Updates
March 01, 2022
Rip Van Wrinkle: The Grandfather of Biometric Laws Awakens

Biometric data is becoming increasingly pervasive in our daily lives—we use it to unlock smartphones, gain entry to entertainment venues, access secured locations, and record time and attendance on the job site.

For many years, the most significant law governing biometric-based products and services has been the Illinois Biometric Information Protection Act (BIPA). Passed in 2008, BIPA is an Illinois state statute requiring private entities that collect or possess certain kinds of biometric data to comply with a range of requirements, including providing notice to and obtaining consent from consumers. BIPA is well known largely because of its private right of action, which has triggered more than 1,400 putative class actions in the last five years alone. Defendants in BIPA class actions run the gamut, from "mom-and-pop" shops to multinational corporations.

This past month, however, another biometric data privacy law woke from a long, undisturbed slumber. Texas's Capture of Use of Biometric Information (CUBI), Tex. Bus. & Com. Code § 503.001 et seq., was actually the first state law to govern the collection and use of biometric data, predating BIPA by seven years. CUBI is enforceable only by the Texas attorney general and imposes requirements similar to BIPA's. CUBI was enacted in 2001, but without a private right of action or any public enforcement activity, CUBI has not generated nearly as much attention as BIPA. However, that may change, thanks to *Texas v. Meta Platforms, Inc.*, the Texas attorney general's first action under CUBI, which alleges that Meta (f/k/a Facebook) violated CUBI in its collection and use of biometric identifiers via its photo tagging functionality.

What Is CUBI and How Does It Differ From BIPA?

Covered Data

BIPA covers "biometric identifiers," defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," as well as "biometric information," defined as "any information … based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10. Like BIPA, CUBI applies to "biometric identifiers," but CUBI defines the term differently. Under CUBI, "biometric identifier" means "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry" that is captured for a "commercial purpose." Tex. Bus. & Com. Code § 503.001(a)-(b). Also, while BIPA has a lengthy list of exclusions that narrow the otherwise broad definitions of covered data—e.g., written signatures, photographs, and human biological samples used for valid scientific testing or screening—CUBI has no similar list of exclusions. Also, unlike BIPA, CUBI does not expressly apply to "biometric information."

Broadly, CUBI prohibits the "capture of a biometric identifier" for a "commercial purpose" unless the individual

- Is informed of the capture before it occurs; and
- Consents to the capture of his or her biometric identifier.

Notably, while both BIPA and CUBI require pre-collection notice, only BIPA requires an explanation as to the specific purpose of the collection, length of time for which the data is being collected, and guidelines for data destruction.

Restrictions on Use of Biometric Data

Under CUBI, a private entity that collects covered biometric data that is captured for a commercial purpose "may not sell, lease, or otherwise disclose" the data except in very limited circumstances, namely:

- The individual has provided consent "for identification purposes in the event of the individual's disappearance or death,"
- The disclosure is necessary to complete a financial transaction that the individual requested or authorized,
- The disclosure is required or permitted by a federal or state law (other than the Texas public information laws), or
- Disclosure is made by or to law enforcement for a law enforcement purpose in response to a warrant.

While BIPA includes certain exemptions for specific types of information that do not fall within its scope, such as information covered by the Health Information Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLBA), CUBI only explicitly excludes "voiceprint data retained by a financial institution or an affiliate of a financial institution."

Retention and Destruction

Like BIPA, CUBI sets out parameters for retention and destruction of affected biometric data. CUBI specifically requires that biometric data be destroyed "within a reasonable time." Specifically, once the business purpose for collecting the data no longer exists, the company has one year to destroy it (with some exceptions). In addition, where biometric data is collected by an employer for "security purposes," it must be destroyed when the employment relationship is terminated. (BIPA includes similar, but not identical, retention requirements).

Safeguarding Biometric Data

Both CUBI and BIPA require entities that possess biometric data to safeguard the data. CUBI explicitly requires that the data must be stored, transmitted, and protected from disclosure "using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other confidential information."

Enforcement and Penalties

BIPA and CUBI part ways most notably with respect to how they are enforced. BIPA is enforceable through a private right of action, and BIPA litigation has been extremely active in recent years. Statutory penalties under BIPA may be as high as $5,000 per violation, even though courts are still determining how to define and count violations under the law. There have been numerous seven-digit settlements of BIPA class actions both in the employee and consumer contexts. As a likely precursor to the Texas attorney general's action, Facebook settled one of the earliest BIPA class actions last year for $650 million plus significant injunctive relief.

