Memorandum for the constituents of the state of Mongo

Nicholas Robertson

CYSE 406

October 25, 2023

Concerns with data protection

Data protection is the practice of protecting one's own data in how it is collected, moved, and used throughout the internet. People within the state of Mongo are concerned that their data is being used and harvested by companies and outside sources willing to use and sell their own data without their consent. Unlike federal laws like the Health Insurance Portability and Accountability Act (HIPAA) and the Family Education Rights and Privacy ACT (FERPA) which protects users from having their personal information in the forms of student records and medical records from being leaked out to the public, personal information and data like social security numbers, financial information, login credentials to banks and company organizations, etc. are not protected by any federal law, and can be used without the user's consent, nor knowledge. To put into perspective how impactful this could be for a citizen, if a citizen were to have their social security number stolen online by a criminal without them knowing. This criminal now has access to that citizens personal information and can open a bunch of credit cards in their name and ruin their good credit with the criminal most likely never being caught and tried for their actions. This is why the constituents and even the governing body that runs the state of Mongo should care, because if this is not taken as seriously in the future, then more and more people will loss their information and the confidence they once had to use the internet for there daily activities will soon dwindle.

Terminology

Governor Karras, as you have already heard through the tons of angry voice mails, the constituents of Mongo have been using terminology like PII, biometric data, GDPR and other terms that revolves around privacy protection laws. I'm here to explain what these terms mean, so that you can have a better understanding. To start off, PII is an abbreviation of Personal Identifiable Information, which relates to any data/information that relates back to a particular information. An example of this would be information like social security numbers, credit card numbers, drivers license, home address, etc. Biometric data is data that one produces through the information gathered from there DNA/biological makeup. This includes the information that is gathered from iris scans, figure prints, facial recognition, and voice recognition. The General Data Protection Regulation (GDPR) is a European Union based regulation that focuses on

information privacy laws and how information surrounding the citizens that live in these European countries are handled, stored, and processed, while also explaining the rights for the individuals whose data is being processed. In America we have a similar law/regulation to this called the California Consumer Privacy Act (CCPA), but as you can guess, this is not a federal law/regulation and is only applicable in the state of California, but it's just an example to give you a better understanding of what some other states have in our country. Theres also the data protection/processing agreement (DPA) which "is an agreement between a data controller (such as a company) and a data processor (such as a third-party service provider)." (Ironclad Journal). Essentially what this entails is that companies like The Home Depot, Walmart, Facebook, etc. are seen as the data controllers and they will collect user data for different sources like apps and websites. This data can vary from what websites does this user visit the most, how long has this user use a specific app, or the personal information of an individual. After collecting this data, they will pay another company like Amazon Web Services, Google, IBM, etc. to house this information within their own in-house storage facilities. The DPA in turn sets out standards and guidelines for how the personal data collected by the controllers are supposed to be stored, transferred, used, and safeguarded within the facilities of the data processors. If anything were to happen to the data within the supervision of any of these companies (i.e., a data breach) then the companies would be subjected to massive fines for the improper handling of user data. Now that we discussed the various terminology and you now have a somewhat better understanding of the concerns that people have when it comes to there personal data on the internet, lets move on to possible solutions.

Federally Protected Information

Before we can start talking about possible resolutions to the issues at hand, we need to understand what types of personal data that is and isn't protected by the federal government. We need to assure the people of Mongo that there are federal laws out there that are designed to protect their data and to give a quick explanation to them, we'll start off with the Health Insurance Portability and Accountability Act (HIPAA), which is designed to protect patents private identifying medical information. Theres the federal Genetic Information and Nondiscrimination Act (GINA), that prevents insurance agencies from raising your premiums

