2019 Cyber, Management and Professional Liability Conference
July 10-12, 2019
Boston, MA

New Generation of Wearables & Developments in the Legal Landscape Governing Biometric Information

I. Current Regulatory Framework

Illinois Biometric Privacy Act

The Illinois Biometric Privacy Act ("BIPA"), passed in 2008, was the first of its kind. In recognition of the unique risks associated with access to biometric information, BIPA established minimum practices for the collection, use, sale, and storage of such information. BIPA features a broad definition of "biometric identifier," which includes rentina/iris scans, fingerprints, voiceprints, scan of hand/face geometry, and other information based on an individual's biometric identifier used to identify an individual. What sets BIPA apart from similar statutes in Texas and Washington is that it provides for a private right of action allowing aggrieved individuals to recover actual damages or statutory damages of $1,000 or $5,000 per violation, depending on whether the violation was intentional or reckless vs. merely negligent.

Texas Biometrics Law

In 2009, Texas became the second state to pass a law governing the privacy of biometric information. Although its definition "biometric identifier" mostly parallels that of BIPA, the Texas statute is narrower as it does not contain the catch-all language of BIPA, *i.e.*, "other information based on an individual's biometric identifier used to identify an individual." It also contains an exclusion for voiceprint data collected by financial institutions or their affiliates. Lastly, it diverges significantly from BIPA in its enforcement mechanism. Although the Texas Attorney General may bring an action against individuals and entities for violations of the statute and levy a fine of $25,000 per violation, it notably does not provide for a private right of action.

Washington Biometrics Law

The Washington statute is an interesting mix of both BIPA and the Texas statute. It features a broad definition of "biometric identifier" as data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a

specific individual. However, it specifically excludes, among other things, photos, or recordings. Like the Texas statute, although it is enforceable by the Attorney General, it does not permit consumers to bring actions for violative practices.

II. Trends in Legal Landscape

Due to the fact that the Texas and Washington statutes limit actions to those brought by the respective state's attorney general, the majority of the case law and legal trends involving biometric privacy stem from BIPA actions. In addition, even BIPA went relatively unnoticed by the plaintiff's bar until fairly recently. To that end, it took nearly eight years for companies to be able to appreciate the potential liability created by such statutes. *Sekura v. L.A. Tan Enterprises, Inc.*, Case No. 2015-CH-16694 (Ill. Super. Ct., Cook Cnty. 2016), marked the first settlement of a BIPA case, and it settled for $1.5 million for approximately 37,000 class members. It took almost another two years for a BIPA class to be certified. *See In re Facebook Biometric Information Privacy Litigation*, Case No. 3:15-cv-03747 (N.D. Cal. Apr. 16, 2018). Most recently, the Illinois Supreme Court dealt another blow to the defense bar in *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186 (Ill. Jan. 25, 2019) undercutting the standing argument that companies have relied on with varied levels of success. In *Rosenbach*, the Illinois Supreme Court ruled that a violation of BIPA, by itself, is sufficient to confer standing on a plaintiff—meaning that a plaintiff need not have suffered actual damages resulting from the violative practice to be entitled to sue. Since BIPA features statutory damages, a company's liability under BIPA can be astronomical and threaten its very existence, depending on the number of Illinois residents affected.

Very soon, companies will have another state's residents to worry about as the California Consumer Privacy Act ("CCPA") goes into effect on January 1, 2020. The CCPA governs the collection, use, sale, and storage of the personally identifiable information of California residents, including biometric information, and provides for a private right of action. The CCPA defines as iris/retina scan, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information. This definition reflects the evolution of not only lawmakers' understanding of the potential uses and misuses of biometric information but also the popularization of wearable devices and advances in wearable technology.

III. Wearables

Back in 2008, when BIPA was first passed, iPhones had just been released and wearables were not yet a thing for consumers. Sure, there were heartrate monitors but they were geared towards a very niche market and they did not allow for integration with and across multiple devices (phones, tablets, and computers). Now, wearables are ubiquitous. Also, the sheer quality and quantity of data collected and the purpose for their collection has greatly expanded. Most consumers rely on wearables to track their health, fitness, and wellness information. For example, FitBit and Apple Watch track the wearer's calories burned, heartrate, and sleep information. Other devices allow the wearer to use their biometric information as an authentication token. Due to the nature of the data collected, companies dealing with wearables and the resulting data may face liability under biometric privacy laws.

IV. Best Practices

There are measures companies can take to minimize their potential liability under biometric privacy laws. First, companies must ensure that they obtain consent before collecting or disclosing any biometric information. Consent is key. For underwriters, this means reviewing a company's terms and conditions, privacy policies, and registration process to confirm that the company is obtaining consent and making the necessary disclosures.

The second area of focus is transfer and storage. Companies should encrypt any biometric information—both during transfer and at rest—to minimize the risk of any unintended disclosures of such data. In the same vein, companies should conduct regular risk assessment of its networks and storage systems to ensure that consumers' biometric information is adequately safeguarded. For underwriters, this translates into reviewing and auditing a company's data security policies, procedures, and practices.