

## **Virginia Committee on General Laws and Technology**

**January 28th, 2026**

Dear Chairman Ebbin, Vice Chair Aird, and Members of the Committee,

On behalf of myself as a resident of the state of Virginia, and on behalf of consumers throughout the state, I write to express our concerns regarding SB 85, the Consumer Data Protection Act; social media platforms & model operators, interoperability interfaces.

The legislation is not a modest update to the Virginia Consumer Data Protection Act, but rather an intentional expansion of state power over data flows and product design, particularly targeting social media platforms and AI model providers. It would mandate interoperability and impose sweeping technical mandates of private firms.

They are not small changes; they're a fundamental shift towards government-directed platform design.

In § 59.1-577.2, a mandate is created to redesign private services, requiring that platforms use an open protocol, provide continuous real-time data sharing, avoid discrimination towards third parties, maintain documentation about the interface access, and enable automated notification whenever data updates occur. This effectively is the government engaging in an exercise of designing software systems.

Additionally, it grants consumers broad rights to demand that social media platforms and model operators delete user-generated content, metadata, relational data, and even inferred data. This seemingly mirrors a right to be forgotten that we have seen in European data privacy laws, which presents potential First Amendment issues. It is also worth noting that the European GDPR is being recognized as in need of an overhaul, and we believe that it would be wise to avoid replicating similar regulatory structures here in the States.

Furthermore, the proposal basically forces platforms to allow third parties to pull data in real time, creating serious privacy concerns that might run contrary to the overarching Virginia Consumer Data Protection Act. In mandating the real-time data, the legislation increases the attack vectors for hackers, allows for easier pathways to scrape massive amounts of data, and exposes the system to higher levels of vulnerability.

Interoperability mandates run the risk of locking in technologies of today, favoring incumbents who can afford the compliance regime, and creating legal risks for companies that experiment with how to offer better goods and services to consumers. These burdens will undoubtedly be felt by small businesses that are

trying to enter the marketplace and challenge incumbents, as the legislation will raise the cost to deploy AI platforms, build and launch new social media platforms. Unfortunately, it would serve as a red flag to entrepreneurs, who will feel discouraged from wanting to operate their business in the state.

And while this proposal allows firms to potentially charge “reasonable fees” under certain conditions, this will likely invite a legal challenge down the road. Such mandates attempt to convert social media platforms and AI model providers into utility companies.

This proposal isn’t a minor update to privacy rights. It serves as a major transformation in the design and deployment of products that consumers seek and enjoy. Mandating interoperability in the fashion this proposal seeks to do will not increase competition or improve consumer privacy. It advantages incumbents, and it makes the process of competing in the digital economy more expensive.

It’s for these reasons that I ask the committee to reject the bill.

Respectfully,

James Czerniawski

Head of Emerging Technology Policy

Consumer Choice Center