NOW PLAYING: THE PALMISTRY OF BIOMETRIC DATA PRIVACY LAW

M. Lynne Hewitt

Martin T. Tully

Long the fascination of Hollywood science fiction screenwriters, biometric technology is now a routine part of modern life. Depictions of facial recognition technology, which is now commonly used to unlock our phones, can be found as early as the mid-60s on *Star Trek: The Original Series*—a TV show long credited as an inspiration for technology development. The voice recognition technology envisioned in 1968's *2001: A Space Odyssey* is the backbone of today's virtual assistants, such as Alexa and Google Assistant. And the fingerprint scanning technology that we now encounter daily was foreshadowed in *Diamonds are Forever* when James Bond (played by the superior Sean Connery) used a latex fingerprint to beat a rudimentary scanner to convince jewel thief Tiffany Case (the first American Bond girl, played by Jill St. John), that he is indeed the diamond smuggler she's looking for.

Biometrics are no longer the stuff of spy stories and science fiction movies. Whether through the utilization of smartphones, which employ fingerprint and facial scans for security, a visit to the pharmacy, which uses fingerprint scans to access databases holding patient information, or law enforcement's reliance on everything from fingerprints to DNA to facial recognition to solve crimes, biometrics are ingrained in our daily life. Ever turn yourself into a cat on Zoom? That is facial recognition technology. But what happens to all this biometric data being collected, and are we at increased risk for creating and using it?

In 2020, 47% of Americans experienced financial identity theft totaling $712.5 billion in losses, up 42% over 2019 (LINK). If your social security number is stolen, you can have a new one issued. Email hacked? You can change the password to something more complicated than "password" or "123456." What happens, however, if someone steals your biometric data—the very essence of who you are? You cannot change that so easily.

Coming Soon to a Legislature Near You: The Current State of Biometric Data Privacy Legislation

As of February 2022, nine states – Washington, California, Colorado, Texas, Arkansas, Illinois, Virginia, Maryland, and New York – and the city of Portland, Oregon have enacted

laws governing how private entities use and store biometric information, and 22 states are contemplating similar laws. These laws govern a range of activities related to the collection, storage, use, and selling of biometric information. Many require disclosure and consent for the collection of this data. Illinois' Biometric Information Privacy Act ("BIPA"), in particular, has been at the forefront of biometric privacy laws. BIPA was enacted in 2008 in response to the Illinois General Assembly's finding that the use of biometric information was increasing, particularly in financial transactions, but with little appreciation by the legislature for all that it signified for the future. The Illinois BIPA differs from all other states' laws in that it provides recourse for private individuals to file lawsuits on their own behalf for alleged violations rather than limiting enforcement authority to the state attorney general. This difference has had significant practical consequences and is precisely why Illinois' law continues to make headlines. It should be noted, however, that of the 22 states contemplating new biometric privacy legislation, three have sought to follow Illinois' lead. Maryland's Biometric Identifiers Privacy Act bill (H.B. 259), West Virginia's BIPA (H.B. 2064), and Florida's H.B. 9 include a provision for a private right of action. And in August 2020, Oregon Senator Jeff Merkley introduced S.4400, the National Biometric Information Privacy Act, which is very similar to BIPA and similarly includes a private right of action.

Fade In: What is BIPA?

Illinois' BIPA sets standards for how organizations are required to manage biometric data of Illinois consumers. The statute notes that, unlike other personal identifiers that can be changed when compromised, biometric identifiers are biologically unique to the individual. Once compromised, there is little recourse; thus, an individual is said to endure a much higher consequence if they suffer identity theft related to their biometric identifiers.