based on individual's genetic predisposition. The Gramm-Leach-Bliley Act (GLBA) is a financial safeguard put in place to protect individuals' financial information from being compromised in the event of a data breach or anything else that could jeopardize customers data. The Cable Communications Policy Act (CCPA) protects how their communications network is being used by their customers. The Children's Online Privacy Protection Act (COPPA) is a law enforced by the Federal Trade Commission (FTC) onto all websites hosting services, whether it be a social media website or a gaming website, to put up age verification, to keep children under the age of 13 from having their personal information harvested by tech companies. The Family Educational Rights and Privacy Act (FERPA) is designed to protect the private educational records of individuals so information like permanent records. Finally, we have the Video Privacy Protection Act (VPPA) which was originally a rushed bill to prevent others from knowing the video renting history without the original customer's consent. While this law doesn't seem too impactful now and days, it still seems to be repurposed to better suit the online landscape, in preventing companies from sharing and tracking users' personal information on sites and apps that provide video sharing content. This covers all the personal information that is federally protected under federal law, which mainly protects individuals' private information within companies and organizations, most of which either exist outside of the internet or has a loose connection to the internet. However, I want to now point out the information that is not protected under federal law and can range from sate law examples to not being protected at all.

State/Unprotected Information

Unfortunately, with how the online space works, any and everything that is uploaded on the internet, is up for grabs. As mentioned at the end of the last section, most of the protected information that had federal backing to them were mainly based on already preexisting organization that could stand separate from the online space. For instance, HIPAA has the hospitals, FERPA has the school system and GLBA has the financial institutions. With the exception of COPPA and eventually VPPA, these federal laws could stand separate from the internet. But unlike most of the information that is protected by these companies, there is absolutely no restrictions on what can and will be stolen and or used by other people and companies on the internet without the consent of the original person. As you might have heard,

the constituents of the state have suggested that we enact laws like the General Data Protection Regulation (GDPR) in Europe as it might help with data theft/data leaks within companies, by holding them to a higher standard when it comes to how the individual's personal information is handled. Quite frankly, that's not a bad idea, in fact it would qualm a lot of issues like transparency of data and fast response times to any issues a company might run into, while giving the public a more grounded reassurance that their data is being handled properly. But there are some flaws regarding the GDPR, for instance the vagueness of how the law is set up is an issue with "Undefined terms such as "undue delay," "likelihood of (high) risk to rights and freedoms" and "disproportionate effort" … "Similarly, the regulation offers no definition of what constitutes a "reasonable" level of protection for personal data" (Thomson Reuters). There are other concerns, regarding the strain of meticulous making sure that every individual data that the companies have access too is maintained, protected, and properly handled from the time they receive the data up until it is destroyed, and the heavy fines the companies will face if they do not comply with the GDPR's standards. But while these can be seen as faults and expectations of the companies that these rules apply too, there is an argument to be made in how the law itself should be better explained and written by a person who knows more about data protection practices, to give a bit more clarity to the people trying to follow these laws. So again, while I believe that a regulation like this could work, we will need to rewrite the rules to make them clearer to understand and even after we do that, we will most likely face backlash from these companies, as they will be reluctant to follow these rules. I believe that the state of Mongo should put our efforts in creating a consumer data protection act and follow in the steps of our fellow states like Virginia, California, Colorado, Connecticut, and Utah. This will allow for individuals of the state of Mongo "to access and delete personal information and to opt-out of the sale of personal information, among others." (NCSL, 2022). This will help put peoples fears of their personal data being out of there control to rest. We should also look into implementing the Biometric Information Privacy Act (BIPA) as a state law, as it's designed to keep private companies from identifying and tracking individuals based on their biological make up (i.e., figure prints, facial recognition, and iris scans).

Conclusion

Governor Karras, to conclude with this memorandum, I believe that we should not hesitate, and quickly implement the Mongo Consumer Data Protection Act (MCDPA), the Biometric Information Privacy Act (BIPA), and we should make a new state law that take the elements of the GDPR and condenses it down so that it can apply to a state level, while adding more clarification for the companies trying to follow it. It would be in our best interest to implement these changes within the coming weeks so that the people's unrest may subside, and we can get back to some form of normalness.

Quotes:

“What is a Data Processing Agreement (DPA)?” Ironclad Journal

https://ironcladapp.com/journal/contracts/what-is-a-data-processing-agreement-dpa/

“Top five concerns with GDPR compliance.” Thomson Reuters

https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance

“State Laws related to Digital Privacy.” (June 07, 2022) NCSL

https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy#:~:text=Five%20states%E2%80%94California%2C%20Colorado%2C,of%20personal%20information%2C%20among%20others.