


To: Governor Commonwealth of Virginia

From: Nicole Selo-Ojeme

Subject: Personal Information/Data Protection Concerns and Proposed Legislation

Date: 3/14/24

The basic right to privacy is the ability to limit who can access personal information about oneself. Protecting sensitive data, such as Personally Identifiable Information (PII), which comprises particulars like names, birthdates, social security numbers, and biometric data like fingerprints or facial recognition patterns, is a problem for personal information/data protection in the modern digital era (Schwartz, 2004). Citizens are susceptible to financial fraud, identity theft, and invasions of privacy if they lack proper protection. Unauthorized access to personal information, for example, may result in identity theft, monetary loss, or harm to one's reputation. Facial recognition patterns and other biometric data can be exploited for illegal access to secure systems or monitoring. 

When personal information is handled properly, it can preserve democratic order and protect individual privacy while putting restrictions on market policing, default regulations, data alienation, and exit rights. Under certain restrictions, personal data can uphold democratic order and protect individual privacy. These restrictions include those pertaining to default rules, departure rights, damages, and market policing (Schwartz, 2004).

The European Union (EU) passed the General Data Protection Regulation (GDPR) as a comprehensive data protection law to safeguard the personal information and privacy of its citizens (Tikkinen-Piri et al., 2018). It is applicable to all enterprises, regardless of location, that handle the personal data of inhabitants of the EU. The principles of data protection, which

include legitimate, fair, and transparent processing; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability, are only a few of the areas covered by the GDPR.

Businesses that provide services based on personal data are subject to the GDPR, which has practical ramifications for organizational structures, business plans, and technological advancements (Tikkinen-Piri et al., 2018). Businesses that offer services based on personal data face additional difficulties as a result of the GDPR, which will cost a significant amount of money and human resources to implement and train staff. The General Data Protection Regulation (GDPR) presents new hurdles for businesses even while it is expected to benefit them by providing consistency in data protection activities and obligations across the EU countries and by enabling more integrated EU-wide data protection policies (Tikkinen-Piri et al., 2018).

To safeguard its citizens' private information, a number of US states have passed privacy laws. The California Consumer Privacy Act (CCPA), which gives Californians particular rights to their personal information, is one well-known example. Businesses are required by the CCPA to provide information about the types of personal data they collect, how they use it, and who else they share it with. Additionally, it grants customers the ability to access and remove their data as well as to opt out of having their personal information sold (Stallings, 2020).

A new chapter in state data privacy and consumer protection law is marked by the California Consumer Privacy Act (CCPA), which gives California residents significant rights and safeguards surrounding the gathering, use, disclosure, and sale of their personal information (Stallings, 2020). In order to address concerns about data collection and usage in the era of big data, the California Consumer Privacy Act (CCPA) offers higher protection for conclusions made from personal data than the General Data Protection Rule (GDPR). While the data itself is

undoubtedly protected by the GDPR, some conclusions made from that data might not be as well protected (Stallings, 2020).

The governor must decide whether to support federal legislation or create Virginia's own personal information/data protection statute. By passing state-specific legislation, Virginia would be able to customize rules to address particular privacy issues and cater to the particular requirements of its citizens. For companies that operate in several states, it could potentially lead to irregularities and compliance issues.

However, supporting federal legislation would provide national consistency and universality in data privacy rules, which would facilitate business compliance and offer complete protection for all people of the United States. But federal legislation would take longer to pass and might even supersede state rules that are already in place, including whatever privacy protections Virginia might establish in the future.

In summary, carefully weighing the benefits and drawbacks of each strategy is necessary before deciding whether to concentrate on state-specific legislation or federal advocacy. In the end, the governor must strike a balance between commercial interests and the larger regulatory environment in order to protect the privacy of Virginia residents.

Resources

Blanke, J. (2020). Protection for 'Inferences Drawn:' A Comparison between the General Data Protection Rule and the California Consumer Privacy Act. .

<https://doi.org/10.2139/ssrn.3518164>.

Kesan, J. P., Kesan, J. P., Hayes, C., & Hayes, C. (2019b). *Cybersecurity and privacy law in a nutshell*.

<https://experts.illinois.edu/en/publications/cybersecurity-and-privacy-law-in-a-nutshell>

Schwartz, P. (2004). Property, Privacy, and Personal Data. *Harvard Law Review*, 117, 2056. <https://doi.org/10.2307/4093335>.

Stallings, W. (2020). Handling of Personal Information and Deidentified, Aggregated, and Pseudonymized Information Under the California Consumer Privacy Act. *IEEE Security & Privacy*, 18, 61-64. <https://doi.org/10.1109/MSEC.2019.2953324>.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2017). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Comput. Law Secur. Rev.*, 34, 134-153. <https://doi.org/10.1016/J.CLSR.2017.05.015>.