To: Governor Tar- Míriel

From: Jacen Davis, Cyber Law Intern

Subject: Recommendations on enacting privacy and data protection laws for the state of Númenor.

Date: March 19, 2023

Dear Governor,

Privacy and digital data protection concerns concern what others can collect and obtain from individuals, knowingly and unknowingly, and how said information is stored and processed. Privacy is hard to define, but generally is the right for someone's information (sensitive or otherwise) not to be shared by others who are not authorized or want to be made aware (Paine et al., 2007, p. 526). Privacy ranges from personal, financial, or health information being shared with companies and private third parties to general privacy that protects the individual from government overreach in civil and criminal cases (surveillance and collection). Data protections are measures of how such information must be kept private and are generally up to the private sphere to implement. The government can define laws and frameworks for specific sectors of the economy or broad data protection and privacy, requiring specific organizations to implement recommended protections for individual data. Failure to adequately protect personal, financial and health data can compromise the safety and integrity of institutions and the public. The public's confidence can be eroded depending on the severity, and as people's data are bought, sold, and used for criminal enterprise. General speculation and panic from data leaks and thefts reverberating throughout the economy may occur if companies are left without recourse or requirements to protect people's data appropriately.

Data protection, privacy, and data/information are defined broadly given their vast array of data, protections, and levels of privacy that can be enacted. Some of the most common data required for protection are personally identifiable information (PII), financial information, personal health information (PHI), and authentication credentials like passwords and biometric data. PII consists of information such as your name, date of birth, social security numbers, tax identification numbers, and other similar identifying factors, including authentication like passwords or recovery codes (Kesan & Hayes, 2019, pp. 96-99). Financial information can consist of credit card numbers, bank routing numbers, and bank account numbers that can be used to make authorized (or unauthorized) transactions from an individual or organization's bank or business account. PHI consists of information regarding medical histories, test and lab results, mental health determinations, insurance, demographic, and other information collected by healthcare professionals needed for requisite care (Lutkevich et al., 2023). Finally, biometric data is data used to uniquely identify an individual by using the unique biological characteristics of that individual. Factors like the human iris, gait (how you walk), fingerprints, and facial features are strong examples of biometric data.

In discussing what kinds of data need to be protected and kept private, a new privacy law enacted in Europe cannot be ignored, the GDPR. The GDPR is a broad set of data protection and privacy laws enacted by the European Union. It has broadly affected how data from the E.U. is transferred and stored within and outside Europe and how user data (personal data) is treated (Kesan & Hayes, 2019, p. 243). An individual under the jurisdiction of the GDPR (E.U. citizens) is a data subject whose personal data, by definition and scope, is greater than other countries like the U.S. on privacy protections. Like the U.S., personal data includes PII, PHI, financial, and biometric data. Unlike the U.S., personal data also has special categories of data that cannot be shared without explicit permissions under the GDPR. These special categories include factors of "race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, health data, and data about a person's sex life and sexual orientation" (2019, p. 243). Data subjects include employees as much as customers and critically, whether inside or outside the E.U. (where data is stored and processed); if handling E.U. citizen data, companies must comply with GDPR rules (p. 244). Companies cannot take advantage of lax privacy laws in other jurisdictions outside of the E.U. as it would violate those rules, inviting fines and other legal measures to enjoin them into compliance. The GDPR, therefore, serves as a good role model for all-encompassing privacy protections that guard citizens against abuse by private corporations and business interests.

Within the U.S., other states have made substantial efforts toward defining and guaranteeing privacy within their jurisdiction. Some states follow a similar model to the Federal government's body of regulations and laws. Most states, for example, have a data breach, computer crime, and identity theft laws (Kesan & Hayes, 2019, pp. 269-290) on the books even though the Federal government defines similar laws, such as the Computer Fraud and Abuse Act (2019, pp. 45-47). The Federal government also defines rules that most states do not, such as Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley Act (SOX). However, exceptions exist, such as California's Cal Health & Safety Code § 1280.15 (2019, p. 271). Númenor can follow suit and enact specific laws/codes in line with most states, such as computer crime laws to discourage intra-state digital crimes and data breach laws to enjoin local companies to disclose dangerous personal information leaks. Specifically, the state of California 2018 passed the California Consumer Privacy Act (CCPA), which offers a robust set of privacy controls to further protect personal information from being shared without the individual's approval. The CCPA enshrines privacy rights through a right to know, delete, opt-out, right to non-discrimination, and later starting in 2023 (CCPA was amended in 2020) to include the right to correct and limit disclosure of data being shared (General, 2023). The CCPA deals with privacy concerns and should be considered along with enacting other cybersecurity and data protection laws to give Númenor ample coverage of privacy and data security concerns.

An important consideration is determining whether the state of Númenor should pass legislation and regulations along the lines of other fellow states or pass something along the lines of the GDPR or California's CCPA. The GDPR is as strong as privacy laws can get and offers many advantages to ensure that private interests do not abuse our citizens' data. The CCPA is also a good model of privacy protection in the U.S. Númenor should shore up its local cybersecurity and data security laws and ensure its (if any) computer crimes, identity theft, and

data breach laws are enacted and up to date with the pace of digital crimes and thefts today. The state should also explore the need for health data protection laws (like Cal Health & Safety Code § 1280.15) and further explore the utility and need for privacy protections like the CCPA or GDPR. While Númenor should encourage and caucus with other states seeking more comprehensive laws from the Federal government, it should ensure its local laws are updated and ready to handle cybersecurity data and privacy concerns within its jurisdiction first.

References

General, Office of the Attorney. (Feb. 15, 2023). "California Consumer Privacy Act (CCPA)." State of California – Dept. of Justice. https://www.oag.ca.gov/privacy/ccpa.

Kesan, J. P. & Hayes, C. M. (2019). Cybersecurity and Privacy Law: in a nutshell. West Academic: St. Paul, MN.

Lutkevich, B., Wallask, S., & DelVecchio, A. (2023). "What is PHI (Protected Health Information)?" TechTarget: Health IT. https://www.techtarget.com/searchhealthit/definition/personal-health-information.

Paine, C., Reips, U.-D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions.' International Journal of Human-Computer Studies, 65(6), 526–536. https://doi.org/10.1016/j.ijhcs.2006.12.001.