

Virginia AI Bills Could Serve As Nationwide Model

By **Beth Waller and Patrick Austin** (February 14, 2025)

Virginia — a leader in privacy law — is again blazing a trail regarding artificial intelligence legislation.

Over 18 state privacy laws have been enacted in the last five years, with many other states adopting the Virginia privacy model. With more data centers than any other state in the nation, Virginia has long been a leader in technology law. Pragmatic and business-friendly, Virginia passed a balanced approach to privacy law that was mirrored across the country.

Now, Virginia takes that same pragmatic and tech-savvy approach to AI legislation with two bills introduced in January providing guidance to private and public sector organizations. While the bills are currently in committee, Virginia's General Assembly Joint Commission on Technology and Science, or JCOTS, is thoughtfully considering testimony about the pros and cons of AI legislation.

With Virginia's legislative session only 45 days this year, we will likely know soon whether this legislation will be making waves throughout the nation.

Embracing the Virginia Model

Virginia has taken a unique approach to AI legislation — departing from enacted legislation in Colorado,[1] Utah,[2] California[3] and the European Union.[4]

For example, the draft Virginia legislation bifurcates the requirements for public entities[5] and private sector entities.[6]

The two companion bills — one considering private entities, H.B. 2094; and the other public bodies, S.B. 1214 — are both draft pieces of legislation primarily focused on regulating the use of high-risk AI systems, which are defined under both bills as "any artificial intelligence system that is specifically intended to autonomously make, or be a substantial factor in making, a consequential decision." [7]

A "consequential decision" is defined under both draft bills as "any decision that has a material legal, or similarly significant, effect on the provision or denial to any consumer of, or the cost or terms of" the following:

- Education enrollment or an education opportunity;
- Employment or an employment opportunity;
- A financial or lending service;
- An essential government service;
- Healthcare services;
- Housing;
- Insurance; or
- A legal service.



Beth Waller



Patrick Austin

The regulatory requirements contained in Virginia's draft AI legislation would primarily affect developers, integrators and deployers of high-risk AI systems. Including integrators of high-risk AI systems in Virginia's draft legislation is another notable departure from the Colorado AI Act and the European Union's AI Act.[8]

For context, an integrator of a high-risk AI system is defined as a public body (in the public sector bill) or person (in the private sector bill) that "knowingly integrates an artificial intelligence system into a software application and places such software application" on the open market.

Another notable aspect of Virginia's draft AI legislation that could influence other states is the definition of a "consumer." Under the current iteration of both Virginia AI bills, a consumer is defined as "a natural person acting only in an individual or household context." The bills expressly state that a consumer "does not include a natural person acting in a commercial or employment context."

This language is the same language that Virginia adopted in its privacy legislation that swept the nation. It is significant because it narrows the scope of the AI legislation and removes employees from the mix, focusing instead on consumers. In contrast, the definition of a "consumer" under the Colorado AI Act is much broader, and it does not contain any express limitations on what consumer actions would trigger compliance with the law.[9]

The more targeted definitions of such key terms in Virginia's draft AI legislation could lead to other states viewing the commonwealth's proposed AI regulations as more pragmatic and business-friendly.

The focus on regulating the development, integration and deployment of high-risk AI systems is another element of Virginia's draft AI legislation that other states could mirror.

It's worth noting that Colorado's AI Act also focuses on high-risk AI systems, which is an indicator of where state-based AI regulation could be headed — not regulating the ever-expanding set of AI systems and applications, but instead regulating specific types of AI systems that could be used to adversely affect individuals in specific contexts or through algorithmic discrimination.

Effects to Corporate Compliance Strategies Across the Nation

If the current iteration of Virginia's draft AI bills are signed into law, it could influence the compliance strategies of companies operating in the commonwealth and across the U.S.

For example, companies could consider using Virginia's proposed AI regulatory framework as a guidepost for developing compliance programs, which could affect how both public and private sector entities develop and deploy certain AI systems.

Virginia's draft AI legislation, in addition to Colorado's AI Act, requires developers and deployers of high-risk AI systems to proactively disclose the rationale behind adverse consequential decisions rendered by high-risk AI systems. In addition, developers and deployers of high-risk AI systems would need to implement a robust risk management policy and program that specifies the principles, processes and personnel for managing and mitigating any risk of algorithmic discrimination that is "reasonably foreseeable."

A compliant risk management program must also align with existing regulatory standards.

Both Virginia's draft AI legislation and Colorado's AI Act specifically point to the National Institute of Standards and Technology's AI Risk Management Framework[10] and the International Organization for Standardization's standard for "establishing, implementing, maintaining, and continually improving an AI Management System (AIMS) within organizations." [11]

Virginia's proposed AI regulatory framework could also signal to companies that they will need to establish a viable infrastructure — i.e., principles, processes and personnel — for conducting high-risk AI system impact assessments, annual high-risk AI system reviews, public-facing consumer disclosures, and timely reporting of any indicators of algorithmic discrimination.

Looking Ahead

Whether the Virginia General Assembly ultimately decides to pass the JCOTS draft AI legislation remains an open question that could be answered quickly. Both bills are currently in committee.

The public sector AI bill is being reviewed by the Senate Committee on General Laws and Technology,[12] while the House Committee on Communications, Technology and Innovation is reviewing the private sector AI bill.[13]

And again, with a shorter 2025 legislative session scheduled to last only 45 days, we may very well know whether AI legislation is on a path toward passage within the next few weeks. Stay tuned.

Beth Burgin Waller is a principal and chair of the cybersecurity and data privacy practice at Woods Rogers Vandeventer Black PLC.

Patrick J. Austin is of counsel at the firm.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Colorado AI Act, https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf.

[2] Artificial Intelligence Policy Act, <https://le.utah.gov/~2024/bills/static/SB0149.html>.

[3] Assembly Bill 2013, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2013

.

[4] EU AI Act, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

[5] Draft AI legislation governing the use and deployment of high-risk AI systems by public bodies, <https://lis.blob.core.windows.net/files/1018278.PDF>.

[6] Draft AI legislation governing the use and deployment of high-risk AI systems by private sector entities, <https://lis.blob.core.windows.net/files/1015122.PDF>.

[7] See JCOTS legislative language, *supra*.

[8] Neither the Colorado AI law nor the EU AI Act reference an "integrator" of high-risk AI systems in their respective frameworks.

[9] Under the Colorado AI law, a consumer is simply defined as an "individual who is a Colorado resident," https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf.

[10] <https://www.nist.gov/itl/ai-risk-management-framework>.

[11] <https://www.iso.org/standard/81230.html>.

[12] <https://lis.virginia.gov/bill-details/20251/SB1214>.

[13] <https://lis.virginia.gov/bill-details/20251/HB2094>.