WRITING ASSIGNMENT 1

BY: BRYANT WATKINS

OCTOBER 25, 2024

CYSE 406

Prof: Amanda L. Cheney, Esq.

Memorandum

Date: 10/25/2024

To: Governor Karras

From: Bryant Watkins

Subject: Privacy and data protection

Why Care?

Data privacy and protection is one of the most important aspects of handling data. Whenever people have data that is shared with a domain – there is generally an expectation that the data will be protected and not used for nefarious means. The most consequential form of data is typically what is known as Personally Identifiable Information. Personally Identifiable Information is any information that may be used to identify a person, examples include – name, address, social security number, ethnicity, phone number, etc. Given the prevalence of technology in the world – Personally Identifiable Information is typically stored digitally, though it may be stored on paper as well.

It is crucial to care about the privacy and protection of data because the mishandling of critical data could result in various crimes, with identity theft or fraud amongst some of the most common. Risks are not limited to digital crimes, if someone has their address revealed then that creates the potential for criminals to physically target their residence and attempt bodily harm – something typically seen with higher profile individuals such as political leaders and celebrities. The potential for crimes is only one aspect of the importance of data privacy and protection, the potential for lawsuits as well as reputational hits against companies and governments commonly stem from the mishandling of consumer data. A data breach is something that can cripple a company and put millions at risk of being victims of devastating crimes.

Breakdown of Terminology

There are numerous terms and phrases that crucial to a complete understanding of user data privacy and protection. A term that is commonly used when discussing data is *Biometric* – Biometric data is any unique physical characteristic used to confirm the identity of an individual. Common examples of Biometrics include – Iris scan, Fingerprint scan, voice recognition, and face scan. Arguably the most crucial law to data privacy and security is what is call *General Data Protection Regulation* (also commonly referred to as the acronym GDPR). GDPR is believed to be the “toughest privacy and security law in the world” (GDPR.eu), and even though it was developed in Europe – the implementation of this law reverberates across the world. GDPR seeks to protect the data of all individuals residing in Europe regardless of where said data may be stored and thus provide individuals with added control of their data. There is also severe fines for any individual or organization that is observed to be in violation GDPR regulations or principles.

Data processing is another commonly used term. Data processing refers to “any action performed on data, whether automated or manual” (GDPR.eu). Common examples of data processing include – storing, erasing, modifying, or transferring. *Data controller* is a term that refers to the individual responsible for the handling of personal data, for example – any owner, manager, supervisor, or employee who oversees the handling of critical personal data. *Data processor* is a term that refers to any third party organization that is responsible for the processing of personal data on the behalf of the data controller. Common examples of data processors include cloud servers such as – Google Drive, Proton Drive, Microsoft OneDrive, or Proton Mail (GDPR.eu).

Additional Data to Potentially Enact

There are multiple types of data that unfortunately are not fully covered by federal law. Health data is big one, the Health Insurance Portability and Accountability Act (HIPAA) is simply not comprehensive enough since it provides zero protection of personal health information obtained by third party applications and wearable technologies such as *Fitbit* or *Apple Watch* (epic.org). Children's data is also greatly exposed, Children's Online Privacy Protection Rule (COPPA) simply covers applications or sites specifically geared toward children under 13 – leaving a gaping hole if sites or applications are not directed at children but still collects their data knowingly or unknowingly (epic.org). Location data is one that is commonly overlooked or forgotten. Unless there are known deceptive or unfair practices that fall under the authority of the Federal Trade Commission (FTC) or violates Federal Communications Commission phone carrier rules – there are little to no protections for location data handled by mobile devices or applications (epic.org).

Student data is susceptible as well due to a lack of federal protections. The Family Educational Rights and Privacy Act provides protections for personal data collected by educational institutions – but does not cover student data handled by third parties (epic.org). Online activities may be the biggest of all considering how common internet usage is. Unless proven deceptive or unfair, which would fall under the protection of the Federal Trade Commission, very little protection is offered for users of online activities (epic.org). Given these loopholes in personal data protection, there is a plethora of types of personal data that should be included in the State of Mongo Legislature that currently are not fully covered by federal protections.

The feasibility of any wide scale data privacy and protection is ultimately dependent on monetary assets and pure manpower. Implementing expansive and far-reaching laws or regulations such as the GDPR is incredibly feasible for wealthy developed nations and regions such as the United States or Europe. For poorer, underdeveloped, or smaller nations with limited resources – legislation on the scale of GDPR is simply not possible. Not only must one take into account the initial costs to develop and implement legislation, but said legislation must constantly be maintained and upgraded over time to be capable of effectively adapting to the ever-changing landscape of personal data threats.

Protections provided by laws such as the GDPR certainly have their benefits. Some prominent benefits include – building trust among consumers, preventing expensive and damaging data breaches, and enhanced data migration. There are certainly detrimental aspects to implementing comparable regulations as well that must be taken into account. Some of the downsides of such regulations include – maintenance, costs, excessive regulation(s), and excessive fines/punishments. Ultimately, there is a delicate balance to strike when protecting personal data and this is certainly a matter the will require collaborative efforts of executives, professionals, experts, and even consumers themselves.

References

“Biometric Data.” *Innovatrics*, 7 Nov. 2023, www.innovatrics.com/glossary/biometric-data/.

“What Is GDPR, the EU’s New Data Protection Law?” Edited by Ben Wolford, *GDPR.Eu*, 29 Aug. 2024, gdpr.eu/what-is-gdpr/.

Fitzgerald, Caitriona, and Suzy Bernstein. “Full of Holes: Federal Law Leaves Americans’ Personal Data Exposed.” *EPIC*, 27 Apr. 2023, epic.org/full-of-holes-federal-law-leaves-americans-personal-data-exposed/.

Coos, Andrada. “GDPR: The Pros and the Cons.” *Endpoint Protector*, 10 Dec. 2020, www.endpointprotector.com/blog/gdpr-the-pros-and-the-cons/.