To: Governor Commonwealth of Virginia

From: Noah Salafranca

Subject: Privacy Laws and Protecting the Personal Information of Citizens

Date: 3/14/24

I hope this memorandum finds you well. As you're aware, Virginians are increasingly concerned about the lack of protection for their personal information, and your interest in understanding the issue and proposing legislation is commendable. To provide a comprehensive overview, I'll address the nature of privacy, the concerns related to personal information/data protection, and the significance of safeguarding citizens' data.

The right to privacy is an essential freedom that includes safeguarding personal data and preventing unwanted access. It means deciding what to do with one's life without outside influence. Beyond physical boundaries, privacy also protects a person's online presence, including conversations, online activities, and personal information. Data protection and personal information privacy concerns stem from the unapproved collection, usage, and possible abuse of people's personal information. Data like names, addresses, social security numbers, and financial information are examples of "PII" (Personally Identifiable Information), as is the collection of "biometric data," such as fingerprints or face recognition. Because biometric data may uniquely identify a person and is hard to alter if hacked, it poses special privacy issues. However, personally identifiable information (PII) is a broad category that includes various information that provides a comprehensive picture of an individual's identity and existence, making an appealing target for cyber threats. Citizens risk identity theft, financial fraud, and unlawful monitoring if they don't have proper protection. When biometric data is misused, it can result in invasions of privacy and, in the worst situations, incorrect tracking or identification.

The General Data Protection Regulation (GDPR) is a comprehensive privacy law applicable to European Union (EU) member states. It encompasses safeguarding people's personal information and lays down guidelines, including permission, restriction of use, data minimization, accuracy, storage restriction, integrity, and secrecy. Individuals now have far more control over their data according to the GDPR, allowing them to view, correct, delete, and limit how their data is processed. Additionally, it places severe requirements on businesses that handle personal data, such as responsibility, transparency, and notifying individuals of data breaches.

Numerous states have passed legislation in response to their recognition of the need to protect personal information and data. An example of legislation passed is the California Consumer Privacy Act (CCPA). The CCPA allows citizens to see, remove, and refuse to have their data sold. Businesses are required under the CCPA to seek express consent for data processing, provide information about their data practices transparently, and put in place appropriate security measures to protect personal data. Furthermore, if a corporation fails to maintain acceptable security standards, the CCPA creates a private right of action for customers to seek damages.

Another example of a privacy policy is the Texas Data Privacy and Security Act (TDPSA). The Texas Data Privacy and Security Act is a comprehensive privacy law designed to safeguard the personal data of its citizens. The TDPSA sets forth guidelines for the gathering, using, and disclosing of personal data by businesses in Texas. It gives people control over their data, including the ability to view, update, and remove personal information kept on them by companies. Businesses must also put adequate security measures to protect personal data from unlawful access, disclosure, or use, according to the TDPSA. The TDPSA also mandates that companies notify customers during a data breach and give them transparent and open

information about their data practices. The TDPSA's overall goals are to strengthen consumer privacy rights and encourage confidence in how Texas-based firms handle personal data.

You should pass a personal information privacy and data protection law. There are numerous strong arguments why you should prioritize enacting a personal information/data protection law. First, protecting Virginians' fundamental rights and privacy depends on this law. Due to the widespread gathering, usage, and sharing of personal data in the modern digital age, people are more susceptible to identity theft, privacy violations, and other malicious acts. By passing a comprehensive data protection law, Virginians may have more control over their personal information and provide clear rules for companies and organizations on appropriate data handling practices. Furthermore, a robust framework for data security will improve customer trust in the digital space, promoting innovation and growth. In the end, passing a personal information privacy and data protection law would show your dedication to protecting Virginians’ privacy rights.

References

California Consumer Privacy Act Guide, www.jonesday.com/-/media/files/publications/1/01/california-consumer-privacy-act-guide/files/california-consumer-privacy-act-guide-gdpr-handout/fileattachment/california-consumer-privacy-act-guide-handout.pdf. Accessed 17 Mar. 2024.

Team, The Investopedia. "General Data Protection Regulation (GDPR) Definition and Meaning." *Investopedia*, www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp. Accessed 16 Mar. 2024.

"Texas Data Privacy and Security Act – an Overview." *Davis Wright Tremaine*, www.dwt.com/blogs/privacy--security-law-blog/2023/07/texas-data-privacy-and-security-act-overview. Accessed 16 Mar. 2024.