privacy violations. Under BIPA, an affected individual could potentially recover $1,000 for each negligent violation and upwards of $5,000 for any violation deemed willful or reckless.

The Uptick in Illinois BIPA-Related Litigation: All Harm Doesn't Hurt?

From early September 2017 through December 2017, droves of entities—at least 50 that we know of—were affected by the filing of class action suits claiming violations of Illinois' BIPA. The majority of suits were brought by employees, alleging that the implementation of fingerprint scanning to streamline employer timekeeping systems violated BIPA's notice, consent, and disclosure requirements. A few suits were instituted by consumers against commercial entities, alleging that similar biometric data—ranging from fingerprints to facial scans—were collected during transactions in contravention of BIPA's safeguards. At the heart of each suit was a general sense of uncertainty; no one knew for sure exactly where the line was to be drawn between "enough" and "too much" under the act.

At the onset of the BIPA litigation, it appeared that the private right of action would be a plaintiffs' boon. Businesses braced themselves for the unforgiving wave of suits that seemed certain to follow. However, in a surprising turn of events, a December ruling from the Illinois Appellate Court chilled the breadth of plaintiffs' rights relative to BIPA's private cause of action. In *Rosenbach v. Six Flags & Great America*, 2017 IL App (2d) 170317, the plaintiff alleged that the defendant failed to obtain verifiable written consent and to disclose its policies for the collection, retention, and destruction of consumer biometric data—fingerprints—in connection with season pass purchases. The plaintiff, however, did not allege any actual injury; rather, the plaintiff claimed that if she had known of the defendant's practices, she would not have allowed her son to purchase the season pass. The Illinois Appellate Court homed in on the "aggrieved by" language in BIPA's remedy provision, Section 20, noting that BIPA was silent as pertained to the meaning of "aggrieved," and so the court looked to the plain meaning of the term. Based on such plain meaning, the Illinois court held that an "aggrieved" plaintiff under BIPA must do more than allege a technical violation of the act.

BIPA requires that there be "an actual injury, adverse effect, or harm." *See* 2017 IL App (2d) 170317. So a defendant's failure to provide notice or to obtain consent from a plaintiff before collecting biometric identifiers alone was not enough to meet the "aggrieved" standard under the act. While the *Rosenbach* ruling is not dispositive of the future of pending BIPA suits, it does suggest that plaintiffs may slow their rush to the courthouse in favor of more creative litigation strategies that meet the "aggrieved" standard as clarified in the case.

Ctrl+Amend+Copy…

Both Texas and Washington have mirrored Illinois' footsteps and carved out biometric policies of their own. Capture or Use of Biometric Identifier, Tex. Bus. & Com. Code Ann. §503.00; H.B. 1493, 2017 Sess. (Wash. 2017). Unlike Illinois, however, Texas and Washington bypassed the private right of action, opting to leave the litigation trigger in the hands of their respective state attorney generals. Judging from the influx of litigation that Illinois courts handled in 2017, Washington

and Texas seem to have made the better choice in that regard.

Washington's H.B. 1493, which went into effect July 2017, largely mirrors the outline as set by BIPA; however, H.B. 1493, unlike Illinois' BIPA and Texas' statute, does not include face or hand geometry scans in its protected biometric categories. Washington's H.B. 1493, in contrast to its counterparts, forgoes an expansive regulation of the capture of biometric data and instead focuses on the "enrolled"-"unenrolled" dichotomy. Under Washington's H.B. 1493, biometric identifiers are "enrolled" when an entity captures the data, converts it into a reference template, and stores it in a database, pairing the biometric data with its original owner. If an entity does not enroll biometric data in the method prescribed by Washington's H.B. 1493, the act will not impose its notice and consent requirements. Importantly, Washington's H.B. 1493 includes a broad security exception, unlike Texas and Illinois, which exempt entities that collect and store biometric data in relation to a "security purpose."

