Data and Privacy Protection Memorandum to the Governor of New Virginia

Haley Potts

Department of Cybersecurity, Old Dominion University

CYSE406: Cyber Law

Professor Jude Klena

November 8, 2025

To: Governor of New Virginia

From: Haley Potts

Subject: Data and Privacy Protection Laws for the State of New Virginia

Date: Nov 8, 2025

Data Privacy and Why it Matters

Every person has the right to control what personal data about them is collected and how it is used and shared. In today's digital age, when people use social media, shop online, and walk past security cameras on the street, their data is consistently being collected. The concern for personal data protection occurs because, more often than not, users are unaware that their information is being collected, analyzed, and shared. It comes with no surprise that citizens are concerned about their digital lives being monitored or exploited by organizations, cybercriminals, and government agencies.

A lack of proper safeguards for personal data protection can lead to very serious consequences. A few of the main risks include cyberstalking, identity theft, and financial fraud. When the gate around a user's private data is left open, it may as well be inviting in unwanted guests to take advantage of easy access information. On top of that, misuse of data can lead to discrimination. An example of this is when businesses use personal data to deny employment, credit, or insurance based on biased algorithms. The reduction of privacy also destroys citizens' trust in their government and organizations. Once people begin to suspect that their private data is not secure, they might hesitate to take part in things like online commerce, engage in government programs, or share vital medical information with their health care providers. Fundamentally, privacy protection is about personal freedom, equality, and trust within society.

Biometric Data and Personally Identifiable Information (PII)

Biometric data is certain unique physical or behavioral characteristics that are used to identify an individual. A few examples of biometric data are fingerprints, facial recognition, voice patterns, retinal scans, and DNA profiles. Biometric identifiers are often used for security systems, access to mobile devices, and government identification. Although, the mishandling of this type of data poses a huge privacy risk because biometric traits are permanent and unique. Biometric identifiers cannot be changed, unlike passwords, and breaches can expose individuals to identity theft or permanent surveillance.

Personally Identifiable Information, conversely, is any type of data that can specifically identify an individual directly or indirectly. This data includes information such as social security numbers, names, drivers license numbers, birthdates, email addresses, and even certain combinations of data like gender and zip code. PII also includes digital identifiers like an IP address or geolocation data when this information is linked to a certain individual. The misuse of PII can have catastrophic results for individuals. Some of these are things like financial loss, emotional distress and the destruction of confidence in digital systems. Biometric data and PII are the foundation for identity in the digital age and must be properly protected.

The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) was implemented in the European Union in 2018. This data privacy and security law is one of the world's most robust and influential of its kind. The GDPR applies to all organizations that collect or process personal data of any individual located within the EU, regardless of where an organization is physically based. This means that U.S. companies that process data from European citizens must comply with the requirements of the GDPR.

The GDPR encompasses many different key data protection principles. It requires personal data to be processed lawfully and only collected for legitimate and specific reasons. Additionally, it outlines that only the minimum necessary data be gathered and the data be kept secure and not held longer than needed. The GDPR encourages individuals with the right to access their personal data, make corrections to errors, request deletion, and object to certain processing activities. Another key piece of the GDPR is that it establishes accountability by requiring organizations to exhibit compliance and alert authorities of data breaches. Organizations found to be in violation can be hit with fines of up to 4% of a company's annual revenue. That kind of money has made businesses around the world take privacy much more seriously.

What Other States Are Doing

The United States does not have a single federal privacy law that compares to the GDPR; however, many states have started creating their own frameworks for protecting privacy. The most prominent one is California's Consumer Privacy Act (CCPA) in 2018 and supported by the California Privacy Right's Act (CPRA) in 2020. These laws allow Californians the right to know what personal data companies collect, to request deletion, and to opt out of its sale to third parties. Additionally, the California Privacy Protection Agency was created by the CPRA to oversee compliance.

Virginia is a state that followed California's lead by passing the Virginia's Consumer Data Protection Act (VCDPA) in 2021. This allows consumers the right to access, correct, and delete personal data and opt out of targeted advertising. Other states like Colorado, Connecticut, and Utah have enacted similar laws which reflects a national trend toward improved individual privacy rights. The federal government has yet to act on this matter, but the individual state

efforts highlight a huge shift towards enacting a nationwide federal law to protect all U.S. citizens' data.

Recommendation and Conclusion

After reviewing the issue set forth, I recommend that New Virginia enact its own personal information and data protection law. New Virginia enacting this law would show leadership, directly respond to citizens' concerns, and protect individuals instantly instead of having to wait for uncertainty from the federal government. A privacy law for New Virginia could draw inspiration from both the GDPR and CCPA. Some of these inspirations could include requirements for clear consent, limits on data collection and retention, and the right for citizens to access, correct, or delete personal data. Robust enforcement and penalties for any violations would help establish compliance.

Some of the advantages of a state-level law include flexibility and timeliness. New Virginia can address its citizens' needs without any delay. However, there are some disadvantages. If every state in the U.S. enacts varying laws, then businesses will have to navigate a very tricky patchwork of requirements. On the contrary, one single federal law would provide consistency nationwide but may take years to pass and could end up weaker overall due to political compromise. New Virginia should pass its own protection law while also supporting any federal efforts to create a single national standard.

References

California Legislature. (2020). *California Privacy Rights Act (CPRA).* Cal. Civ. Code § 1798.100 et seq.

European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation).* Official Journal of the European Union, L119.

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

State of Virginia. (2021). *Virginia Consumer Data Protection Act (VCDPA).* Virginia Code § 59.1-575 et seq.