Data Protection and Privacy Concerns in the State of Mongo

William Xue

CYSE 406-36065

20 July 2023

MEMORANDUM

TO: Karras

Governor of the State of Mongo

FROM: William Xue

Aide to Governor

DATE: July 20, 2023

SUBJECT: Data Protection and Privacy Concerns in the State of Mongo

This memorandum is to address the data protection and privacy issues raised by Mongo constituents and to provide the governor with a comprehensive understanding of the matter.

According to the complaints we received, data protection and privacy concerns involve about protecting individuals' personal data from unauthorized use, access, and disclosure by other people or industry entities. The primary concerns from the potential risks of misuse of personal data, which may cause identity theft, financial fraud, and/or other types of privacy violations. Currently, we are in an increasingly digital world. There are huge amounts of personal information are collected and processed. It is critical that we establish a robust method to protect people's privacy.

The rights of privacy are important to Constituents, you, and me. According to Cloudian, data privacy helps ensure that sensitive data is only accessible to approved parties and prevents criminals from being able to maliciously use data and helps ensure that organizations meet regulatory requirements. Constituents seriously care about data protection and privacy because those issues may directly impact their personal rights and security and may cause identity and

financial lost. Constituents lose control of their data and information without data protection and privacy when individuals' data is collected and used without consent. To subject those concerns, as the Governor of Mongo, you should demonstrate your commitment to safeguarding the rights and interests of Mongo citizens.

In the complaints of Constituents, they mentioned some terms about data protection and privacy, like biometric data, PII, the GDPR. To be clear, here are the definitions for each term. Biometric data: According to Kesan, J. P., & Hayes, C. M. (2019), each state has promulgated a slightly different policy and implement appropriate balance between corporate interests and individual privacy rights. Also, the definition of biometric data is slightly different. In common, biometric data refers to individual's unique biological characteristics for identification and authentication. Such as: fingerprints, voiceprints, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual (Kesan & Hayes, 2019). PII: PII stands for Personally Identifiable Information. PII is any information that can be used to distinguish or identify an individual directly or indirectly. For example: name, date of birth, address, social security number, medical records, financial records. Misuse of PII can cause identity loss and privacy breaches. GDPR: GDPR is the abbreviation of General Data Protection Regulation. Wolford (2020) stated that GDPR is the toughest privacy and security law in the world. It was drafted and passed by the European Union to protect personal data in the EU. It provides individual more control over their privacy data and places obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. Also, the GDPR outlines strict penalty policies for non-compliance.

Based on our research, the State of Mongo legislature might enact laws to protect the following types of personal data which are not already protected by federal law. Consumer data:

if this personal data was collected by business entities, such as online shopping habits, online behaviors, and preferences. This could cause consumers to receive many unknown malicious ads and lose trust to the merchants. Location data: Legislation should try to limit the collection and use of geolocation data from devices to ensure individual's location privacy.

Implementing laws like the GDPR in the State of Mongo is feasible, it comes with both profits and challenges. Strict laws like GDPR can enhance privacy protection which can strengthen people's privacy rights, increase individual's confidence in state businesses and institutions. On the other hand, GDPR-like regulations will increase the complexity of law's implementation and increase the cost to comply the new requirements.

Overall, addressing data protection and privacy concerns is foremost for defending Mongo constituents' rights and guaranteeing their trust in the state government and businesses. While implementing GDPR-like legislation is feasible, cautious consideration of the related pros and cons is necessary before proposing new laws. I believe this memorandum helps Governor Karras to understand the issue better and aids in formulating informed decisions for the benefit of our constituents.

References

Data Protection and privacy: How to protect user data. Cloudian. (2023, June 21). https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/

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

Wolford, B. (2022, May 26). *What is GDPR, the EU's new Data Protection Law?* GDPR.eu. https://gdpr.eu/what-is-gdpr/