Texas' statute, Capture or Use of Biometric Identifier (CUBI), went into effect within a year of Illinois' BIPA. Tex. Bus. & Com. Code Ann. §503.00. Notably, CUBI is only applicable to biometric data captured for commercial purposes. An interesting feature of CUBI lies in its exceptions to the selling and disclosure of biometrics. There are certain exceptions that overlap with Illinois' BIPA, such as disclosures required by law; however, Texas' CUBI also includes a specific exception for "purposes of identification in cases of disappearance or death." Tex. Bus. & Com. Code Ann. §503.01. Nevertheless, although Texas' CUBI noticeably bypasses some of the hallmarks of Illinois' BIPA—*i.e.*, attorney general-filed suits in lieu of the private right of action—CUBI still manages to raise the stakes drastically with civil penalties of up to $25,000 per violation.

Following this trend, in August 2017, Delaware passed an amendment to its existing data breach notification law that became effective in April 2018. 6 Del. C. §12B-100. The amendment specifically expanded the definition of personal information to include biometric data. While this measure is in no way an attempt to tackle biometrics comprehensively, it does represent a series of introductory steps that multiple other states have taken or are currently considering. For example, in November 2017, New Jersey introduced a similar bill that was aimed at developing a comprehensive information security framework for consumer data that would include protection for biometrics. 2016 N.J. Laws A5206.

On the other hand, states such as Alaska, Connecticut, Massachusetts, and New Hampshire have chosen instead to strengthen the protection of biometric data by implementing comprehensive biometric legislation similar in scope to Illinois' BIPA. Alaska's legislature recently considered a bill that would mandate "full consent" to the collection, use, and retention of biometric data. H.B. 72, 30th Leg., Reg. Sess. (Alaska 2017). The proposed Alaska bill defines biometric data broadly as "fingerprints, handprints, voices, iris images, retinal images, vein scans, hand geometry, finger geometry, or other physical characteristics of an individual." Alaska's biometric act would follow in the footsteps of Illinois, allowing citizens a private right of action for intentional violations; for each violation, the statute would allow damages of up to $5,000. The New Hampshire legislature also contemplated a comprehensive biometric data bill that would permit a private right of action, allowing $1,000 for negligent violations and up to $5,000 for willful violations. H.B. 523, 2017 N.H. H.R., Reg. Sess. (N.H. 2017).

Connecticut's attempt at biometric legislation takes a slightly more targeted approach. The legislature previously considered a bill that would "prohibit retailers from using facial recognition software for marketing purposes." H.B. 5522, 2017 Gen. Assemb. Reg. Sess. (Conn. 2017). In 2015, Connecticut implemented Public Act No. 15-142, which strengthened safeguards for data breaches and amended the statutory definition of protected personal information to include biometric identifiers such as fingerprints, retinal scans, and voiceprints. Similarly, Massachusetts has also toyed with the idea of modifying its current statutory framework to include biometric identifiers as a subset of personal information. H.B. 1985, 190th Gen. Court, Reg. Sess. (Mass. 2017).

Can We Cover Our Behinds with Coverage Part B? Biometric Breaches and CGL Policies

It goes without saying that potential violations of state biometric privacy legislation would trigger coverage under many specialized cyber-insurance policies. However, for employers and vendors that have not yet made that investment or that are faithful to their preexisting commercial general liability (CGL) policies, Coverage B (covering personal and advertising injury) may be the only source of indemnity. Whether Coverage B will actually provide protection in instances of class action suits, though, largely depends on the year in which the policy itself was issued. Roughly four years ago, insurers—perhaps sensing the impending trends of biometric technology and cybersecurity in general—started to include exclusionary provisions, as promulgated by the Insurance Services Office (ISO). These provisions took sweeping measures to bar coverage in instances of data breaches and other cybersecurity-related incidents.

Businesses braced themselves for the unforgiving wave of suits that seemed certain to follow. However, in a surprising turn of events, a December ruling from the Illinois Appellate Court chilled the breadth of plaintiffs' rights relative to BIPA's private cause of action.

Specifically, the ISO created several methods, in effect, to vanquish data and

cybersecurity coverage under traditional CGL policies, mainly removing coverage for personal and advertising injuries derivative of privacy violations, removing coverage for bodily injuries related to cybersecurity incidents, and in some cases, removing both forms of coverage altogether. The Insurance Services Office's exclusionary endorsement provides that

An ounce of prevention is worth several pounds of cure: get covered, understand your coverage, and stay covered at all costs.

