INSTRUCTOR: AMANDA L. CHENEY, ESQ.

CYSE 406

10/25/2024

Data Privacy and Protection in the State of Mongo

Memorandum to Governor Karras

From: Akpovi, Daniel
GOVERNOR'S AIDE

Governor Karras,

Data protection and privacy are among the most critical issues of our time, especially when one thinks of personal data being collected and processed without the knowledge and explicit consent of most residents of Mongo's constituency. As more and more services shift towards digital platforms where protecting the private sphere fall victim to ease of use and broader advancements, there is an increasing risk of privacy concerns and abuse related to a personal data. The purpose of this memorandum will be to outline some critical concerns regarding data protection, define specific terms, including biometric data and Personally Identifiable Information (PII), and discuss Mongo's legislative options for safeguarding data protection. This includes the feasibility of legislation like the GDPR one.

I. Overview of Data Protection and Privacy Concerns

Data privacy is the right of individuals to control the use and circulation of personal information about themselves (De Capitani Di Vimercati et al., 2012). Without regulation, people are exposed to identity theft, fraud, and the targeted use of their personal information in manners that violate primary privacy considerations. Data privacy matters to Mongo’s constituents because it directly affects their autonomy and security in the growing digital world. Data protection means that entities collecting personal information must do so in ways bound by rules protecting people's privacy; and for reminder, this issue is not just about protecting private information but also about building trust between the government and its citizens. If people fear that their own government might not keep their data safe, they lose faith in the institutions charged with protecting them and have every reason to withdraw from public life, perhaps in potentially dangerous ways. The rise of technology threatens to blur the line between people's private and public lives and needs strong protections against public intrusions into private.

II. Key Terms Explained

A handful of terms related to privacy and data protection are particularly useful for understanding what the State of Mongo constituents care about.

Biometric data: It is any data of a person's physical nature that can be used to identify them, including, but not limited to, fingerprints, facial recognition, or DNA (Department of Homeland Security, 2024). The collection of biometric data is problematic because such information is unique for each person, and its misuse could cause severe privacy violations.

Personally Identifiable Information (PII): PII is any information that may be used to identify a specific person, directly or indirectly (Narayanan and Shmatikov, 2010). Names, email addresses, and social security numbers are a few examples. PII can provide information on an individual whose identity has been stolen, thus putting them at risk, therefore, it is essential to protect and stop its unauthorized access.

General Data Protection Regulation (GDPR): Under the GDPR, which is a European Union law that lays out strict regulations for how organizations must treat specific data, citizen consent is required for any data gathering, and individuals have a right to have their data deleted (IT Governance Privacy Team, 2020). This may be the law that the State of Mongo's constituents are referring to in their requests for action, and it provides some of the most complete protections for access to and storage of personal data.

Data breach: When hackers get their hands on people's personal information.

Consent: Permission granted by individuals for their data to be collected and used. Under regulations like the GDPR, consent must be informed, specific, and revocable.

III. Legislative Recommendations for Mongo

With these concerns in mind, the State of Mongo should pass laws to cover types of data not currently covered by federal law; therefore, research and coursework suggest the following:

Protection of Biometric Data: Mongo could pass laws on the classifications and transmissions of biometric data, similar to Illinois' Biometric Information Privacy Act (BIPA). Under BIPA, anyone collecting biometric data such as fingerprints, retina scans, or other measurements of unique body features must have the person's informed consent, and any violation of those laws could result in a lawsuit (ACLU Illinois, 2021).

Stricter PII Protections: Laws must be passed to ensure that companies handling PII disclose exactly what sort of information they collect and why, require individuals to provide consent, and give them rights to see and correct any of their data.

Data breach notification laws: Mongo could pass laws requiring organizations to swiftly alert users, should a data breach occur, to mitigate harm from unauthorized access to personal information.

In terms of the feasibility of GDPR-like laws being applied in Mongo, on the one hand, they will increase transparency, support for local businesses, and consumer protection, as well as increase public trust; on the other hand, implementing this legislation will make it more expensive for businesses, especially small and medium size businesses, to comply with the law, and it will be difficult to enforce. While the GDPR is an idealistic model, Mongo may need to start smaller with more specific and, thus, more manageable laws aimed at protecting against the most prominent data breaches without placing an unbearable burden on small and medium-sized enterprises, particularly those in Mongo.

The State of Mongo must take immediate action to pass legislation that addresses the urgent issues of data protection and privacy with a focus on biometric data protection, increasing the effectiveness of PII protection, and mandating responses to data breaches to protect its constituents. As it can be seen from the GDPR, these areas of the law are comprehensive, but it will be needed to assess whether these laws are realistically attainable for Mongo, considering what is possible in your own state's economic and regulatory environment.

Very respectfully,

Daniel Akpovi

Governor’s Aide.

References:

ACLU Illinois. “Biometric Information Privacy Act (BIPA).” *ACLU of Illinois*, 26 Apr. 2021, www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa.

De Capitani Di Vimercati, Sabrina, et al. “Data Privacy: Definitions and Techniques.” *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 20, no. 06, Dec. 2012, pp. 793–817, https://doi.org/10.1142/s0218488512400247.

Department of Homeland Security. “Biometrics.” *Department of Homeland Security*, 4 Mar. 2024, www.dhs.gov/biometrics.

IT Governance Privacy Team. “EU General Data Protection Regulation (GDPR) – an Implementation and Compliance Guide, Fourth Edition.” *IT Governance Publishing*, Oct. 2020, https://doi.org/10.2307/j.ctv17f12pc.

Narayanan, Arvind, and Vitaly Shmatikov. “Myths and Fallacies of ‘Personally Identifiable Information.’” *Communications of the ACM*, vol. 53, no. 6, June 2010, p. 24, https://doi.org/10.1145/1743546.1743558.