While BIPA has been in effect for over a decade, it has newly risen to prominence as a result of several recent court decisions that have made it easier to maintain BIPA suits. For example, in *Rosenbach v. Six Flags Entertainment Corp* (2019), the Illinois Supreme Court held that the plaintiff did not have to allege an actual injury to be considered an "aggrieved person" to have standing under the statute and "be entitled to liquidated damages and injunctive relief." The U.S. Court of Appeals for the Seventh Circuit provided more clarity in *Bryant v. Compass Group USA, Inc.*, holding a person merely alleging violation of BIPA has suffered an injury-in-fact sufficient to support standing under BIPA Section 15(b). This reversed the district court's ruling that Compass's alleged violations were bare procedural violations that caused no concrete harm to Bryant. The Court, in its opinion, stated, "Compass did not make the requisite disclosures to Bryant or obtain her informed written consent before collecting her fingerprints," and that

failure "inflicted the concrete injury BIPA intended to protect against, *i.e.*, a consumer's loss of the power and ability to make informed decisions about […] her biometric information."

Since being rebooted, lawsuits under BIPA have hit some organizations harder than Godzilla. In one high-profile example, Facebook settled *Patel v. Facebook, Inc.* in 2020 for $650 million in one of the largest consumer privacy settlements in U.S. history. The suit alleged Facebook collected user biometric data without consent (a key provision in the BIPA statute). Currently, several major class actions suits are pending in Illinois concerning the collection of biometric data. All these suits come as the Illinois Supreme Court is preparing to determine how claims accrue under BIPA — a lingering issue that muddies the waters of litigation under the statute.

The Plot Thickens: Clarification of BIPA – Coming Soon to a Courtroom Near You?

Several key questions have already been answered by the Court regarding the interpretation of BIPA, but the biggest question remains—how do claims accrue under BIPA? Do damages rack up for every day a company demands an employee's fingerprint without informed consent or just the first time? This is the crucial question for the Court to answer in *Cothron v. White Castle System, Inc., et al.* and one that could have major ramifications for small businesses if the Court interprets the statute to favor plaintiffs seeking redress for alleged violations under the statute. BIPA allows for recovery of up to $5,000 per violation, so it is easy to see how this could become ruinous for organizations accused of violating the statute numerous times. On the other hand, it would also put a premium on protecting the privacy of individuals. Seeing that history often repeats itself, it is easy to think that the Court, with a history of pro-consumer BIPA rulings, will come down on the side of the plaintiffs again. But we won't know for sure until the credits roll.

The Resolution: Compliance with BIPA

To the layperson, compliance with BIPA appears relatively straightforward. But to private businesses, there are challenges to compliance, and the consequences of non-compliance have the potential to be very steep.

Compliance requires proactive effort. Information governance is already something many organizations struggle with, so it is critical to have a plan that complies with the law. If a private entity is going to collect, store, use, or disseminate biometric data, they need to give notice and obtain written consent from the individual. Private entities

cannot sell or otherwise profit from individuals' biometric data. Private entities need to maintain and subsequently destroy the data in accordance with the statute, not keeping it longer than necessary or using it for purposes other than for which it was initially collected. (This is a wise practice for other reasons, too, but that is a subject for a sequel.) And, you guessed it, private entities must have their biometric data privacy policy in writing and publicly available to consumers at the point of collection.

To Be Continued: How can Redgrave LLP Help?

Redgrave LLP's data privacy professionals have the 411 on BIPA. We can assist with establishing compliant BIPA privacy policies and advising on navigating the proper way to collect and use biometric information to avoid the harsh statutory penalties that can arise from running afoul of legal mandates. This includes data minimization best practices that comport with requirements that information not be retained longer than necessary. Think of us as the "Q" to your "007."

For additional information on this topic or further details on Redgrave LLP's Data Privacy services, please contact **Martin Tully** at mtully@redgravellp.com or at 773.782.0352 .

Redgrave LLP *is one of the largest legal practices focused exclusively on addressing the legal challenges that arise at the intersection of the law and technology, including eDiscovery, information governance, and data privacy. We employ some of the most experienced professionals in the field. We provide clients with practical, innovative, and cost-effective solutions and serve Global and Fortune 500 companies across a diverse array of industries. We also work collaboratively with Am Law 100 law firms in roles ranging from co-counsel to consulting and testifying expert witnesses and have appeared in state and federal courts throughout the United States.*