June 30, 2026

Pennsylvania State Senate
501 N. 3rd Street
Harrisburg, PA 17120

Re: HB 78- "An Act Providing for Consumer Data privacy, for Duties of Controllers and for Duties of Processors; and Imposing Penalties" (Oppose, Seeking Amendments)

Dear Members of the Pennsylvania State Senate,

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully request amendments to HB 78. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms. For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA supports comprehensive privacy legislation that ensures consumers' personal information is handled responsibly. However, the bill should be amended to avoid unconstitutionally compelling speech from online service providers, and to make certain requirements more administratively feasible.

The bill's required disclosures violate the First Amendment.

HB 78 requires covered businesses to compile and submit data protection assessments containing "a data protection assessment for each of the controller's processing activities that present a heightened risk of harm to a consumer". Multiple federal appellate court rulings have held that such mandatory disclosures constitute compelled speech in violation of the First Amendment.[1] In 2024, the Ninth Circuit held that "requir[ing] the forced creation and disclosure of highly subjective opinions about content-related harms" constitutes "State attempts to indirectly censor the material available… online[] by delegating the controversial question… to the companies themselves."[2] Such requirements therefore "fall[] well short of satisfying strict First Amendment scrutiny" and are unconstitutional.[3]

CCIA recommends that any assessment framework be limited to evaluating specific, objectively defined data practices — without requiring controllers to make open-ended editorial judgments about whether their content choices impose a "heightened risk of harm" to consumers. A targeted, practice-specific assessment requirement can achieve meaningful accountability without the constitutional deficiencies that attend content-focused mandates.

[1] *See, e.g.*, *NetChoice v. Bonta*, 113 F.4th 1101 (9th Cir. 2024); *X Corp. v. Bonta*, 116 F.4th 888 (9th Cir. 2024).
[2] *NetChoice*, 113 F.4th at 1122.
[3] *Id.*

The bill designates national origin as "sensitive data" even when unrelated to immigration.

Businesses routinely collect data regarding consumers' national origin in contexts unrelated to immigration enforcement. For example, companies may need customers' country of origin for tax compliance, shipping receipts, or compliance with foreign and domestic trade laws. HB 78 treats this routine commercial data the same as sensitive immigration enforcement information. Rather than designate all data concerning nationality and country of origin as sensitive data, the bill should designate such data as sensitive only when used in an immigration enforcement context.

The definition of "essential goods and services" requires clarification.

HB 78 defines "Decisions that produce legal or similarly significant effects concerning the consumer" to include the provision or denial of "essential goods or services." However, the bill does not define "essential goods or services", and it is difficult to objectively determine which products or services this category includes. The reference to "essential goods or services" should therefore be replaced with "access to food and water", as in other state laws.[4] This language is more concrete and provides greater certainty as to which decisions, products, and services are covered.

The bill's portability requirement should be removed.

The bill requires controllers to present requested copies of consumer data in portable format. This requirement should be removed, as it waters down online security. Forcing websites to build public-facing interfaces would require businesses to send data to less secure locations, risking increased data breaches and unauthorized access by foreign adversaries. Beyond these security gaps, such proposals often undermine users' privacy, potentially allowing personal data to be extracted without the consent of everyone involved in a social interaction.

* * * * *

We appreciate the legislature's attention to the important subject of consumer privacy and your consideration of these comments. CCIA stands ready to provide additional information and perspectives to ensure a balanced approach that protects consumers while fostering digital innovation.

Sincerely,

Kyle J. Sepe
State Policy Manager, Northeast Region
Computer & Communications Industry Association

[4] *See, e.g.*, Tex. Bus. & Com. Code § 541.001(11)(F); Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-575 (2025), https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/.