

Privacy and Personal Data Protection in New Virginia

STEVIE JOHNSON

CYBER LAW CYSE 406

PROFESSOR JUDE T. KLENA

NOVEMBER 6, 2025

Memorandum

To: The Honorable Governor of New Virginia

From: Stevie Johnson, Intern, Office of the Governor

Date: November 6, 2025

Subject: Privacy and Personal Data Protection in New Virginia

I. Overview

Privacy is the right of individuals to control the collection, use, and disclosure of their personal information. In the digital age, personal data is collected and processed by governments, businesses, and online platforms at unprecedented levels. According to Kesan and Hayes, the widespread use of networked technologies and data analytics has increased the risk of unauthorized access, misuse, and exploitation of personal data. Inadequate privacy protections can result in identity theft, financial fraud, discrimination, and loss of trust in both public and private institutions (*Kesan and Hayes 2022*).

Protecting privacy requires more than securing data, it also involves ensuring fairness, transparency, and accountability in how personal information is gathered and shared. As Kesan and Hayes explained, without strong legal safeguards, individuals lose control over their digital identities and sensitive personal information.

Recent incidents in New Virginia, where citizens financial and medical data have been exposed through data breaches, have heightened public concern. As more daily activities from banking to healthcare move online, personal data has become a valuable asset for both legitimate and

malicious actors. Citizens now expect their state government to safeguard this information as part of its responsibility to ensure public security in the digital age.

II. Biometric Data and Personally Identifiable Information (PII)

Biometric data refers to unique physical or behavioral traits such as fingerprints, facial recognition data, iris scans, or voice patterns used to identify individuals. Because these characteristics are permanent and unique, the misuse or theft of biometric data poses severe and lasting risks; once exposed, biometric identifiers cannot be changed like passwords (*Kesan and Hayes 2022*).

Personally Identifiable information (PII) includes any data that can identify or locate an individual, such as names, addresses, Social Security numbers, driver's license information, and financial account details. According to Kesan and Hayes, personally Identifiable information is routinely gathered and examined on various platforms, which increases its worth but also exposes it to potential security breaches and improper use. Strong privacy safeguards such as clear consent, limited data collection, and robust cybersecurity standards are essential to prevent harm to individuals and maintain public confidence.

Biometric technologies are increasingly used in workplaces, airports, schools, and smartphones, making them part of daily life. However, when databases storing biometric data are compounded as seen in several high-profile corporate breaches affected, individuals face long-term risks since their physical identifiers cannot be replaced.

III. The General Data Protection Regulation (GDPR)

The European Union's General Data Protection Regulation (GDPR), enacted in 2018, is one of the most comprehensive and influential data privacy laws worldwide. The European Commission

stated that the GDPR is based on important principles like lawfulness, fairness, transparency, limited purpose, minimizing data collection, accuracy, restricted storage, integrity, and accountability. It also gives people essential rights, like accessing their personal information, correcting mistakes, asking for deletion (“the right to be forgotten”) and objecting to certain ways their data is used (*European Commission 2025*).

The GDPR applies to all organizations processing the personal data of EU residents, regardless of where the organization is based. Its enforcement mechanism includes substantial fines for violations, which encourage compliance and strengthen data protection culture. The GDPR demonstrates how privacy can be treated as a fundamental right and serves as a valuable model for jurisdictions, such as New Virginia, seeking to modernize their data protection frameworks.

IV. What Other States Are Doing

Several U.S. states have enacted privacy and data- protection laws to fill gaps in federal regulation. For instance, North Carolina’s Identity theft protection act mandates responsible data security measures, breach notifications, and restriction on the use of personal information (Ferguson III 191). Other states such as California, Colorado, and Virginia have established laws granting consumer rights to access, delete, and limit the sharing of personal data (NCSL 2022).

The California Consumer Privacy act (CCPA) allows residents to opt out of the sale of their data, while Colorado Privacy act requires companies to conduct data protection assessments for high-risk processing. These state laws also impose penalties for noncompliance, sealing a nationwide trend towards empowering consumers and holding business accountable for digital misconduct. These initiatives demonstrate growing recognition that privacy protections are essential to safeguard citizens in a data-driven economy.

V. Recommendation

New Virginia should enact a comprehensive personal-data protection law modeled after effective frameworks such as the GDPR and state level statutes. A state privacy law would ensure transparency in data practices, require informed consent, and hold organizations accountable for misuse or neglect. On the other hand, a state-by-state approach can create inconsistencies that complicate business operations and compliance. However, this decentralized approach also allows states to innovate and tailor protections to their citizens specific needs, potentially influencing future federal legislation.

Acting now would position New Virginia as a leader in privacy and cybersecurity policy, strengthen residents' trust in government, business, and offer immediate protection while federal legislation remains uncertain. Though compliance may impose short term costs on business, long term benefits are stronger consumer protection, legal clarity, and enhanced public confidence outweigh the challenges (Ogletree Deakins).

Works Cited

- European Commission. “GDPR – The Fabric of a Success Story.” *European Commission*, 2025, https://commission.europa.eu/law/law-topic/data-protection/gdpr-fabric-success-story_en.
- Ferguson III, James H. “Protecting Personal Data: A Survey of Consumer Protections Throughout North Carolina’s Identity Theft Protection Act.” *Campbell L. Rev.*, vol. 42, 2020, pp. 191–.
- Kesan, Jay P., and Carol M. Hayes. *Cybersecurity and Privacy Law in a Nutshell*. 2nd ed., West Academic Publishing, 2022.
- National Conference of State Legislatures (NCSL). “2022 Consumer Privacy Legislation.” *NCSL*, 2022, <https://www.ncsl.org/about-state-legislatures/2022-consumer-privacy-legislation>.
- Ogletree Deakins. “U.S. Continues Patchwork of Comprehensive Data Privacy Requirements: New Laws Set to Take Effect Over Next 2 Years.” *Ogletree Deakins Insights*, 2025, <https://ogletree.com/insights-resources/blog-posts/u-s-continues-patchwork-of-comprehensive-data-privacy-requirements-new-laws-set-to-take-effect-over-next-2-years>