May 22, 2026

401 S 2nd St
Springfield IL 62701

Re: SB 340 - Illinois Consumer Data Privacy Act (Oppose)

Dear Chairperson Williams and Members of the Illinois House Executive Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to express our continued concerns with Senate Bill 340, Senate Amendment 2. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] Proposed regulations on the interstate provision of digital services therefore can have a significant impact on CCIA members.

We appreciate the sponsor's continued engagement with stakeholders and acknowledge that the latest amendment contains several constructive changes, including the removal of the Private Right of Action provision. That modification represents meaningful progress and addresses one of the most significant concerns raised by industry and other stakeholders. However, despite these improvements, the bill continues to include numerous provisions that remain overly broad, operationally burdensome, and legally problematic. Specifically, the following concerns remain:

SB 340's data processing limitation puts Illinois businesses at a competitive disadvantage.

Absent a federal privacy framework, interoperability between state privacy laws is crucial to avoid placing a difficult, confusing, and costly compliance burden on businesses. Several aspects of SB 340 differ from other existing state privacy laws and therefore will cause difficulty for businesses of all sizes operating in Illinois. In particular, SB 340 disadvantages Illinois businesses by holding them to a stricter data minimization standard than their out-of-state counterparts. Most state privacy laws limit data processing to what is "reasonably necessary" for the disclosed purposes for which the personal data is processed.[2] However, SB 340 adds the requirement that controllers not process personal data unless "strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the sensitive data pertains."

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 Illinois. Furthermore, it would effectively

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

[2] *See, e.g.*, Texas Data Privacy and Security Act, Tex. Bus. & Com. Code § 541.101(a)(1) (West 2024), https://statutes.capitol.texas.gov/?tab=1&code=BC&chapter=BC.541&artSec=; Connecticut Data Privacy Act, Conn. Gen. Stat. § 42-520(a)(1) (2024), https://www.cga.ct.gov/2024/sup/chap_743jj.htm.

prohibit businesses from acquiring third-party data, which would greatly stifle innovation. CCIA therefore recommends using only the standard limitation, under which controllers may process data that is reasonably necessary for a disclosed purpose.

Besides introducing a novel data minimization standard, the bill subjects data processors to liability they would not face in other states. Typically, processors are not bound by the restrictions on selling personal data that controllers must follow.[3] However, SB 340 requires both controllers and processors to not sell personal data (unless one of the listed exclusions applies). Consequently, data processors will face new potential sources of liability by expanding into Illinois, undermining the state's ability to attract new businesses. CCIA therefore recommends limiting this requirement to only controllers.

Businesses operating online depend on clear regulatory certainty across jurisdictions nationwide.

Ambiguous and inconsistent regulation at the state level would undermine this business certainty and deter new entrants, harming competition and consumers. This particularly applies to new small businesses that tend to operate with more limited resources and could be constrained by costs associated with compliance. While larger companies may be able to more easily absorb such costs, it could disproportionately prevent new smaller start-ups from entering the market.

The bill's key definitions require clarification.

SB 340 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 definition of "Sensitive data" also requires clarification. Currently, it includes "the processing of biometric identifiers or information or genetic information for the purpose of uniquely identifying an individual." However, such information can be processed in a way that does not allow others to reconstruct the biometric identifier, and thus not pose a privacy risk to a consumer. Accordingly, subsection (2) of the definition of "Sensitive data" should be amended to clarify that "the purpose of uniquely identifying an individual" does not include processing mathematical representations from which biometric identifiers or information cannot be reconstructed.

[3] *See, e.g.*, Conn. Gen. Stat. § 42-520; Va. Code Ann. § 59.1-577.
[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/.

The bill creates potential conflicts with existing law.

If enacted, both SB 340 and the Biometric Information Privacy Act of 2008 (BIPA) would regulate Illinois residents' biometric information. The two laws assign covered entities' responsibilities differently: While SB 340 exempts data processing, transfers to fulfill requests, and transfers of publicly available information from the definition of "Sale", BIPA has no such exemptions.[5] Accordingly, the exemptions introduced in SB 340 will not be available to covered entities unless language is introduced to modify BIPA accordingly.

The bill should grant the State Attorney General exclusive enforcement authority.

Rather than allow "the Attorney General or the State's Attorney of any county" to bring an action against a noncompliant entity, the State Attorney General should have exclusive enforcement authority. This would eliminate the possibility of different law enforcement authorities making inconsistent demands of covered entities. It also allows administrative and judicial guidance to remain uniform throughout the state, an essential tool for businesses to ensure they are meeting the law's requirements. Precedents regarding what practices constitute compliance or noncompliance should remain uniform throughout the state.

* * * * *

CCIA appreciates the opportunity to engage on this legislation and remains committed to working collaboratively with lawmakers to develop balanced policy solutions that protect consumers while preserving innovation, competition, and free expression online.

Sincerely,

Megan Stokes
State Policy Director
Computer & Communications Industry Association

[5] *See* 740 Ill. Comp. Stat. 14/15(c) (2008), https://www.ilga.gov/Legislation/ILCS/Articles?ActID=3004&ChapterID=57&Print=True.