Privacy Laws in the State of Mongo

Meagan E. Whaley

Old Dominion University

CRJS-406: Cyber Law CRN 36065

July 21, 2023

1. Background: Privacy issues and concerns deal with the fact that people both desire and expect certain information to be known only to people whom they deem necessary, usually on a need-to-know basis. Data privacy specifically refers to who has what data, what they do with it, and who they share that data with (Stouffer, 2023). These issues apply to everyone because everyone has personal (sensitive) data. Most people, including those living here in Mongo, don't want random people, including other private citizens or the government, to know any more information about them than is strictly necessary. People worry about how the information may be gathered and used to target them in certain ways. They are tired of being manipulated by other people, companies, politicians, etc. using information they (the individual) never realized they had. Sometimes this information is used to harm them and can cost a lot of time and money to try to make it right. It can lead to big issues such as identity theft or theft of finances or smaller issues like targeted advertisements (Stouffer, 2023). This information may include things like health information, financial information, educational information, criminal information, employment history, social security numbers, credit card information, telephone numbers, biometric data, religion, sexual orientation, race, and ethnicity, to name just a few things. Some of this sensitive information is addressed by federal privacy laws such as medical information, financial information, and information collected by telecommunications services. Federal statutes were also passed to specifically protect the privacy of children and students (Kesan & Hayes, 2019). Many of these issues, however, are not addressed by federal laws such as biometric data, notification of data breaches, data-correction laws, and opt-in vs. opt-out laws. We should be discussing these issues and making a plan to address and resolve them not only because the constituents of Mongo care but also because they affect everyone, including those that make up our most

vulnerable populations such as children and the elderly. Private and sensitive data can cause great harm to people when not handled correctly and cost a lot of money to fix. Addressing issues now and enacting well-thought-out laws can help save time and money in the long run as well as help simplify confusion regarding data in an ever-changing and growing digital world.

2. Key Words and Concepts:

   PII: Personally Identifiable Information: any information that may help to identify a person whether by itself or in combination with other personal information; may include information like names, social security numbers, passport information, or birthdates and may or may not be combined with other types of sensitive information like race, religion, medical, information, etc. (Kesan & Hayes, 2019).

   Biometric data: is defined individually by states: generally, any biometric-type data (i.e. biological characteristics) that can be is stored and can be used to identify an individual; can include eye (retina or iris) scans, fingerprints, voiceprints, hand geometry, and/or face geometry (Kesan & Hayes, 2019).

   GDPR: General Data Protection Regulation, enacted by the EU and went into effect in 2018: privacy laws apply to both governments and private parties; discusses the rights of individuals concerning their private data, the responsibilities of people who have access to individuals' private data, the transfer of personal data, penalties for breaking the law, and administration issues (Kesan & Hayes, 2019).

   DPAs: Data Protection Assessments: required form to assess high-risk activities concerning data processing including information about children, biometric data, and data about race, ethnicity, religion, and sexual orientation (Augustinos & Cox, 2022)

3. Potential data protections:
    a. We should enact laws restricting the collection and use of biometric data and only allow it to be used with a person's direct consent.
    b. We should enact laws regarding the notification of data breaches, making sure people know and understand what has occurred in the event of a data breach. These laws should also include penalties for companies that allow breaches to occur and corrective actions they must employ to help resolve issues for people who had their data breached.
    c. We should enact laws that require informing people of their rights when it comes to their data including who has what data and how that data is being used, the right to correct incorrect data, and the right to restrict access to their data.
    d. People should opt in for their data to be used (not opt out) and be given the choice to opt out of their data usage at any point.
    e. We should also consider laws regarding the encryption of personal data, requiring companies to encrypt personally identifiable information during both the storage and transmission of that data.
    f. Several states already require assessments concerning high-risk data processing (DPAs) (Augustinos & Cox, 2022) and I think we should consider using those as well. These assessments would help to control who has access to certain personal data and how that data is used.

GDPR-like laws are possible in Mongo, but it will require considerable resources to enforce them. One of the benefits to the GDPR is that it applies to all of the European Union, which means that data can cross many countries' borders where the same laws apply. In the United States, it will be much harder to keep track of and enforce some of these laws when so much of

our data crosses state lines and each state has its own state laws. It will be costly in terms of time, energy, manpower, and money. However, it would be worth it to provide the high levels of data privacy that the GDPR provides. Several other states have already created laws similar to the GDPR including California, Colorado, Connecticut, Utah, and Virginia. We can consider, perhaps, creating a new agency such as California's Privacy Protection Agency (Augustinos & Cox, 2022) to enforce the new laws.

Protecting peoples' data is important, and only becoming more complicated as more and more data is being collected, compiled, held, and shared or sold to other companies or organizations across states and countries. This data is being used in ways that people neither know nor comprehend, and they definitely didn't (knowingly) give their consent. The people are very concerned with it; thus, we should also be concerned with it. If we are to be a voice for the people of Mongo, we need to listen to and address their concerns, and those concerns right now are for privacy.

References

Augustinos, T.P., & Cox, A.R. (2022, December). U.S. Sate Privacy Laws in 2023: California, Colorado, Connecticut, Utah and Virginia. *Privacy & Cybersecurity Newsletter*. https://www.lockelord.com/newsandevents/publications/2022/12/us-state-privacy-laws-2023

Kesan, J.P., & Hayes, C.M. (2019) *Cybersecurity and Privacy Law in a Nutshell*. West Academic Publishing. https://platform.virdocs.com/read/1949083/21/#/4/2/8,/5:0,/5:0

Stouffer, C. (2023, May 26). What is data privacy and why is it important? *Norton Lifelock, Inc*. https://lifelock.norton.com/learn/identity-theft-resources/what-is-data-privacy-and-why-is-it-important