CUBI, in contrast, includes no private right of action. It is enforceable only by the Texas attorney general's office, but the penalties are harsh; violations may result in civil penalties up to $25,000 per violation.

What Does the Texas Attorney General's CUBI Action Portend for the Statute?

Texas Attorney General Ken Paxton has long touted his focus on regulating "Big Tech." On his website, Attorney General Paxton states that "Big Tech has controlled the online sphere for long enough" and that Big Tech has allegedly collected information without being clear to users on how it would be used. The website also notes that the attorney general's office currently has four lawsuits pending against tech companies. The attorney general's focus on Big Tech comes as the tech market has exploded in Texas. Companies like Tesla, Samsung, Facebook, and many others have increased their footprint dramatically in Texas over the past decade, including in Austin and the Dallas-Fort Worth Metroplex.

The attorney general's new suit—again, the first public enforcement action under CUBI—opens a new and significant chapter in the attorney general's increased regulatory scrutiny of so-called Big Tech. The attorney general's complaint specifically alleges that Meta's Facebook, along with related social media website Instagram, used its "tagged" and "tag suggestion" features to "unlawfully capture the biometric identifiers of Texans," including both Facebook users and nonusers, "for a commercial purpose without their informed consent, disclosed those identifiers to others, and failed to destroy collected identifiers within a reasonable time." The complaint further alleges that Meta captured biometric information from Texan users' phones and videos without their permission and then, "unbeknownst to users," disclosed that information to others, including "other Facebook subsidiaries and related entities." Further, the complaint alleges that Meta failed to destroy biometric data within a reasonable time, thereby "exposing Texans to ever-increasing risks to their well-being, safety, and security." According to the attorney general, that alleged conduct violated both CUBI and the Texas Deceptive Trade Practices Act (DTPA). The attorney general therefore seeks injunctive relief, statutory penalties of $25,000 for each allegedly unlawful capture of a biometric identifier under CUBI (and additional statutory fines for each violation of DTPA), as well as attorneys' fees and costs. Meta has not yet responded publicly to the complaint. The attorney general's allegations are very similar to the allegations in the BIPA litigation previously settled by Facebook.

Early Takeaways From the Attorney General's Litigation

The litigation may portend more aggressive enforcement of CUBI going forward and sheds some light on the attorney general's interpretation of CUBI. For example:

- A broad interpretation of "commercial purpose." CUBI does not define the term "commercial purpose." The complaint alleges violations of CUBI based on alleged internal uses of biometric identifiers to train internal algorithms and improve product features. The attorney general does not allege specific financial gain through use of biometric identifiers.
- CUBI notice and consent requirements might be satisfied through terms of use or privacy policy disclosures. The attorney general alleges that Texans were not informed of the capture of their biometric identifiers, and the allegations suggest that disclosure of biometric identifier collection in some written

form (such a privacy policy or terms of service) would have satisfied the notice component of CUBI to users.
- Sharing biometric identifiers with affiliates or subsidiaries may lead to allegations of violating CUBI's disclosure restrictions. The attorney general's allegations are based in part on sharing of biometric identifiers with Facebook's own affiliates.

CUBI Risk Mitigation

Although we are in the early days of CUBI enforcement, the attorney general's suit shows that companies can no longer assume that CUBI will remain a paper tiger. Mitigation strategies to consider include the following:

- Review privacy policies and terms of service to confirm that appropriate disclosures are made concerning the collection of biometric identifiers and to better align with CUBI's notice and consent requirements.
- Where biometric identifiers are collected or captured, have a defensible method of showing that the CUBI notice and consent requirements were satisfied.
- Strictly limit (or, even better, prevent) any connection between data that could be deemed to satisfy CUBI's definition of "biometric identifiers" and other identifying information such as name or account.
- Limit any sharing of biometric identifiers, including sharing with any subsidiaries or affiliates, to the type of sharing allowed under CUBI.

Perkins Coie's Biometric Privacy Practice

Companies with questions regarding BIPA, CUBI, or other privacy laws should seek experienced counsel. Perkins Coie attorneys have been litigating cases involving biometric privacy and helping companies minimize risk under biometric privacy laws for over a decade. For more information please contact one of our biometrics professionals or one of our privacy attorneys in Dallas or Austin.

Authors

Explore more in

Litigation Privacy & Security Retail & Consumer Products

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality’s Voter ID Law