The State of Mongo Memorandum

Peter MacMillan

CYSE 406

03/23/2023

As we understand it, data protection and privacy issues are everywhere in our society. We see threats to information security every time we log into computers or watch it unfold in the news. Countries waging cyber warfare on other countries because of past relationships or even current ones. All data must be protected and secured regardless of whether or not relationships are good. Both national security and state security are of the upmost importance and can lead to disastrous conditions if any information is leaked or hacked. Data protection and privacy are one of the most important components of a state or country. Each one has information about themselves that's worth protecting. Some examples of privacy concerns and issues revolve around data and information as a whole. We all know about data breaches and know that they aren't committed just for fun. This is a way for any outside influence or group to gain information about the state or country that might oppose, or the group has a problem with. Data breaches serve as a way to get into servers that may contain valuable information and use that as leverage over a country, state, or entity. Trade and company secrets fall under the data breach section because these files may be located in these servers under more complex encryption but are still somewhat accessible. Cyber fraud is another example of a data protection concern. Again, these outside groups or influences may hack into servers and take financial information and any other personal information from different devices and use it for their own means. With that comes identity theft, which can ruin many lives if it happens. Constituents should care about this information and data protection because much of their information and employment information might be stored on these servers and in the wrong hands, this can easily result in turmoil and disaster. While these things might be protected, each way of encryption has its flaws and cybercriminals are paid to exploit those weaknesses. Everyone, constituents and civilians,

should be worried and care about the event of a breach and should take care to secure all things that may be important when it comes to information.

The constituents bring up a good point with references made to certain information types and what each of them are. Each state has their own definition of biometric data, as is required. With all definitions in mind, biometric data can easily be defined as physical characteristics of an individual that can be used for automated access to certain things. Things like fingerprints, voiceprints, iris/retina scans, and hand or facial geometry scans are considered to be biometric data. PII, or personal identifiable information, are also forms of information that should require data protection and privacy. PII can be defined as any information that can be used to identify an individual. Examples include social security numbers, street addresses, phone numbers, and even credit card numbers, but the list goes on. Of course, we all know about how financial information is and will be protected. Even financial information is vulnerable to breaches and cyber-attacks and should be protected just like any other. Financial information is anything that is used to purchase goods or services for an individual or group of people. Types of this information are bank accounts and statements, credit and debit cards, checks, loan information, school/university accounts for students, or even government approved spending reports. This was not mentioned by the constituents above, but it is one of the most important collections of information that a state can store and keep track of. Health information is usually protected right off the bat and the state adds some help to the federal protections in place already. Medical history and genetic information are just a few examples of health information.

Looking back at what types of personal data and other information covered in this memorandum, biometric data and financial information, both state and civilian, must be protected if legal policies about data protection and privacy are to be established within the state.

Just about everything else is covered by federal laws that are already in place. When considering other policies or laws that can be useful in data protection and privacy, GDPR, or general data protection regulation, is one that stands out the most. This is a way to observe how information that is collected is processed and controlled. However, GDPR deals mainly with physical information rather than personal identifiable information. The information that is covered by this process includes; name, identification number, location data, online identifiers, and any factors, physical, genetic, mental, etc., to a data subject. Currently, this is only something that exists in the EU, or European Union. If we were to adopt something like this, we could see a greatly increased security of information and how this information is stored, used, and deleted. Along with these safeguards with information, GDPR requires certain security measures to ensure that this information stays safe. A big part of this is the requirement of having a data protection officer. The officer oversees much of the processing and storing of this information and is called upon to report to higher powers when a breach occurs. Having a policy like this in place could very much change the scope of information security and could easily be adopted in the United States or any other country in the world. The EU has been trying to get the States and certain companies to transition over to their policies and ideas for the betterment of the future.

References

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