WRITING ASSIGNMENT #1

MARCH 23, 2023

JASON RIVERS
Cyber Law | CYSE 406

What are Privacy Laws/Data Protections?

Hello Governor Karras, I have reviewed your questions, and am entirely willing to answer them, and give any assistance I can, on the condition you make some changes to Mongo's policies regarding privacy. After I explain it all, I think you'll see why so many people under your constituency are as concerned and outraged as I am about this.

To begin, privacy laws and data protections are designed, and implemented to protect people first and foremost from their government, and secondly from their own fellow citizens. Important private information and documents are restricted to that person's access, or in some cases, a person they designate like a spouse, or parent for citizens that aren't yet of legal age. Entities like corporations or businesses are also affected by a type of privacy laws falling under data protection, designed to outline how they need to protect and store consumer data so that confidential information does not leak, and potentially damage that consumer. Without these privacy and data protection laws in place, people could steal our personal information, and use it to damage us, potentially frame us for different crimes, or use it to assume our identity, among other things. Because of these reasons, the privacy concerns of your citizens should be a top priority for your term in office.

Types of Private Information

It's very easy to talk about privacy and data protections, and why it's important, but now we need to explain what that data is. One type which is highly contested, and widely defined is "biometric data". Generally, "biometric data" is considered any way of recognizing you from your biometric information, including fingerprints, iris or retina scan, voice, or facial shape. This sort of information is regulated different depending on where you go, but it is very important to keep it protected and private. If people’s biometric data is widely available, it could be used to frame them for a crime, bypass some security measures they or their company have, or to identify them in other context. Usually, biometric data is only available in government record, and maybe medical records as well, both of which are generally kept private (Kesan & Hayes, 2019).

Another example of highly confidential information is Personal Identifiable Information, or PII. PII is any information which can be used to identify a person, whether directly, such as a social security number or a driver’s license number or indirectly, such as ethnicity, age, or occupation. Generally, PII is important for employees in the government sector, or for people involved in law enforcement, to protect their families, and self. It’s important to keep this information private and confidential, otherwise it can be used to pressure or otherwise harm government employees, law enforcement, and the like (Kesan & Hayes, 2019).

One type of data that is protected and doesn’t usually require direct governmental protection is medical information, which is protected by many different federal privacy laws. One of the most comprehensive is the Health Insurance Portability and Accountability Act, or HIPAA. Essentially what it does is it protects your medical information from being disclosed without your consent; you can sign off to have medical professionals, or family members access it. Without protections like HIPAA, anyone could go into a doctor’s office or call an insurance provider, and ask for your medical information, or anyone else’s medical information. Not only that, but many protections currently in place might not exist, making it too easy for someone to steal it, rather than simply ask for it (Kesan & Hayes, 2019).

Now, obviously our data isn't just under threat of being stolen by citizens of Mongo, or even of the country. The threat is international in nature, and anyone can fall victim to it without privacy protections in place. Even if they are in place, there is still the threat of an international actors accessing our private information. An example of something in place to protect against international threats would be The EU's General Data Protection Regulation, or the GDPR. Going into effect in 2018, this comprehensive regulatory framework helps to clarify some concepts, give examples to some more complex issues, and even allows some EU states to deviate from the regulations, if the issue of privacy is being promoted as a result of the deviation. The GDPR enforced personal privacy for citizens of the EU, and to an extent worldwide, requires companies, and governments to have secure processes in place to safeguard, handle and, if needs be, transfer people's personal information. It also established individual privacy as a protected human right (GDPR, 2022).

The EU also has a much more comprehensive definition of "personal information" than what is outlined in some states. Information like location, online usernames or identifying information, information regarding a person's psychological state, genetic material, economic or ethic information, and many other pieces of information are protected under EU law. They even include a list of special categories of information regarding potential occupation, political leanings, beliefs, and other information. This comprehensive, and broad definition of personal information protects many aspects of a person's identity, including information that could indirectly identify them, or be used against them in various circumstances. I believe Mongo could stand to benefit from a defined protections not unlike the EU's.

Personal Data Protections of Mongo

To begin with, I believe Mongo requires a vast overhaul of what they define as personal data. Some other states have a very lax definition that may not provide sufficient protections. Mongo needs to very clearly define what it defines as personal information, so that it does not slip back into its old ways where private data protections were either non-existent, or barebones. Information like medical info, PII, biometrics, and various other information is already protected under federal law, but we can continue to build on it. Our main concern starting off would need to be implementing protections for what the federal government won't cover: consumer data, health information, financial information as well as educational information, and communication privacy. I think we need to have privacy concerns more robust than what is already on the table, but less complex than what the EU currently has.

One of the more controversial concerns is consumer data, which has been hotly debated for years. It should require consumers to be able to opt into having the data recorded and shared, not just allowing it to happen. It should also be minimized as well. If a person's consumer data can be tracked, it can be used against them by linking it to their financial situation, potential occupation, medical information, and many other types of information as well. It might not seem like a big deal to some citizens, but I think Mongo should address these issues as a foundational point going forward. It's something I believe we can build off of if we take the proper steps and implement these new privacy laws correctly.

Works Cited:

European Union. (2022, September 27). *General Data Protection Regulation (GDPR)*. GDPR-Info. Retrieved March 12, 2023, from https://gdpr-info.eu/

Kesan, J. P., & Hayes, C. M. (2019). *Cybersecurity and privacy law in a Nutshell*. West Academic Publishing.