Privacy Laws in The State of Mongo

Brandon Z. Pearson

Old Dominion University

CYSE 401: Cyber Law

Amanda L. Turner, Esq.

November 11, 2022

When it comes to data privacy there are multiple ways it is addressed all covering different aspects of data. There are Federal laws that cover a level of data security that all states must stick to. While the Federal laws that protect data don’t cover all aspects of data protection and privacy it is a good standard. This is where the state must step in to further the protection and privacy of its citizens' data. Each state can implement laws that are different from other states which is why addressing online data privacy can be complex.

The importance of addressing data protection and privacy issues is due to data being a valuable asset and tool for companies. The concern with not having privacy laws is that the data that companies have gathered from the users of their websites, apps, or devices could be at risk. Due to data being valuable it could potentially be sold, exploited, or exposed to other sources that the user didn’t know or want the data being used for. This is a concern that many constituents express when it comes to their data. Not knowing what data is going to be collected or potentially used can put constituents at risk. Additionally, the concern with data is that cyber criminals could potentially gather the data and sell it to unethical sources. Potentially leading to massive amounts of personal data being leaked.

Biometric data and or information has come into greater use in recent years. With the development of technology and the way we use technology it demands greater protection. This has sparked the use of biometric data in order to aid in confidentiality, integrity and availability of information. Biometric data is typically considered something that can be used to identify an individual. The most common biometric data that is used are fingerprints, facial recognition, and retina scans. The state law of Washington describes biometric information as “a biometric identifier is defined as ‘data generated by automatic measurements of an individual biological characteristics,’ including ‘fingerprints, voiceprints, eye retinas, irises, or other unique biological patterns or characteristics that used to identify a specific individual.” (Kesan & Hayes, p. 260). Personal Identifiable Information or “PII” is similar in regard to biometric data but goes on or further to include things that can identify an individual. Typically, this means things such as social security numbers, names, or other individualized IDs. This is covered in the Privacy act of 1974, which was set to protect the privacy of individuals. This covered the areas of data that could be used to locate someone or see transaction history. The “GDPR” or the General Data protection regulation, is the law for the European Union. The E.U. addresses the rights to privacy more than the United States does. The E.U. feels that the right to privacy is a basic human right whereas the U.S. doesn't explicitly state it.

The State of Mongo should enact an act similar to the California Consumer Privacy Act (CCPA). This would allow citizens to have a say in how their data is used. The CCPA creates an environment where users have the right to know, right to delete, and right to opt out. The right to know covers the ability for the consumer to know where their data is going and how it is being used. Right to delete allows the user to delete the data that is collected on them if desired. Finally, the right to opt out allows the consumer to not allow the sale of their information. Having a CCPA like law for the state of Mongo would make the constituents feel at ease knowing that they can acquire the data that companies have on them. The state should also pass a law that requires companies to post their privacy policies to the consumer. This would allow the consumer to know what data is taken, used, and stored. The state should also set in place a biometric privacy law that covers the right to privacy on people's biometric data. This is to ensure that the gathering, safe keeping, and destroying of biometric data is secure. The GDPR provides a good goal for the U.S. to get to. The concern is that the U.S. each state must come up with their own privacy laws. This means that the state would have or want to pursue something like the GDPR. Overall, the GDPR would be a good thing for the consumer in the U.S. The main issue that comes with having a GDPR like act in the U.S. is that it would take time to implement as well as have an economic impact. Due to the extensive cost, it would have on large and small businesses having to ensure they are meeting the policies. In my opinion the U.S. will not have a GDPR act at the federal level but could be done over time at a state level. Due to the positives being heavily favored to the citizens rather than to the business it would be easier to have state support than federal support.

Overall, privacy laws have a positive impact on the constituents. Therefore, implementing the privacy laws from this memorandum would grant more support from the constituents. Creating a better secured cyberspace as well as a more informed citizen.

References

California Consumer Privacy Act (CCPA). State of California - Department of Justice - Office of the Attorney General. (2022, March 28). Retrieved November 4, 2022, from https://oag.ca.gov/privacy/ccpa#:~:text=The%20CCPA%20requires%20business%20privacy,the%%20to%20Non%2DDiscrimination.

Kesan J. P., & Hayes C. M. *Cybersecurity and Privacy Law in a Nutshell*. (2019). West Academic Publishing