Cyber Law Writing Assignment

CYSE 406

By Latitus Jones

2/22/24

To: Governor of the Commonwealth of Virginia

From: Latitus Jones

Subject: Privacy and Data Protection

Date: 2/22/24

Privacy is the ability of individuals or groups to selectively seclude themselves or information about themselves, controlling what is shared and with whom. Personal information and data protection concerns focus on safeguarding sensitive data from unauthorized access, use, or disclosure, encompassing issues like identity theft, surveillance, and infringements on individual freedoms. Protecting personal information and data is vital to citizens for several reasons: it upholds the fundamental right to privacy, ensures security against identity theft and fraud, fosters trust in institutions through respectful handling of data, and empowers individuals to make informed choices autonomously. Without proper protection, personal information can be stolen, leading to identity theft and financial loss. Privacy is compromised as data is collected and used without permission, potentially damaging one's reputation. Surveillance and tracking become easier, risking freedom and autonomy. Discrimination based on personal data can occur, and cyberbullying may increase. Data breaches can expose sensitive information, eroding trust in organizations. In essence, without protection, individuals face risks to their finances, privacy, and overall well-being. Examples of biometric data include fingerprints, facial recognition, and retina scans, while personally identifiable information comprises data like names, addresses, social security numbers, and financial or medical records.

The General Data Protection Regulation (GDPR) is a comprehensive set of data protection laws enacted by the European Union (EU) to safeguard the privacy and personal data of EU citizens. It applies not only to organizations within the EU but also to those outside the EU

that process the data of EU residents. The GDPR encompasses various areas broadly, including the principles it sets forth for data protection. These principles include ensuring that personal data is processed lawfully, fairly, and transparently; collecting data for specified, legitimate purposes and not further processing it in a manner incompatible with those purposes; keeping data accurate and up-to-date; limiting data storage to what is necessary for the intended purpose; and ensuring the security and confidentiality of personal data. Additionally, the GDPR grants individuals rights over their personal data, such as the right to access, rectify, and erase their data, as well as the right to data portability and the right to object to processing in certain circumstances. The GDPR establishes a robust framework for protecting individuals' privacy and personal data in an increasingly digital world.

States across the United States have been taking proactive measures to enhance privacy protections for their residents. California, for example, often at the forefront of privacy legislation, enacted the California Consumer Privacy Act (CCPA), which went into effect in 2020. The CCPA grants California residents various rights regarding their personal data, including the right to know what information businesses collect about them, the right to opt-out of the sale of their information, and the right to request deletion of their data (Bonta 2023). Additionally, the law imposes obligations on businesses to provide transparent privacy notices, implement reasonable security measures, and refrain from discriminating against consumers who exercise their privacy rights. The CCPA has set a precedent for comprehensive data protection legislation at the state level and has influenced discussions around privacy regulation nationwide. Other states have since followed suit, introducing similar laws or considering their own versions to strengthen privacy protections for their residents.

Governor Tar-Míriel faces a critical decision regarding whether to prioritize enacting a personal information/data protection law within Númenor or to focus efforts on advocating for a federal-level law. Both courses of action present distinct advantages and drawbacks. Enacting a local law within Númenor would allow for tailored regulations that directly address the unique needs and concerns of the populace. This approach could foster a sense of trust and confidence among residents, demonstrating the government's commitment to safeguarding their privacy. Moreover, Númenor could serve as a model for other regions, potentially influencing broader legislative efforts. However, implementing a standalone law might result in inconsistencies or conflicts with federal regulations, complicating compliance for businesses operating across jurisdictions. Conversely, prioritizing federal legislation could ensure uniform standards and streamline compliance for businesses operating nationwide. It would also demonstrate unified national commitment to data protection, potentially carrying more weight in international negotiations and partnerships. However, navigating the complexities of federal policymaking may entail prolonged deliberations and compromises, delaying the realization of robust data protection measures. Governor Tar-Míriel must carefully weigh these factors, considering the immediacy of local needs, the potential for broader impact, and the political feasibility of each approach before deciding on the most effective course of action.

References

Bonta, R. (2023, November 9). *California Consumer Privacy Act (CCPA)*. State of California - Department of Justice - Office of the Attorney General. https://oag.ca.gov/privacy/ccpa