February 4, 2026

Senate Health and Public Affairs Committee
490 Old Santa Fe Trail
Santa Fe, NM 87501

RE: SB 53 – Community and Health Information Safety and Privacy Act (Oppose)

Dear Chair Lopez, Vice Chair Hickey, and Members of the Senate Committee on Health and Public Affairs:

On behalf of the Computer & Communications Industry Association (CCIA), I write to raise several concerns regarding SB 53. CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. CCIA strongly supports consumer data protection and understands that New Mexico residents are rightfully concerned about keeping their data safeguarded properly. CCIA also appreciates lawmakers' continued efforts to allow innovation to thrive while preserving meaningful consumer protection. However, several provisions of SB 53 would place New Mexico businesses at a competitive disadvantage and incentivize companies to collect more data from younger users than they would otherwise.

CCIA appreciates the chance to share the following concerns, as noted below:

SB 53's data processing limitation puts New Mexico 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 53 differ from other existing state privacy laws and therefore will cause difficulty for businesses of all sizes operating in New Mexico. In particular, SB 53 disadvantages New Mexico 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.[1] However, SB 53 adds the requirement that controllers not process personal data except "as necessary to provide the specific online feature, product or service with which the consumer is actively and knowingly engaged."

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

[1] *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.

Requiring opt-in consent for targeted advertising disadvantages New Mexico businesses without significantly improving privacy.

SB 53 requires covered entities to obtain consent via an opt-in mechanism for both contextual advertising and first-party advertising. This provision removes a critical tool for businesses without meaningfully improving privacy. Targeted advertising lowers consumer costs by allowing businesses to sell products more efficiently (particularly smaller businesses),[2] and allows services that connect billions of people to operate without charging users. Additionally, growing a business requires leveraging first-party data collected from consumers to better evaluate their needs and reach new customers. Such advertising also benefits consumers by allowing them to more easily find the products and services they need.[3]

While consumers should have the option not to share their data with third parties, an opt-out provision provides consumers with the same options without giving out-of-state companies an advantage over New Mexico businesses. Accordingly, CCIA recommends removing the opt-in requirement for first-party advertising entirely, and changing the opt-in requirement for contextual advertising to an opt-out requirement.

SB 53's contains requirements that are not well-defined.

SB 53 contains several provisions that are vague, subjective, or not well-defined. Most privacy laws that prohibit the use of "dark patterns" do so only in highly specific contexts, such as to obtain consent.[4] SB 53, however, prohibits the "use [of] dark patterns to cause a consumer to provide personal data, beyond what is reasonably expected to provide the online feature, product or service, to forego privacy protections." Deciding when design features cause a consumer to provide "personal data beyond what is reasonably expected" is far more subjective than determining when such features impair the choice to provide consent. This requirement should therefore be specific to the consent context.

SB 53's characterization of feeds is also vague and contradictory. The requirements for default settings mandate that consumers must be able to "choose between a privacy-protective feed and a profile-based feed," even though many covered entities' websites will not contain feeds at all. For such businesses, it is unclear what this provision requires. Moreover, these types of feeds are defined inconsistently: the bill defines "expressly provided data" as data provided "for the purpose of a profile-based feed," while defining a "privacy-protective feed" as being not based on any personal data *except* "expressly provided data." CCIA recommends clarifying and clearly differentiating these concepts.

---

[2] *See, e.g.*, Marimer Guevara et al., *Digital Tools Offering Channels for Success: Facilitating a Small- and Medium-Sized Business Renaissance*, CCIA Res. Ctr. (Nov. 28, 2023), https://ccianet.org/wp-content/uploads/2023/11/CCIA_SMB-Retail-Channels-to-Market.pdf

[3] *See also* Jesse Lieberfeld, *Lessons Learned from California's Privacy Rulemaking*, Disruptive Competition Project (Oct. 28, 2025), https://project-disco.org/privacy/lessons-learned-from-californias-privacy-rulemaking/.

[4] *See, e.g.*, Texas Data Privacy and Security Act § 541.001(6)(C); Connecticut Data Privacy Act § 42-515(7)(C).

SB 53 incentivizes overcollection of minors' data.

SB 53 also requires that covered entities disable notifications between the hours of 10:00 p.m. and 6:00 a.m. mountain standard time". Such requirements inevitably require that covered operators track when it is nighttime in a given device's location. This requirement therefore effectively mandates location-based tracking of minors' devices, thus undermining the privacy of the very population the bill is designed to protect. Requiring covered operators to track their users serves no benefit, particularly since covered operators regularly offer users the option to turn off notifications themselves.

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 private right of action would result in the proliferation of frivolous lawsuits and questionable claims.

SB 53 permits users to bring legal action against persons that have been accused of violating new regulations. The bill provides that "a consumer who claims to have suffered a deprivation of the rights secured under the Community and Health Information Safety and Privacy Act may maintain an action to establish liability and recover damages and equitable or injunctive relief" By creating a new private right of action, the measure would open the doors of New Mexico's courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. Such a danger is particularly acute given the numerous vague and subjective requirements noted above, which will limit courts' ability to resolve such claims quickly. As lawsuits prove extremely costly and time-intensive, it is foreseeable that these costs would be passed on to individuals in New Mexico, disproportionately impacting smaller businesses and startups across the state.

* * * * *

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,

Aodhan Downey
State Policy Manager, Western Region
Computer & Communications Industry Association