

# Cyber Law Writing Assignment

By: Bradyn Ritchie

CYSE 406

3/15/23

To: Governor Tar-Míriel

From: Bradyn Ritchie

Subject: Privacy Concerns

Date: 3/15/2023

Hello Governor Tar-Míriel,

In regard to your questions about privacy:

In short, privacy is a right that many individuals have in order to control the access to information about themselves. As you can imagine, this is an extremely controversial topic, especially as the world relies on new technology and the constant development of the Internet. Many different individuals lobby for data privacy related regulations and legislation due to the various concerns that they have. For example, no one would want their sensitive medical records or financial information spread to third parties that do not require it. They would only want the necessary people to have access to this information, such as a family doctor, physician, or themselves. Many current privacy laws regulate what specific information individuals and organizations may collect, how that information can be used, and potential punishments if these regulations are broken (*Importance of data privacy laws explained*, 2022). Without privacy protection laws in place, companies and businesses would be able to make a profit off of users' and customers' potentially sensitive information that they have collected. Also, anyone may be able to request someone else's information. In addition to this, depending on what information is shared, individuals may become victims to various types of fraud, such as identity fraud.

Biometrics are simply physical characteristics that make a person unique, such as their retinas, voice, fingerprints, and much more. These can all be used to identify a specific person, as no other individuals have the same matching attributes. However, in order for identification to be successful of course, the person being identified must have a record of their biometric in the identification service. When stored in an authentication system, this record is more commonly known as their biometric data. Due to their originality, biometrics is widely considered to be a form of personally identifiable information, also known as PII. PII is a piece of information that can be used to successfully identify an individual. However, it's also important to note that some factors that are not PII by themselves may become PII when combined with other pieces of identifying information. Some common examples of potential PII include an individual's date of birth, first name, last name, street address, and social security number.

The General Data Protection Regulation (GDPR) is a strict privacy law that was created for all the nations located within the European Union and all countries located within the European Economic Area (*General Data Protection Regulation (GDPR)*). Every citizen within

the European Union is covered and protected by the GDPR. Under the GDPR, any information that can potentially be utilized to identify an individual is protected, such as the more obvious PII mentioned above to a person's cookies that are stored within their web browser, and much more. In order to be effective, the GDPR is built upon seven main principles to protect citizens' information. These principles regulate numerous aspects of the information, such as how long companies can store information on an individual, what measures must be taken to protect this data, and how the data is permitted to be processed by third parties, if need be. However, it's also worth noting that citizens in various other countries may be affected by the GDPR as well, such as when visiting websites that are hosted within the European Union. In addition to this, international companies must comply as well if they sell goods or services overseas to citizens within the European Union.

In recent years, many states within the United States have set forth legislation in order to better protect their citizen's privacy and sensitive information. For example, in Illinois, the Biometric Information Privacy Act (BIPA) was recently passed, which is meant to regulate how biometric information is stored, collected, and utilized by various organizations located within the state of Illinois. Numerous other states have adopted similar laws related to access of biometric information, including Washington, Maine, Texas, and New York. Other types of privacy related legislation has been enacted in various other states as well, such as ones pertaining to consumer information, data brokerage, and the protection of minors online. These include the California Consumer Privacy Act, Vermont's data brokerage law 9 V.S.A § 2446-2447, and Delaware state Code § 1204C (*State laws related to digital privacy*, 2022).

I believe that you should certainly push to enact a personal information or data protection law rather than wait for the federal government to pass a similar law. Having at least some form of privacy protection for citizens would certainly be better than none at all. It could take the federal government potentially years in order to pass an all encompassing privacy protection act such as the GDPR. If they have not already proposed a bill, I doubt they will in the near future. However, the American Data Privacy Protection Act is expected to be passed in the coming years in order to provide a nationwide framework for new privacy regulations (*The American data privacy and protection act*, 2022). Personally, I feel like enacting a federal law similar to the GDPR would be significantly more beneficial than the patchwork of privacy laws that each state's government develops. It would provide a much more uniform set of statutes for both citizens and companies to better understand and follow. However, state issued privacy laws have their advantages as well. State laws are much more likely to reflect the wants and needs of the citizens better than the national law, due to the states servicing a smaller number of individuals as opposed to the federal government (Bowers, 2018). Therefore, the laws can be more finely tweaked in order to meet the majority of citizens' needs within that specific state or territory. According to Security Week, if the government enacts a federal privacy law, it will most likely be more business oriented rather than focused on the consumers or citizens of the nation (Bowers, 2018). As I stated above, I believe that one uniform privacy law is significantly more effective than the various different laws throughout the states. However, it would certainly be

beneficial to enact a state law in order to sooner resolve the privacy concerns that the citizens of Númenor express. This privacy law that the state of Númenor may enact could be similar to the GDPR and cover a broad spectrum of privacy issues throughout the state, or numerous smaller laws can be implemented. Either way, it should cover many of the citizens' concerns, such as the collection and use of their biometric data and PII.

## Works Cited

- Bowers, K. (2018, November 13). *State vs. federal privacy laws: The battle for consumer data protection*. SecurityWeek. Retrieved March 10, 2023, from <https://www.securityweek.com/state-vs-federal-privacy-laws-battle-consumer-data-protection/>
- General Data Protection Regulation (GDPR)*. (n.d.). Tufts University. Retrieved March 9, 2023, from <https://access.tufts.edu/general-data-protection-regulation-gdpr>
- Importance of data privacy laws explained*. (2022, May 24). DataGrail. Retrieved March 8, 2023, from <https://www.datagrail.io/blog/data-privacy/importance-of-data-privacy-laws-explained/>
- State laws related to digital privacy*. (2022, June 7). Legislative News, Studies and Analysis | National Conference of State Legislatures. Retrieved March 2, 2023, from <https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy>
- The American data privacy and protection act*. (2022, August 30). American Bar Association. Retrieved March 10, 2023, from [https://www.americanbar.org/advocacy/governmental\\_legislative\\_work/publications/washingtonletter/august-22-wl/data-privacy-0822wl/](https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/august-22-wl/data-privacy-0822wl/)