Arkansas Updates Data Breach Notification Law to Include Biometric Data

May 22, 2019 - The State of Arkansas has updated its definition of "personally identifiable information" or PII, with regard to the state's data breach notification law. With the update, PII now includes biometric data such as fingerprints, DNA, retina scans, etcâ€¦ The updated law actually defines biometric data as "Any other unique biological characteristics of an individual if the characteristics are used by the owner or licensee to uniquely authenticate the individual's identity when the individual accesses a system or account."

Under the law, people and businesses in Arkansas are required to disclose data breached immediately upon their discovery regardless of their size. Breaches covering 1,000 or more people must also be reported to the state's Attorney General if it is determined that there is a substantial chance of harm to the consumers whose data was stolen.

The law also now requires any entity experiencing a breach to retain their records for a period of five years.

We see this update as a plus. More and more states are beginning to include biometric data in their data breach notification requirements, but there are still many states that have not done so. Biometric data has a wide variety of security applications. At this time we suspect that many of the future uses for this data have not been adequately considered by lawmakers or individual consumers. Unfortunately, once the data is out there, there is no getting it back.

It is also worth noting that freely sharing DNA or other biometric data is unadvisable. It's something that could come back to haunt a large segment of American consumers who presently see no issue with sharing this data openly. More than 1 million people have done so on an open database called GEDMatch, and both federal and state agencies are using that database in criminal cases to identify family members of suspected criminals. While you may not have any issue with this type of usage, we'll say it again. There is no telling how this data will be used in the future. Until we have some idea of what that future will look like, we believe that consumers should keep their DNA private.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS