Technologies which use permanent physical characteristics for identification are increasingly popular. These “biometric” identifiers offer clear advantages over traditional passwords and keys: they can’t be lost or forgotten, and they are much more difficult to steal. No longer only the stuff of spy thrillers and science fiction, fingerprint and facial geometry scans are now commonly used to ensure that only authorized employees can access restricted facilities and computers. Fingerprints are also widely used to secure smartphones and to access banking applications. The technology has potential application well beyond security as well. Along with these commercial benefits, however, come significant risks. Unlike traditional identifiers, if biometrics are compromised they are not easily changed. That risk of compromise will likely increase as technology develops. For this reason we are seeing an increase in both biometric laws, and biometric lawsuits. In this series of posts we will look at the laws that impact a company’s collection of biometrics, and the risks when things go wrong.

Putting it Into Practice: Companies who collect or possess biometric information should follow this series and think carefully about how they collect, use and protect biometric data.

Copyright © 2020, Sheppard Mullin Richter & Hampton LLP.

Source URL: https://www.natlawreview.com/article/biometric-breakdown-part-i