To: Governor Tar-Míriel

From: Nathan Mack

Subject: Necessary Advancements in Cyber Law

Date: October 27, 2023

Privacy is a cornerstone in the complicated fabric of modern society, embodying an individual's right to regulate the access and use of their personal information. It encompasses sensitive aspects such as biometric data and personally identifiable information and goes far beyond the traditional realms of name and addresses. Concerns about personal information/data protection come from the growing hazards posed by the unrestricted collecting and exploitation of individuals' data. Recent studies emphasize the need of addressing these problems, revealing a world rife with data breaches, identity theft, and illegal access to personal information. Because Númenor has strong privacy regulations, its inhabitants are vulnerable to not only money fraud but also possible harm to their personal and digital identities. Citizens prioritize the protection of personal information/data for a variety of reasons. Individuals without proper protection face the bleak reality of identity theft, in which hostile actors assume their identities for fraudulent activity, resulting in financial losses and reputational damage. Furthermore, the unlawful observation and probable manipulation of biometric data poses issues. The degradation of privacy also creates opportunities for the exploitation of individually identifiable information, allowing for targeted advertising, uninvited profiling, and even discrimination. In essence, personal information protection is a fundamental right that protects persons against a variety of abuses while preserving their autonomy and generating a sense of security in an increasingly digitized environment.

Biometric data are distinctive physical or behavioral features that can be used to identify people. Fingerprints, facial recognition patterns, iris scans, voiceprints, and even gait analysis are examples. These distinguishing characteristics are used in a variety of scenarios, ranging from unlocking smartphones to improving security systems. Personally Identifiable Information (PII), on the other hand, includes any information that can be used to differentiate or trace an individual's identity. Names, addresses, social security numbers, email addresses, and financial information are all examples. PII is critical in identity verification processes and is frequently targeted in cyber assaults for identity theft or fraudulent activities. Both biometric data and PII are sensitive types of information that must be safeguarded to prevent unauthorized access, misuse, and potential harm to peoples' privacy and security.

The General Data Protection Regulation (GDPR) is a comprehensive legal framework put in place by the European Union to govern personal data processing. The GDPR, which has been in effect since May 2018, applies to all EU member states, ensuring a consistent approach to data protection. It applies to a wide range of people, including EU residents and citizens, regardless of where they live, and extends its jurisdiction to enterprises that process personal data. The GDPR

is based on several essential principles, the most important of which are transparency, lawfulness, and fairness in the handling of personal data. It gives individuals more control over their information, including the ability to access, amend, and remove personal data. Furthermore, the GDPR requires data controllers and processors to establish rigorous data protection measures that ensure the security and integrity of the processed information. The rule also establishes the concept of Privacy by Design and by Default, urging firms to build data security into their systems and processes from the start. Overall, the GDPR establishes a high bar for data protection, intending to create a more secure and privacy-conscious digital environment for European Union citizens.

Several states throughout the United States of America have been aggressive in implementing privacy laws to protect their inhabitants' personal information. California, for example, has set a precedent with the California Consumer Privacy Act (CCPA), which went into effect on January 1, 2020. The CCPA gives California residents more control over their personal data by allowing them to see what information is being collected, request deletion, and opt out of data sales. It is applicable to businesses that meet certain conditions, such as those with yearly gross revenues of more than $25 million or those that handle vast amounts of personal information. The CCPA not only reiterates some of the GDPR's principles, but it also provides additional aspects geared to the growing digital landscape. This includes measures protecting kids' rights, increasing openness in data collection procedures, and enforcing consequences for noncompliance. The CCPA's passage reflects a growing global trend in which states are taking proactive steps to address privacy issues and provide individuals more control over their personal information.

I now request that you, Governor Tar-Míriel, prioritize efforts to have Númenor create its own personal information/data protection law. A localized approach provides for personalized rules that can quickly address Númenorean individuals' specific concerns, displaying a commitment to protecting their privacy. When compared to federal legislation, the benefits of a state-specific law include greater agility in responding to immediate risks, the flexibility to connect closely with the state's cultural environment, and a faster implementation process. Given the immediacy of privacy concerns in Númenor, a state-specific law provides a more responsive and personalized approach, allowing you, the Governor, to address urgent challenges while actively advocating for a comprehensive national law in the long run.

Sources used:

California Consumer Privacy Act (CCPA). State of California - Department of Justice - Office of the Attorney General. (2023, May 10). https://oag.ca.gov/privacy/ccpa