A Legal Analysis of Biometric Scanning and Data Collection

Written By: Altamash Ali

Publication Date: February 08, 2021

As technology has progressed over time, so have the security measures and techniques for authentication. Some of the newest technology in this realm includes biometric scanning, which may be the most pervasive yet. These scanners are capable of voice recognition, fingerprint scanning, facial recognition, and even heart-rate sensing [1]. It is without a doubt that biometric scanners accurately fulfill the purpose they were designed for, but at what cost? Some states have weighed in on the ethicality of collecting biometric data as a means of authentication. In this assignment, I will analyze whether or not the cost of collecting biometric data for security purposes outweighs the cost of an individual's right to privacy and evaluate the role that state jurisdiction has played in the suppression of sensitive data collection.

Biometrics is short for "biological measurements." These biological measurements are usually physical characteristics that can be used to identify an individual such as the shape of their ear, unique body odors, or facial contortions. There are three main types of biometrics security: biological (DNA, blood, etc.), morphological (structure of your body, eye color, etc.), and behavioral (how you walk, how you speak, etc.) [2]. Given the sheer depth of data which these scanners collect, it should not be a surprise that people have privacy concerns. The main one being the possibility for employers to, easily and without consent, collect one's data. Now while legislation regarding biometric data collection varies across the United States, a select few states have set the precedent when it comes to determining whether or not companies should be allowed to collect such data.

In Illinois, the Biometric Information Privacy Act (BIPA) has made the collection of a person's biometric information illegal unless the individuals has given informed and written consent [3]. Furthermore, BIPA obligates companies to protect and store the biometric data of consented individuals. In a landmark decision made by the Illinois Supreme Court in 2019, "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act" [4]. Amongst the pool of acts contrived by other states, BIPA holds an individual's data to the highest regard.

States such as Texas and Washington have implemented their own version of Illinois' BIPA which hope to have a similar effect. What makes BIPA unique, however, is that it provides a private right of action [5]. The California Consumer Privacy Act (CCPA) seems to broaden the

playing field when it comes to establishing which type of data cannot be collected. This includes anything that can be used to establish one's individual identity from vein patterns to sleep data.

Although a majority of states do not have exclusive protections against the collection of biometric data, they are certainly working towards it. It is reassuring to see states in important circuits establish concrete guidelines which companies need to follow. Regulating this field prevents companies from abusing their privilege to use biometric data collection techniques. Furthermore, I hope to see regulation such as BIPA play an important role in suppressing the collection of biometric data altogether. Data powerful enough to reconstruct an individual's identity such as fingerprints and face scans should not be left in the hands of any private entity. The potential implications of biometric data breaches can be far more damaging than breaches pertaining to other information. I believe it is better to settle for less pervasive authentication techniques while putting a larger emphasis on internal security practices. Therefore, in the case that a data breach does occur, it does not compromise the privacy of individuals involved to the extent that a biometric data breach may allow it to. In conclusion, pushing for such extreme security measures poses an unnecessary breach of privacy.

Sources

[1] https://www.natlawreview.com/article/privacy-and-cybersecurity-issues-to-watch-2019

[2] https://www.kaspersky.com/resource-center/definitions/biometrics

[3] https://www.jacksonlewis.com/sites/default/files/docs/IllinoisBIPAFAQs.pdf

[4] https://courts.illinois.gov/Opinions/SupremeCourt/2019/123186.pdf

[5] https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020