Writing Assignment 1

Clyde Cabico

UIN 01243616

CYSE 406 Cyber Law

February 1, 2024

THE STATE OF MONGO

February 1, 2024

PRIVACY AND DATA PROTECTIONS MEMORANDUM

MEMORANDUM FOR: GOVERNOR KARRAS

FROM: Clyde Cabico
Governor's Aide

SUBJECT: State of Mongo Privacy and Data Protections Importance

I. PURPOSE

This memorandum identifies and explains the importance of the establishment of state laws concerning privacy and data protections concerning the collection of personal data including and not limited to biometric data and personally identifiable information (PII) for constituents of the State of Mongo.

II. DEFINITIONS

Personal Data: Information linking to the identification of a person through social security number, financial account numbers (including credit and debit accounts) in combination with the verification information needed to access the account, and driver's license numbers or other numbers of government issued identification cards and documents.

Biometric Data: Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.[1]

[1] See "Biometric Data - European Commission." Home-Affairs.ec.europa.eu, home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/biometric-data_en#:~:text=Definition(s). Accessed 28 Jan. 2024.

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. [2]

Medical Information: Any individually identifiable information, in electronic or physical form, regarding the individual's medical history, treatment, and/or treatment by a healthcare professional.

General Data Protection Regulation (GDPR): (May 25, 2018) The toughest privacy and security law in the world; Europe's data privacy and security law includes hundreds of pages' worth of new requirements for organizations around the world.[3]

III. OVERVIEW

Issues concerning many Mongo constituents have been concerned of the lack of protection of personal data to include but not limited to biometric data and PII being used without their authorization by other parties' outside of the intended party or parties' use. Federal statues do not cover these personal data issues these constituents have and must be addressed by the state by the establishment of Mongo State laws.

Data protection and privacy issues revolve around safeguarding individuals' personal information and ensuring its proper handling. Concerns arise from the collection, storage, processing, and sharing of personal data by organizations and entities. Individuals worry about unauthorized access, data breaches, and the potential misuse of their information, leading to identity theft or financial fraud. Privacy issues also encompass the transparency of data practices, "the first major category of privacy law concerns protection of citizens from the government," (Kesan and Hayes 227) giving individuals the right to know how their data is being used and the ability to control its dissemination. Emerging technologies and the increasing digitization of information amplify concerns, "states are increasingly

[2] See "Personally Identifiable Information (PII) | Protecting Student Privacy." Studentprivacy.ed.gov, studentprivacy.ed.gov/content/personally-identifiable-information-pii#:~:text=Personally%20identifiable%20information%20(PII)%20includes.

[3] See Wolford, Ben. "What Is GDPR, the EU's New Data Protection Law?" GDPR.eu, European Union, 2023, gdpr.eu/what-is-gdpr/.

acknowledging and regulating the use of biometric data,"(Kesan and Hayes 230) especially in the context of surveillance, tracking, and profiling. Although there are special exemptions like, “Under Section 40702 of Title 42 of the U.S. Code, law enforcement is authorized to collect DNA samples from individuals in custody and from individuals who are on supervised release, parole or probation.” (Kesan and Hayes 234) Balancing the benefits of data-driven services with the need to protect individual privacy is an ongoing challenge for policymakers, businesses, and society as a whole.

Handling biometric data is crucial due to its unique and sensitive nature, as it involves the physical or behavioral characteristics of individuals, such as fingerprints, facial features, or iris patterns. Privacy is paramount because biometric information is irreplaceable, “limit the use of disclosure of the information to the minimum necessary amount,” (Kesan and Hayes 234). This minimum necessary amount is referring to covered entities in connection with the Health Insurance Portability and Accountability Act (HIPAA). Once compromised, individuals face long-term risks such as identity theft or unauthorized access. Biometric data is unique to each individual, “CEO impersonation scams, which have caused at least $3 Billion in losses to companies since the FBI began tracking these scams in 2013.” (Kesan and Haynes 34) Represents the multitude of lost revenue, hence, privacy is at its utmost importance concerning biometric data. Mishandling biometric data can result in severe consequences, including personal security breaches and potential misuse of the information for malicious purposes, like the fact mentioned previously. The compromise of biometric data, especially of political officials, such as yourself, Governor Karras, may have unforeseen consequences to State and National Security. Strict privacy measures are essential to build and maintain public trust in biometric technologies and their responsible use.

