June 8, 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's definition of "sale of personal data" is overbroad.

All other comprehensive state privacy laws define "sale of personal data" to exclude personal data disclosed to third parties to provide products or services the consumer expressly requests.[1] HB 380, however, deviates from this standard in crucial respects, which make compliance far more difficult to objectively evaluate. Requiring that such transfers be "strictly necessary" to provide the products or services in question turns compliance evaluations into highly technical endeavors. Determining every potential means of providing a consumer with a product or service and then deciding which ones require processing a given piece of data requires much technical expertise and would be cost-prohibitive for both smaller businesses and regulators, with Delaware taxpayers ultimately bearing the costs of these expensive investigations.

Furthermore, this definition allows data transfers to be classified as sales retroactively, preventing covered businesses from knowing in advance if they must institute Subsection (12)'s extensive protocols. If a regulator decides that a prior data transfer was not "strictly necessary" to provide a given product or service, the covered business can be found liable for failing to institute these protocols, even if it had no way of anticipating that it would be obligated to do so. This constant legal jeopardy will likely reduce services that Delaware's most vulnerable residents regularly rely upon, such as telehealth providers and community lending

[1] *See, e.g.*, Connecticut Data Privacy Act, Conn. Gen. Stat. § 42-515(37)(B) (2023), https://www.cga.ct.gov/2024/sup/chap_743jj.htm; Texas Data Privacy and Security Act, Tex. Bus. & Com. Code § 541.001(28)(B) (West 2024), https://statutes.capitol.texas.gov/?tab=1&code=BC&chapter=BC.541&artSec=; Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-575 (2026), https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/.

organizations. Accordingly, CCIA recommends eliminating the exceptions to the rule that sensitive data transfers to third parties to fulfill consumer requests are not "sales of sensitive data," and removing the definition's "strictly necessary" requirement.

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.[2] 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 themselves."[3] Such requirements therefore "fall[] well short of satisfying strict First Amendment scrutiny" and are unconstitutional.[4]

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. It would also require controllers to make and share such lists before obtaining consent to transfer sensitive data. 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

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

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, as noted above, 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.

Furthermore, the bill's recent amendments require covered businesses to retain all consumer consent records for five years, a rule seen in no other state. Securely handling this volume of sensitive data is a technically complex and costly undertaking. While larger businesses may possess these capabilities, many smaller ones will not. This requirement will thus deter smaller businesses from scaling up their operations, undermining competition and reducing service quality for Delaware residents.

HB 380 puts Delaware at a competitive disadvantage.

When HB 380 was introduced, its synopsis listed "more closely align[ing] the DPDPA with similar consumer data protection laws enacted in other states" as a key aim. However, in its current form, the bill does the opposite. Many of the aforementioned provisions would be unique among states, discouraging out-of-state businesses from expanding into Delaware. Imposing substantial new compliance costs and sources of liability on businesses wishing to enter the state deters them from serving Delaware consumers. CCIA recommends aligning HB 380's requirements with the consensus standards among other states to better achieve the bill's objective.

* * * * *

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