Privacy Laws Regarding the State of Númenor

Liam Redman 01214332

CYSE 406

October 29th, 2023

To: Governor Tar-Míriel

From: Liam Redman

Subject: Privacy Laws

Date: 10/29/2003

Privacy is a significant issue in the current era with the use of widespread technologies and the consolidation of personal information into these technologies. Unlike previous centuries, many citizens' data is now stored in extensive digital databases. Ensuring this information stays private and in the right hands is of utmost importance. This can be best done by enacting digital privacy laws that can outline a legal framework for businesses and institutions to follow. These rules ensure that our citizens' data is stored in safe hands. These laws will protect sensitive details, like address names, and essential financial data, like bank account passwords, from unauthorized access. Without these laws and safeguarding procedures, citizens can fall victim to many different digital attacks. These can include identity theft, fraud, doxing, and other malicious acts. Today, the most common owners of these databases are large corporations and financial or governmental institutions. Setting rules and standards for these companies to secure your citizens' data will ensure you protect your citizens from unwanted digital attacks.

Currently, there are two main types of data stored in digital technologies: biometric data and PII (personally identifiable information). Biometrics use our distinctive physical and behavioral traits to identify who we are. This data needs to be stored and kept in databases to identify us. These databases can hold our fingerprints, eyes, faces, and voices to determine us. For example, when you log on to your phone now, it uses your biometric face or fingerprint data. To identify you, they must store that data to compare it with the input data. PII is data that can distinguish and pinpoint an individual, like phone numbers, email or home addresses, and social security numbers. For example, when you log on to social media accounts, they usually ask you

for your email and a password. They ask for your email to identify which person's account to log onto. This data is all stored on digital databases connecting people with their email addresses to identify them.

The General Data Protection Regulation (GDPR) is a new European Union privacy law that took effect on May 25, 2018. This privacy law provides organizations with guidelines and a framework to collect and store information on EU citizens. It applies to any institution or company that deals with the data of EU citizens, regardless of where that company operates. Even if your company is based and operated in China, you still need to follow these rules and regulations when dealing with data from EU citizens. For example, many companies will sell their databases of information they collect from clients to advertisers or the highest bidder. With GDPR, companies must lay out the information they collect and ask for your consent to let this happen. The GDPR also has rules on how companies store your PII. PII now must be kept with encryption. These rules help give your citizens control over their personal information and ensure companies are fair and secure with the confidential information of citizens.

Most countries have now enacted digital privacy laws, as it is becoming a vast and prevalent issue. The GDPR was not the first of its kind; many laws like this have been enforced worldwide for years. However, in the USA, there is no single law that regulates digital privacy due to the inaction of the federal government. This has created many problems and complex legal situations because of the need for more rules and regulations. Many states have taken the matter into their own hands to protect their citizens' data and privacy. The state with the most online protection and best digital privacy is California. This is due to the implementation of the California Consumer Privacy Act (CCPA). The CCPA imposes requirements on companies handling data and gives California citizens special rights surrounding their personal information.

California citizens have rights under the CCPA to seek the deletion of their information, to know what personal information is being collected about them, and to refuse to have their information sold to third parties. Just like EU citizens with the GDPR, California citizens can now have a say on how their personal and private information is held.

Enacting digital privacy laws is crucial in today's technologically advanced era. With the widespread use of digital technologies and the centralization of personal information in large databases, safeguarding privacy has become paramount. These laws establish a legal framework businesses and citizens can follow, ensuring that sensitive information remains in trusted hands. Without such protections, individuals are vulnerable to various digital threats, including identity theft, fraud, doxing, and other malicious acts. By implementing digital privacy laws, we empower individuals to have greater control over their personal information and hold organizations accountable for safeguarding their data. This not only protects citizens from unwanted digital attacks but also creates trust in the digital world. Just like we see in California and many other states, enacting these laws will do good for your citizens. Waiting for the federal government will do nothing but waste time and keep your citizens at risk.