MEMO

UNDERSTANDING DATA PROTECTION AND PRIVACY CONCERNS

To:	Governor Karras
From:	Gavin Williams
Date:	10/25/2023
Class:	CYSE46 – Cyber Law

COMMENTS: This Memorandum will be a short aid to explain the current concerns that have been occurring regarding data protection and privacy issues. With this document you will learn about why these issues are important and what meaning they have for government and people alike. Along with definitions for terms such as biometric data, PII, GDPR, and so on. By the end of this read, you will have a better understanding of the topic, allowing you to make informed decisions and take appropriate actions.

Overview of Data Protection and Privacy Issues

Data protection and privacy issues are vital in today's digital world. These concerns deal with how personal information is handled, collected, used, and shared. Protecting this data is important because if it's not handled correctly, it could lead to issues such as unwanted marketing or in more severe case's identity theft and financial fraud. Privacy is about keeping our personal lives away from prying eyes. When privacy is breached, someone could learn information about us that we didn’t want them to know. These issues matter to everyone because they're about keeping our personal information safe and maintaining our right to a private life. This is why we all should care about how our data is protected and our privacy is maintained. To reiterate these are the key topics for why data protection and privacy are crucial.

- **Privacy as a Fundamental Right**: Privacy is generally considered a fundamental human right. The misuse of personal data may cause an invasions of privacy.
- **Identity Protection**: wrongful use or theft of personal data can lead to identity theft, financial fraud, and other personal risks.
- **Individual Independence**: Controlling someone’s personal information may make them feel as if they don’t have personal freedom or independence.
- **Trust in Power**: Effective data privacy laws help in maintaining public trust. Lack of trust can hurt social and economic stability.

Key Terms and Concepts

It is important to learn these terms, so you know what the people are concerned about. Here are some key definitions and concepts that you need to know.

- **Personally Identifiable Information (PII)**: PII is any information that can be used to identify a specific individual. such as a person’s name, address, Social Security number, medical information and so on. The illegal use of someone's PII can result in identity theft and breach of privacy.
- **General Data Protection Regulation (GDPR)**: This is a comprehensive data protection law in the European Union and is considered one of the world’s strongest set of data protection laws. It states strict guidelines for data collection, processing, and privacy. Its main features include consent for data processing, data subject rights, and severe consequences for failed compliance. Note that the protection laws are the same regardless of if the processing occurs online or offline.
- **Biometric Data**: This refers to a person's physical characteristics used to identify individuals. For example, fingerprint scans, facial recognitions, retina scans, and so on.

These are the three terms you must know but you should also know these terms as well.

- **Right to Access**: individuals have the right to request access to their personal data and information about how the data is being processed.

- **Right to be Forgotten:** the individual has the right to have their personal data removed for any reason or no reason at all.
- **Data Minimization**: Personal data collected should be minimal so that only the data necessary is collected.
- **Data Portability**: the individual has the right to receive their data in a structured, commonly used, and machine-readable format, and to send it to another data controller.
- **Data Controller**: controls the procedures and the purpose of data usage.

Recommendations for the State of Mongo

Because of the concerns of Mongo's constituents and existing gaps in federal law, the state should consider legislating protections for these.

- **Digital Footprints**: Information individuals leave behind while using the internet, for example, someone's internet history.
- **Location Data**: Geographical data collected from smartphones and other devices.
- **Consumer Behavior Data**: Information on what individuals purchase and what products they would be likely to buy.
- **Communication Data**: Protecting the content of emails, messages, and calls from unauthorized access and surveillance.
- **Employee Privacy laws**: Employers monitoring the actions of employees through digital software, and collecting unauthorized emails is a growing concern. Specific State laws can offer clearer boundaries as to privacy rights for employees.

These are some forms of data that must be protected at the state level as they are not protected at the federal level.

Feasibility of Implementing GDPR Laws:

- **Pros**:
- Creates clear guidelines for businesses and individuals.
- Improves public trust and confidence in how their personal data is handled.
- Aligns Mongo with international data protection standards, which will benefit trade and international relations.
- **Cons**:
- Implementation will be costly and complex, especially for small businesses.
- May hurt certain types of data-driven innovation. For example, those target advertising and other systems that use personal data.
- Balancing privacy with free speech and access to information may be difficult.

Informed Opinion:

Implementing GDPR laws in Mongo will be beneficial in the long term, by better protecting the people's data and privacy. However, the state must consider the economic impact it will have, especially on small businesses. We should take a balanced approach that will still encourage innovation while also protecting individual privacy rights. It is important to keep in mind both the protection of individuals' rights and the practical implications of this legislation. Collaborative work with stakeholders from business, civil society, and legal experts will be important to effectively balance its implementation.

[see references on next page]

References

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

Wolford, B. (2023, September 14). *What is GDPR, the EU's new Data Protection Law?* GDPR.eu. https://gdpr.eu/what-is-gdpr/

ICO. (2022, September 22). *Key data protection terms you need to know*. Information Commissioner's Office. https://ico.org.uk/for-organisations/advice-for-small-organisations/key-data-protection-terms-you-need-to-know/

NCSL. (2022, June 7). *Report state laws related to Digital Privacy*. National Conference of State Legislatures. https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy#:~:text=Five%20states%E2%80%94California%2C%20Colorado%2C,of%20personal%20information%2C%20among%20others.