WINSTEAD

Businesses, Technology, and the Law

03.19.18

Technology has changed the way we interact, shop, work, and relax. Advances in biometrics now help us login to our computers, phones, apps, and even open doors. Biometrics like fingerprints, retina scans, and voice and facial recognition help add a simple level of security to our interactions with electronics. For example, some businesses are now using biometric time clocks to prevent their employees from signing in for each other. However, my guess is that many Texas businesses are unaware that they have legal obligations stemming from the biometric data that they collect and retain.

Most Texas businesses that use or interact with biometric information have three basic duties:

- **Informed Consent,**
- **Protect, and**
- **Destory.**

Informed Consent.

Businesses in Texas are required to get informed consent before it captures someone's biometric data (fingerprint, image, voice, etc.). Also, Texas businesses are generally required to get informed consent before they sell, lease, or otherwise disclose of a person's biometric identifier. That means that the business should inform its employees or customers that it is capturing their biometric data, why it is being captured, and how long it will be maintained. It is also important for businesses to maintain a record of the employee's or customer's consent to the capture of the requested biometric data.

Protect.

Texas businesses are required to protect biometric data. Specifically, the law requires a business to store, transmit, and protect biometric data using reasonable care and in a manner that is equally or more protective than how the business handles other confidential information. This could involve password protection, access control, non-disclosure agreements, and/or encryption.

Destroy.

Businesses are required to destroy the biometric data within a reasonable time after the purpose of the data no longer exists. However, under Texas law generally a reasonable time is limited to no longer than one year after the data no longer serves a purpose. For employee biometric data, the law presumes that the biometric data no longer serves a purpose on termination of the employment relationship. This destruction requirement makes it worthwhile for a company to develop a document retention policy that limits the period when this data is retained and develop tracking methods to account for the end of the data's purpose.

The Cloud.

Many businesses now use third-party or cloud based data storage. These businesses may need to take additional precautions. First, the business will generally want to obtain informed consent from the employee or customer that the biometric data will be disclosed to and stored on third-party or cloud based storage. Those businesses may also want to ensure that the company, which will be maintaining the biometric data has systems in place that will adequately protect the biometric data.

Businesses (or individuals for that matter) may face penalties up to $25,000 per violation in an action by the Texas attorney general. Other states have much broader laws, which may even allow private suits for violations. Therefore, it is important to look at each of the states (or countries) wherein you operate.

Contact:

Justin Ratley
713.650.2688
jratley@winstead.com