April 8, 2026

Senate AI and Social Media Subcommittee
Attn: Kelsey Wilson
State Capitol Building
309 State Capitol
Springfield, IL, 62706

Re: Senate Executive Subcommittee on AI and Social Media - Privacy Group 1

Dear Subcommittee Chair Cunningham and Members of the Senate Subcommittee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to offer the following recommendations regarding the proposed privacy laws currently being considered by the Committee. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] CCIA supports comprehensive privacy legislation that ensures that consumers' personal information is handled responsibly no matter where it is collected or who is processing it. This framework should set consistent transparency requirements, consumer controls, and accountability measures for data controllers. Such a framework should be risk-focused, technology-neutral, and provide safe harbors and flexibility for organizations to make adjustments according to individuals' needs and evolving technology.

Developing comprehensive and durable privacy legislation requires balance. Such legislation should encourage innovation and unlock the incredible social value of data without infringing on related rights such as freedom of speech. Overly prescriptive or onerous regulation risks creating high barriers to entry for new companies and may even prohibit the creation of beneficial new technologies and privacy protection techniques and services. To achieve these objectives, CCIA recommends the following:

Privacy laws should contain narrow and precise definitions.

Definitional clarity is not merely a technical preference — it is essential to allow businesses of all sizes to structure compliant operations, and to allow regulators and courts to apply the law predictably. CCIA recommends revising overbroad definitions to ensure that the laws do not unintentionally regulate broader swaths of the economy than necessary, and to tie obligations to specific contexts (such as the consent context for dark pattern prohibitions) rather than to open-ended assessments of a feature's impact on consumer behavior.

Several key terms in SB 1858 and SB 1995 are defined using vague or overbroad criteria that make it difficult for covered businesses to understand their obligations or assess their compliance posture. For instance, SB 1858 covers all contractors and businesses that store,

[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.

maintain, or purchase criminal justice data for Illinois government entities, but fails to differentiate those who control such data from those who only process data under client direction. Many technology companies process such data only in the latter capacity, and holding such companies liable for data sharing practices they did not choose to institute is neither far nor workable in practice. SB 1858 should therefore be amended to clarify that processors who solely serve government controllers are not liable for their government clients' data sharing decisions.

Similarly, SB 1995 covers much data that businesses routinely collect in contexts unrelated to immigration enforcement, including countries of origin, nationality, and citizenship 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. The bill's scope should therefore be limited to data used in an immigration enforcement context rather than all data concerning nationality and country-of-origin. State comprehensive bills routinely grant additional protections to sensitive data, and applying those protections to such information is the best way to safeguard it.

Privacy laws should align across states.

When laws regulating digital services differ substantially across states, consumer confusion and multiplied costs of compliance can result. Given the significant costs of developing privacy management systems, minor statutory divergences regarding definitions or compliance obligations create immense burdens for covered organizations. 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 compliance costs. While larger companies may be able to more easily absorb such costs, it could disproportionately prevent new smaller start-ups from entering the market.

Legislators should therefore harmonize key definitions and business obligations, such as the rights to access, correct, and delete data, with consensus consumer privacy standards already established in other states. A divergent approach leaves businesses uncertain of how to comply and leaves consumers confused about how to exercise their rights. SB 2875 in particular is well-suited to this objective, as many of its provisions mirror those in the 20 states with comprehensive privacy laws in place.

Comprehensive privacy laws should be enforced exclusively by state authorities.

Vesting authority solely in regulators with particular expertise in the data at issue gives the best chance of uniform interpretation, application, and enforcement of privacy statutes. Enforcement authorities should engage with organizations that create best practices and frameworks for their members and stakeholders to follow, such as DTSP and NIST. Enforcement authority should be vested with a single regulatory agency to avoid legal uncertainty and conflicting requirements for businesses.

Comprehensive privacy legislation should avoid broad private rights of action that contravene existing court precedents. Indeed, recent opinions express skepticism with congressional grants of broad statutory damages without clearly showing injury and actual damages.[2] Lawsuits prove extremely costly and time-intensive, with the costs often being passed on to individual consumers. Such a measure would disproportionately impact smaller businesses and startups. Furthermore, all 20 states that have established a comprehensive consumer data privacy law have enforced these laws through their state attorney general. This allows for the leveraging of technical expertise concerning enforcement authority and allows public interest to determine which enforcement actions are brought.

Privacy legislation should include safe harbor provisions, a right to cure, and sufficient lead time to ensure compliance.

Safe harbor provisions are important for fair and effective enforcement. Safe harbors (1) provide valuable predictability to both market actors and consumers, (2) enable speedier compliance, and (3) deter vexatious, meritless litigation if in fact parties other than the federal government are authorized to enforce the statute. When a federal agency alleges noncompliance with a privacy or security obligation, businesses should therefore be allowed to use compliance with an established privacy framework like NIST and ISO as an affirmative defense against such allegations. Businesses should also receive advance notice of complaints and have the opportunity to cure violations before enforcement actions are brought, both to minimize costly enforcement actions and focus agency resources on large-scale and repeat offenders.

Additionally, privacy legislation should include a mandatory opportunity-to-cure provision,. Providing advance notice of complaints and a cure period encourages organizations acting in good faith to rapidly resolve concerns and bring their data practices into compliance, thereby minimizing costly enforcement actions and allowing regulators to focus resources on large-scale and repeat offenders.

Implementing the requirements of a new privacy regime is a lengthy, complex process for businesses of all sizes. Covered organizations must thoroughly review their IT systems, reconfigure data management structures, and renegotiate contracts with vendors and service providers. To ensure businesses have adequate opportunity to meet their compliance obligations, the legislation should allow a minimum implementation period of 18 to 24 months following enactment.

* * * * *

We appreciate the Committee's consideration of these comments and stand ready to provide additional information as the legislature considers proposals related to technology policy.

Sincerely,

Megan Stokes

[2] *See, e.g.*, *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021) (holding that plaintiffs suing for damages for misuse of credit report data under FCRA did not meet constitutional standing requirements without showing injury in fact).

State Policy Director
Computer & Communications Industry Association