Employers Take Note: Regulations on the Use of Biometric Data

Insights
5.09.17

The use of biometric data is continuously increasing, including in the workplace. Biometric data may include facial characteristics, hand geometry, a retina/iris scan, a fingerprint or a voiceprint. Employers often collect and use biometric data to establish records of employee hours, to restrict access to specific areas, computer systems, data or devices, to provide security and to promote employee health, including through wellness programs.

Employers who use biometrics should be mindful of regulations that impact their ability to collect, retain and use biometric data. Numerous states, including Iowa, Michigan, Nebraska, Texas and Wisconsin, have data breach notification laws that require notifications relating to the disclosure of biometric data. New Mexico is the most recent state to enact such a law. On April 6, 2017, New Mexico Governor Susana Martinez signed into law the state's first data breach notification statute which will become effective on June 16, 2017. Similar to laws in other states, New Mexico's Data Breach Notification Act addresses the security of personal identifying information ("PII"), disposal of PII, and notification of a security breach. The Act defines PII to include biometric data - an individual's "fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry that is used to uniquely and durably authenticate an individual's identity when the individual accesses a physical location, device, system or account."

In addition to data breach notification laws identifying biometric data as PII, some states have separate laws governing the collection, retention, storage, and use of biometric data. These include the Illinois Biometric Information Privacy Act, which imposes stringent notice and consent requirements relating to an entity's ability to "collect, capture, purchase, receive through trade or otherwise obtain" biometric data, and Texas Business & Commerce Code § 503.001, which offers similar protections for biometric data but does not contain a private right of action. More states are following suit. In 2017 alone, new legislation has been proposed in Alaska, Connecticut, New Hampshire and Washington that would regulate the collection, retention, storage and use of biometric data. In many ways, these proposed laws are similar to the currently existing laws in Illinois and Texas.

Laws relating to the collection and use of biometric data continue to develop and evolve. Employers who are collecting and using biometric data should be vigilant about monitoring the current state of legislation in their geographic area. To mitigate potential risks, employers should also consider:

1. Creating and regularly updating processes to inform employees about the collection, retention, storage and use of biometric data;
2. Creating and regularly updating processes to obtain employee consent to the collection of such data;
3. Drafting, regularly updating, and distributing policies to properly address the collection, retention, storage and use of biometric data;
4. Implementing and regularly monitoring the adequacy of data security systems to protect biometric data;
5. Developing and regularly updating policies to address the retention and regular destruction of biometric data.

Related People

Heather Zalar Steele
Partner
610.230.2134
Email