May 26, 2026

Delaware Senate Committee on Banking, Business, Insurance and Technology
Legislative Hall 411
Legislative Avenue
Dover, DE 19901

Re: HB 380- "An Act to Amend Title 6 of the Delaware Code Relating to Personal Data Privacy" (Oppose)

Dear Chair Mantzavinos, Vice Chair Paradee, and Members of the Senate Committee on Banking, Business, Insurance and Technology:

On behalf of the Computer & Communications Industry Association (CCIA), I write to provide input and respectfully raise concerns regarding HB 380. 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 proposed modifications to Delaware's privacy bill create additional hurdles for covered businesses to serve their consumers without meaningfully improving user privacy. The bill presents the following concerns:

The bill designates national origin as "sensitive data."

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. The bill 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 bill's required disclosures violate the First Amendment.

HB 380 requires covered businesses to compile and submit data protection assessments containing "An analysis of whether profiling poses any known or reasonably foreseeable heightened risk of harm to a consumer, and, if so, a description of... The nature of the heightened risk of harm" and "The steps that have been taken to mitigate the heightened risk of harm". The U.S. Court of Appeals for the Ninth Circuit has ruled multiple times that such mandatory disclosures constitute compelled speech in violation of the First Amendment.[1] In 2024, the court 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

[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).

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.

The bill creates unnecessary compliance burdens that do not improve transparency or privacy.

HB 380 would require controllers responding to consumer requests to list each individual third party with whom they share personal data, rather than categories of third parties. However, listing each individual third party will not necessarily be efficient for businesses or consumers. Businesses often have lengthy lists of such third parties that would need to be updated constantly, and consumers might struggle to discern the relevant information if flooded with a list of such third parties. A list of categories would most effectively convey the essential aspects of a controller's data practices.

Similarly, HB 380 would require controllers to "[n]ot disclose sensitive data in a sale of personal data unless… "strictly necessary to provide or maintain a product or service affirmatively requested by the consumer to whom the sensitive data pertains." This requirement applies even when the consumer has consented to the disclosure, and thus institutes an unnecessary compliance burden that does not improve consumer choice. Moreover, determining whether a product or service can be provided without processing a given piece of data will likely require significant technical expertise, even for businesses without technically complex operations. This regulation is likely to create barriers to entry in many industries, and deter out-of-state businesses from expanding into Delaware.

* * * * *

We appreciate the committee'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

[2] *NetChoice*, 113 F.4th at 1122.
[3] *Id.*