Coverage B is inapplicable to injuries "arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information." ISO Form CG 21 07 05 14 (2013). Traditionally, businesses could rest assured that CGL policies would cover some or all of the liabilities arising from third-party allegations of privacy violations. However, the ISO's exclusionary endorsement deprives entities of protection from the litany of expenses that accompany data breaches—specifically, the cost of notification, credit monitoring, forensics, data recovery, and public relations.

Despite the ISO's targeted exclusions, all hope is not lost. Companies facing liability for cyber-related incidents may still be able to secure coverage if an incident occurred over a period of several years, potentially seeking coverage under an earlier version of their CGL policy that did not include the cyber-exclusion endorsement. Still, the development of separate cyber-insurance policies that specifically address potential data breach and cybersecurity liabilities makes it far less likely that companies can use this backward-looking solution. Regardless, the onus falls on policyholders to understand the scope of their policies, CGL or otherwise.

According to the Ponemon Institute's "2017 Cost of Data Breach Study: Global Overview," businesses have as high as a one in four chance of suffering from a data breach attack. No business is immune, and with expenses rising into the millions for even "small" data incidents, it pays to be covered. With insurers scrambling to exclude cyber claims from traditional CGL policies, businesses would do well to purchase cyber-insurance policies, which position them to win—or at least not to fail so miserably—in the face of data incidents. Moreover, policyholders should still review cyber-insurance policies for definitions and language that precludes coverage arising from biometric data incidents, given that traditional iterations of "confidential information" have not been broad enough to encompass fingerprints, facial scans, or voice recognition. An ounce of prevention is worth several pounds of cure: get covered, understand your coverage, and stay covered at all costs.

I'm Not Touching You… What to Expect in the Future

Biometric technology and the data germane to it are boldly going where no man has gone before. No one—policymakers, policy providers, or policyholders—are finding themselves able to keep pace with this behemoth. To date, only one-fifth of the states have actively contemplated or passed some form of legislation that addresses best practices for handling, collecting, storing, and terminating biometric data. Still, Illinois—thanks to BIPA's private right of action—is the only state that has allowed its courts to enforce biometric laws for consumer-claimants. As the appellate court illustrated in *Rosenbach*, however, Illinois plaintiffs alleging violations will likewise have to demonstrate some actual harm to support their complaints. While the *Rosenbach* ruling may have delayed things in the Prairie State, there is still the possibility that plaintiffs will get more creative in alleging harms, allowing anxious spectators to get a better idea of how biometric suits will unfold in full-blown litigation. It is also just as likely that plaintiffs in Washington or Texas or Alaska (as it attempts to pass its own biometric legislation) will incite their own attorney general to fight on their behalf. To say that the litigation horizon is unclear is a vast understatement. What is clear, though, is that the torrential downpour of class action suits under Illinois' BIPA is only the beginning of the battle for biometrics.

In addition to all this, as courtroom diatribes rage on in one jurisdiction or another, businesses themselves may awaken in a fight for their own protections under traditional and specialized insurance policies. Data incidents have been on the rise for years; it seems, however, that the ISO was simply the first to enact "CYA" measures through the promulgation of its exclusionary endorsements. Nevertheless, while the legislature and judiciary are chiseling out the contours of biometric privacy, commercial entities and insurance providers will likewise be in a tug of war over the indemnities owed to policyholders in the event of cyber-related data incidents.

The concept of biometrics is like clay; even at this moment, it is being shaped and molded in ways that we may not comprehend for years to come. It would be remiss to discount the staying power, the convenience, and the absolute value that biometric technology now has in our everyday lives. American infrastructure has become less reliant on things that we have (keys, credit cards) and know (passwords), and instead turned its attention to those things that we *are* (biometrics such as fingerprints, facial scans, eye scans, and vocal recognition). Across the board, consumers and business entities alike are on a quest to find security, to safeguard those thoughts and memories of things that speak to the very core of who they are, whether they are personal or commercial.

The only way to "tame"—if that's even possible—the specter of biometric technology is to understand and respect it. Now is the time for our legislators and members of the judiciary to match the pace of industry before they find themselves, and us, left in an antediluvian darkness. Biometric technology is both the present and the future; our understanding of life, laws, and legislation must adapt to it. FD