Old Dominion University

Data Privacy Memo to Governor

Writing Assignment Spring 2024

Evan Jenkins

Cyber Law 406

Professor J. Klena

March 16, 2024

To: The Governor of the Commonwealth of Virginia

From: Evan Jenkins

Subject: Privacy and Data Protection

Date: March 16, 2024

For the citizens of your constituency, privacy is the fundamental right to manage their personal information. With a world that is increasingly dependent on the Internet, it is now more important than ever to push for comprehensive and codified protection of this right. This also means there is a growing number of criminal actors trying to illegally profit by violating your citizens' privacy and stealing their Personally Identifiable Information, as well as other sensitive data. Any type of information that could be leveraged to identify an individual is considered to be Personally Identifiable Information (Klena). Examples of this could be a person's name, phone number, account numbers, any form of government-issued IDs, even biometric data such as fingerprints, and a wide range of other information forms, depending on the specific scenario. Pew Research Data shows that Americans are concerned about their privacy and data. 81% of Americans responded that they were concerned about the use of their data by companies, and 71% were concerned with how the government used their data (McClain et al.). The majority also express a feeling of having no control over how their data is managed. The same poll also found bipartisan support for increased regulation on corporate use of collected data. Their concerns are more than justified as over a third of the respondents answered that they had faced fraudulent charges, had a social account or email hacked, or had credit fraud attempted with their name, in just the last year (McClain et al.). The Pew Research also showed that the majority of

U.S. adults feel comfortable deciding on their personal data use, but only 21% felt confident in the ability of others to oversee their data. Each day that Virginia goes without a solution to securing the personal data of citizens, more Virginians will fall victim to their privacy being violated and crimes such as identity theft, credit card theft, blackmail, extortion, and cyberstalking. Additionally, Virginia will fall further behind other states such as Illinois and California, as well as European Union nations, which have the General Data Protection Regulation.

The General Data Protection Regulation was the European Union's solution for its citizens who had many of the same concerns as those in Virginia. The GDPR's main concern was personal processing data, which is defined as "any operation or set of operations which is performed on personal data or on sets of personal data" (Klena). It also characterizes the actors of data processing with the controller and the processor. The first is the entity that decides on the purpose of data processing involving personal data. The processor is an entity working for the controller and is processing the data. For example, an electronics store wants to send out a flyer notifying its customers of an upcoming sale. They give the contact information of their customer base to a printing company to make and mail the flyers. The electronics store is the controller as they determined how they would use the data, while the printing company would be the processor ("Struggling to Understand Your Obligations? Here's a GDPR Overview"). Each role is expected to uphold a list of principles regarding data protection, or they can be subject to fines or other punishments. The principles include being transparent with customers, collecting as little data as possible for the intended purpose, and ensuring that the data is not stored longer than it needs to be. They are also expected to take measures to protect the data (Klena). Before an entity can process data, it must meet at least one of six criteria. The processing must have the consent

of the individual whose data is being collected, or be necessary to enter a legal contract, be done to comply legally, be done for the safety or wellbeing of someone's life, be a public duty, or be considered another legitimate interest. The third major component of the GDPR is of the rights of the individual. The individual has a right to be informed, access, rectify, erase, or restrict the processing of their data. Data portability and the ability to object are also listed as rights (Kesan and Hayes 245). It is also important to note that GDPR protection is granted to EU citizens, whether the controller and/or processor is based in the EU or outside of the Union.

Other states across the nation have already enacted legislation to address data protection and privacy. In 2008, Illinois passed the Biometric Information Privacy Act, focusing on the processing of biometric data ("Biometric Information Privacy Act (BIPA)"). Other states have already written, or at least proposed, similar laws largely following the structure of the BIPA. Under the BIPA, individual citizens are put in control of their biometric data. Private companies are not allowed to collect biometric data without informing each individual on what data they intend to collect, and why they intend to collect it, and for how long the data will be stored. They must provide this information in writing and receive written consent from the individual before proceeding with the collection of data ("Biometric Information Privacy Act (BIPA)"). Companies are also banned from selling any collected biometric data. Illinois's BIPA also grants a citizen to take a company to court for violating the above requirements, which no other state currently does.

California has put in place legislation that in many ways reflects the principles of the GDPR, with its California Consumer Privacy Act of 2018. The CCPA regulations must be upheld by any for-profit organizations with the state, which reach a gross revenue of $25 million a year, collect data on 100,000 or more Californians, or earn at least half of their revenue from selling

information collected from residents of California ("California Consumer Privacy Act (CCPA)"). Californians have a right to be informed on the use of their personal information, to request the deletion of their information from databases, to correct and limit the data collected on them, or to completely opt out of the data collection altogether ("California Consumer Privacy Act (CCPA)"). The CCPA always lays out instructions for citizens to challenge organizations that they feel have violated their rights. There are also additional consent requirements for residents of the states who are less than 16.

Ultimately, in my opinion, it is time for you, as Governor of Virginia, to push for a personal information and data protection law here at the state level. I feel this course of action would be better than a federal level as it would provide flexibility and the power to craft a plan that considered Virginia's unique situation. Given the number of people with government-related jobs living in Northern Virginia on the outskirts of Washington, D.C., and the military presence with the Pentagon and Naval Station Norfolk, which is the largest naval complex in the world, their information could be highly desired by criminals due to their clearances and connections. The state legislature could cover additional protections and rights necessary within the Old Dominion state that could be overlooked at the Federal level. While a law at the Federal government level would provide a less complex legal system for organizations to navigate instead of dealing with each state's idiosyncrasies, the matter of data protection and privacy lies in returning power to the people. Even if federal protection is to come in the future, there is no disadvantage to the state to provide additional rights at the state level. The rights of Virginians can be secured now without waiting for the federal government to pass a GDPR level bill. Virginia has the opportunity to help lead the way for other states and to show a commitment to the protection of an individual's right to privacy.

Works Cited

"Biometric Information Privacy Act (BIPA)." *ACLU of Illinois*, 29 Apr. 2022, www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa. Accessed 16 Mar. 2024.

"California Consumer Privacy Act (CCPA)." *State of California - Department of Justice - Office of the Attorney General*, 13 Mar. 2024, oag.ca.gov/privacy/ccpa. Accessed 16 Mar. 2024.

"Federalism: Advantages and Disadvantages of Federalism | SparkNotes." *SparkNotes*, www.sparknotes.com/us-government-and-politics/american-government/federalism/section4. Accessed 16 Mar. 2024.

Kesan, Jay P., and Carol M. Hayes. *Cyber Security and Privacy Law in a Nutshell*. West Academic Publishing, 2019.

Klena. "Privacy Law and Data Protection." *Old Dominion University*, canvas.odu.edu/courses/152809/pages/module-6-power-point?module_item_id=5715811.

McClain, Colleen, et al. "Views of Data Privacy Risks, Personal Data and Digital Privacy Laws in America | Pew Research Center." *Pew Research Center: Internet, Science & Tech*, 18 Oct. 2023, www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws. Accessed 16 Mar. 2024.

"Struggling to Understand Your Obligations? Here's a GDPR Overview." *GDPR EU*, 15 June 2023, www.gdpreu.org/the-regulation. Accessed 16 Mar. 2024.