The proper handling and privacy of personally identifiable information (PII) are paramount in safeguarding individuals' personal data. “According to the FTC, online fraud — of which identity theft is a major component — cost Americans $8.8 billion in 2022, with median losses of $650; some private estimates are much higher. Nearly one in five (18%) of our survey respondents report continued financial loss today as a consequence of identity theft.” (Lever) Unauthorized access or misuse can lead to significant harm financially. Maintaining the confidentiality of PII is crucial for preventing identity theft, financial fraud, and other malicious activities; exposure of such information can have long-lasting consequences. “July 2023 HCA Healthcare announced personal data from some 11 million patients was compromised in a breach that exposed their names, dates of birth, email, and telephone numbers.” (Lever) Responsible handling of PII fosters trust between individuals and organizations, creating a secure environment for data exchange; this trust is foundational for healthy relationships in various sectors, including healthcare. Compliance with data protection regulations and implementing robust security measures are essential to uphold the integrity and confidentiality of personally identifiable information.

Implementing laws like the GDPR in the European Union (EU) could be feasible, offering enhanced data protection and individual rights. There seems to be many pros concerning the GDPR, however, challenges include potential compliance burdens for businesses, especially

smaller ones, and navigating cross-border complexities. This is led by the stance of information security, "The relationship between security and convenience is inversely proportional," (Ciampa) Larger organizations with a hefty financial status and manpower may overcome these complexities easier than small business entities and may drive them out of the market. Enacting strict and stringent laws requires thorough overview as it may jeopardize e-commerce. Protecting citizen's individual rights and data is obviously one of the top priorities' governments should have and enforce, but balancing comprehensive protection with practicality is crucial. Adequate enforcement mechanisms and robust awareness campaigns will be vital for successful implementation.

IV. OPINION

As you can see, Governor Karras, from the overview provided, I hope that you have a greater understanding of the importance regarding safeguarding the personal data of the constituents of The State of Mongo. It is of great concern to me, as privacy involving these defined factors that involve personal data can cause imminent undue harm to myself, family and most importantly to the Nation and State of Mongo as I hold political position as your aide. As of this date and time, there is currently no Federal Statues established concerning breach of these categories of defined personal data. It is imperative we devise and propose State of Mongo statues to address the overviewed concerns and perform our elected duties as political officials to protect and serve the constituents of Mongo.

V. PROPOSAL

Mongo Unauthorized Biometric Data Protection Act (MUBDPA)

Section 1: Prohibition of Unauthorized Disclosure

(a) No person shall knowingly disclose, share, or make accessible to any unauthorized party the biometric data of an individual without explicit and written consent.

(b) Unauthorized disclosure includes, but is not limited to, sharing biometric data for commercial purposes, third-party marketing, or any activity not explicitly approved by the individual.

Section 2: Improper Handling and Negligence

(a) Any entity, public or private, collecting, storing, or processing biometric data is required to implement reasonable security measures to prevent unauthorized access, disclosure, or theft.

(b) Negligence in securing biometric data, resulting in unauthorized access or disclosure, may lead to civil penalties, including fines and potential legal action by affected individuals.

Section 3: Enforcement and Penalties

(a) Violation of this statute may result in both criminal and civil penalties, with fines of a minimum of 10,000 Mongo Mezos (MM) not to exceed 500,000(MM), imprisonment, or a combination thereof, depending on the severity and intent of the violation.

(b) Individuals affected by unauthorized disclosure, theft, or improper handling of biometric data have the right to pursue legal action against the responsible parties for damages and injunctive relief.

Mongo Personal Information Protection and Accountability Act (MPIPAP)

Section 1: Digital Health Information Security

(a) Entities handling digital health information must employ advanced encryption measures and implement secure access controls to protect individuals' health records.

Section 2: Enforcement and Penalties

(a) Violation of this statute may result in both criminal and civil penalties, with fines of a minimum of 10,000 Mongo Mezos (MM) not to exceed 500,000(MM), imprisonment, or a combination thereof, depending on the severity and intent of the violation.

(b) Individuals affected by unauthorized disclosure, theft, or improper handling of biometric data have the right to pursue legal action against the responsible parties for damages and injunctive relief.

V. Conclusion

Governor Karras, the absence of comprehensive state statutes addressing privacy and personal data collection necessitates a careful examination of legislature to enhance protections for individuals. In the United States for example, “States respond differently to

changes in society, but it should come as no surprise that all fifty states emphasize the idea of authorization in their cybercrime laws." (Kesan and Hayes 96) The people have spoken and it is imperative for The State of Mongo to enact robust regulations that strike a balance between personal data and privacy rights and enforcement and penalties. "States vary a bit on what they consider to be PII." (Kesan and Haynes 121) The proposed state statutes under deliberation, such as those addressing biometric data protection and digital health information security, showcase a proactive approach toward closing existing gaps. These potential statutes help to establish a foundation and emphasize the need for clear guidelines, transparency, and stringent penalties to ensure accountability in the handling of sensitive personal data. Your, The State of Mongo Governor's Aide, Clyde Cabico.

Sincerely,

Clyde Cabico

The State of Mongo Governor's Aid

UIN 01243616

CYSE 406 Cyber Law

Tel: 757 777 7777

Email: FakeMongoAide@mongo.fake.gov