Data Privacy Memorandum:

Governor Karras

Jasmyn Wilhelm

Department of Cybersecurity, Old Dominion University

CYSE 406: Cyber Law

Professor Cheney

27 October 2023

Data privacy and protection concerns have heightened since technology has evolved and become the main source of information. Not only is it used for work, but some places only accept paying from a bank account or card online instead of going in person. While the convenience is there, the protection isn't always there. The concern with this topic is hackers getting that bank account or card information or using the data to steal someone's identity. Places will ask you to input your social to confirm your identity, but if that isn't protected, then it could be anyone. Females are cautious when walking down the street during the day and especially at night. Location information gotten by the hackers could make someone petrified in their own home too.

To elaborate more on the Mongo voters' concerns, I would like to explain what the specific concerns listed mean or entail. Biometric data is a unique way to directly identify a person. This includes but is not limited to, facial recognition, which iPhones use to unlock the phone and access card information to make sure it is you who is about to use the card. Fingerprinting, eye scanners, and voiceprints are other ways this can be used. Navy Federal is an example of this, as they set up "My voice is my password" to get access to your account over the phone.

PII stands for Personal Identifiable Information, which can range from many things, such as employment information, a home address, an email address, and a Social Security number. While it may seem obvious why you would not want someone to access this information, another thing to consider is that just one piece of this information can lead to so much more. Getting information about your mother's maiden name is one step closer to a hacker getting the rest of the information or access to a bank account.

Another demand brought up by the people is GDPR. GDPR is a law that was passed in Europe in 2018 and protects the privacy and data of citizens of the EU, even if they were not located in the

EU at the time. The GDPR sets very specific standards for data privacy and protection and delivers very large penalties to those who do not follow them. Another article in the GDPR is "The Right to Be Forgotten," which states that the subject has the right to request to be erased from an organization's database. This is not a guarantee and can take about a month to complete, but essentially, if the organization's data collected on a member is no longer necessary, they can request for it to be erased.

Additional laws can be put into place by the state itself, but it has proven to be more difficult as only five states currently have additional privacy laws to go with the federal law. For example, California passed the California Privacy Rights Act in 2020, which entails the right to correct inaccurate information, certain information that must have special privacy and protection, like social security numbers, and the right to limit the disclosure of sensitive data. These laws could help the state protect the citizens of Mongo. An act that can limit the amount of time a company can hold onto such information could also be useful.

Overall, the privacy of citizens is a priority, as people should feel safe going to a doctor's office without worrying about the information being sold to another company or risking being put on the black market for people to steal. All it takes is for one person to get enough information to ruin someone's credit and hurt their livelihood, which can make or break the economy depending on the severity of the people being affected. Companies should be held responsible for the sensitive data that they hold, as the next person that could be affected could be you. As technology evolves, hackers adapt to get the information they are after, so why shouldn't the state demand the same? Complying with the demands will take a toll as it will take effort, and small businesses may struggle to implement items such as GDPR as they are trying to get off the

ground. Complying with the same policies could be costly, but ultimately, citizens want to feel safe. If we have laws for citizens to follow regarding safety with driving, theft, etc., then companies should follow the same with the protections of the people who are going for help, whether at a hospital or bank. I urge you to look over this document and consider their concerns with this new information. All their demands may not be feasible at the state level and may take time and effort, but nothing will change unless we try to make them happen.

References

Guide to identifying personally identifiable information (PII). Guide to Identifying Personally Identifiable Information (PII) | Information Technology | University of Pittsburgh. (2022, April 18). https://www.technology.pitt.edu/help-desk/how-to-documents/guide-identifying-personally-identifiable-information-pii

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

Staff, O. (2023, July 6). *Data Privacy Laws: What you need to know in 2023*. The Intuitive Data Privacy Platform for Simplifying Compliance. https://www.osano.com/articles/data-privacy-laws

Wolford, B. (2023, September 14). *Everything you need to know about the "right to be forgotten."* GDPR.eu. https://gdpr.eu/right-to-be-forgotten/