How BIPA May Impact Your Voice Solution & Workforce

What is BIPA?
A Biometric Information Privacy Act (BIPA) is a law that focuses on protecting biometric information, which consists of physical characteristics that can be used to identify individuals, such as fingerprints, facial recognition scans, retina scans, and voice. The purpose of this type of law is to protect individuals' biometric information from being collected, stored, or used without their informed consent.

Where does BIPA apply?
BIPA is not currently a federal regulation, but each state could potentially have its own version over time. Illinois was the first to pass such legislation in 2008. There are multiple states that have a BIPA law or have recently introduced BIPA legislation.

Why consider BIPA?
Recently, advancing litigation proceedings, rulings allowing class action lawsuits, and awarding of potential damages under BIPA enforcement are raising concerns. Please take any voice solution provided by Mountain Leverage into account when considering compliance with any BIPA laws.

How is a voice solution related to BIPA?

- During the course of business between Mountain Leverage and our customers, which may include voice-optimized workflow execution, voice data is being processed through both a voice hardware device and voice device management software.
- The software may store a voice template, but only as a range value that cannot be reverse-engineered to an operator. These templates are solely used to correspond to vocabulary that an operator is properly speaking to synchronize with the appropriate word or phrase.
- The software does not automatically delete voice operators or templates after a period of inactivity; however, once an operator profile is manually deleted, all voice templates are deleted as well.
- Customers are responsible and accountable for all voice data and for complying with any and all data privacy laws applicable to its business.

How should employers become BIPA compliant?
It is important to work with your legal counsel on how best to comply with BIPA across all applicable states. Here are 4 steps we've seen organizations take in attempt to protect themselves from a BIPA violation:

1. Obtain written consent from individuals before collecting, using, or storing biometric data.
2. Develop & publicize policies and procedures governing the handling of biometric data and limit access to authorized and trained individuals.
3. Ensure that biometric data is encrypted and securely stored, and regularly audit and monitor the use and access to biometric data.
4. Stay up-to-date on BIPA law and regulations in your jurisdiction.

Published by Mountain Leverage on March 4, 2024.