King & Spalding
Client Alert

MARCH 15, 2022

For more information, contact:

Thomas Ahlering
+1 312 764 6949
tahlering@kslaw.com

Andrew Cockroft
+1 312 764 6917
acockroft@kslaw.com

King & Spalding

Chicago
110 N Wacker Drive
Suite 3800
Chicago, IL 60606
Tel: +1 312 995 6333

All Eyes on Texas After Filing First Enforcement Action Under State's Biometric Privacy Law

Series 2, 10 in 10: Issue 8

The Attorney General for the State of Texas recently filed suit against Meta (formerly Facebook) alleging that the company violated the Texas Capture and Use of Biometric Identifier Act ("CUBI") and the Texas Deceptive Trade Practices-Consider Protection Act ("DTPA") by collecting the biometric information from Texas residents without their consent through photos uploaded to Facebook. Despite the law being on the books since 2009, this is the first time the State of Texas has brought an action to enforce CUBI. While it is too early to tell if this action is a sign of future enforcement actions in Texas, businesses should be aware of potential liabilities even in states without a private right of action and implement general best practices relating to biometric privacy.

OVERVIEW OF CUBI

Under the CUBI, a private entity may not capture a person's biometric identifier—defined as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry"—for "a commercial purpose" unless the entity informs the person prior to capturing the biometric identifier and receives the person's consent to the collection. Once an entity is in possession of the biometric identifier, the entity:

- may not sell, lease or otherwise disclose the identifier unless they receive consent from the person from whom the identifier was collected or if the disclosure completes a financial transaction, is required or permitted by a federal or state statute, or is made by or to a law enforcement agency in response to a warrant;
- must use reasonable care in storing, transmitting and protecting the biometric identifier from disclosure; and

- must destroy the biometric identifier within a reasonable time following capture, but no later than one year after the purpose of collection has expired.

The CUBI provides for a civil penalty up to $25,000 for "each violation," and is enforceable only by the Texas Attorney General.

KEY DIFFERENCES WITH OTHER BIOMETRIC PRIVACY LAWS

CUBI shares some important features with other biometric privacy laws like Illinois' Biometric Information Privacy Act ("BIPA"). Both laws prohibit the collection and transmission of biometric identifiers without a person's consent and both place retention and destruction obligations on entities in possession of biometric identifiers. Likewise, both statutes carry potentially significant penalties.

However, there are important differences including the following:

- CUBI restricts the capture of biometric identifiers, but not information "derived" from the identifiers. BIPA, on the other hand, is concerned with a broader set of information including anything "based on" an individual's biometric identifier.
- CUBI requires only that the entity obtain "consent" from the person prior to capturing their biometric identifier, whereas BIPA specifically requires "written consent."
- CUBI only restricts the capture of biometric identifiers for a "commercial purpose," whereas BIPA restricts all collections or capture of biometrics with only limited exceptions, like collections for payment, treatment or operations under HIPAA or collections by a financial institution subject to the Gramm-Leach-Bliley Act.
- CUBI may only be enforced by the Texas Attorney General, whereas BIPA may be enforced by any individual "aggrieved by" a violation of BIPA.

OVERVIEW OF THE PETITION

The State of Texas alleges Meta violated the CUBI and the DTPA by collecting Texans' biometric identifiers without their consent through Facebook's "Tag Suggestions" feature. The Petition alleges that Meta used facial recognition technology to analyze the facial geometry of individuals who appeared in photos uploaded to Facebook. Specifically, the Petition claims Meta used the facial geometry data collected from photos uploaded to the website to create DeepFace, a "deep-learning facial recognition system," which was then used to transmit biometric identifiers to third-parties. The Petition asserts several causes action under the CUBI alleging collection and transmission of biometric identifiers without consent and failure to destroy identifiers within one year after the purpose for collection expired. The Petition alleges that Meta violated these respective provisions "billions" of times and, thus, seeks the statutory maximum of $25,000 for "each" violation of CUBI.

The action is unique in that it was filed after private plaintiffs obtained a $650 million settlement with Meta in a suit that advanced substantially similar allegations under BIPA. Therefore, it is unclear if the Texas Attorney General intends to file similar actions without the benefit of an existing record from a previously filed suit.

The suit also appears to be motivated by the Texas Attorney General's concern with businesses allegedly profiting from individuals' biometric data and the potential collection of minors' biometric identifiers. In announcing the suit, Attorney General Paxton said "Facebook will no longer take advantage of people and their children with the intent to turn a profit at the expense of one's safety and well-being[.]"

The CUBI has yet to be interpreted by courts and businesses should continue monitor any further enforcement activity.

CONCLUSION

Companies should implement general best practices relating to biometric privacy as the use of biometric technology grows and additional states push for biometric privacy laws in the absence of a uniform federal law.

- **Analyze Existing Technologies to Determine Whether Biometrics are Collected.** Audit existing technologies to assess whether, when and how biometrics are being collected and in what jurisdictions.
- **Provide Notice of Collection and Obtain Consent.** If utilizing biometric technology, provide notice and obtain consent prior to capturing biometrics.
- **Establish a Written Policy.** Develop a policy establishing retention and destruction limits and make it publicly available.
- **Ensure That Biometric Data Is Not Sold or Disclosed**. Ensure that the company, nor any third-party, sells or discloses biometrics and does not use the biometric data for any purpose outside of which consent was obtained.
- **Establish Protocols for Protecting Biometrics**. Protect biometrics in the same manner as other confidential and sensitive information in its possession.
- **Ensure Compliance with Applicable Data Breach Notification Statutes If Biometric Data Is Compromised**. Follow the requirements of data breach statutes with regard to informing affected individuals of breaches/suspected breaches—particularly where state law includes biometrics within the definition of personal information subject to security requirements.
- **Continue to Monitor Legislative Developments**. Stay abreast of developments in various jurisdictions to avoid running afoul of any pending or new laws.