February 4, 2026

Senate President Mary Felzkowski
House Speaker Robin Vos
Wisconsin State Assembly
2 E Main St
Madison, WI 53702

Re: A.B 172/S.B. 166, Consumer Privacy Legislation

Dear President Felzkowski and Speaker Vos,

The undersigned organizations write to request amendments to A.B. 172/S.B. 166, consumer privacy legislation. The bill seeks to provide to Wisconsin consumers the right to know the information companies have collected about them, the right to access, correct, and delete that information, as well as the right to stop the disclosure of certain information to third parties. However, in its current form it would do little to protect Wisconsin consumers' personal information, or to rein in major tech companies like Google and Facebook. The bill needs to be substantially improved before it is enacted; otherwise, it would risk locking in industry-friendly provisions that avoid actual reform.

This legislation is almost identical to Connecticut's comprehensive privacy law that passed in 2022. But four years is a long time in technology regulation, and since then, we've learned much about what does and doesn't work in comprehensive privacy laws, while states have continued to iterate and improve on Connecticut's approach. States have made a variety of targeted improvements, such as creating heightened protections for kids data and location information (e.g. Oregon),[1] reining-in unnecessary data collection (e.g. Maryland),[2] and closing unduly broad exemptions (e.g. Montana).[3] Even Connecticut's own Attorney General has requested legislative improvements to its privacy law in

[1] Oregon recently amended their comprehensive privacy law to ban the sale of children's data and precise geolocation information outright. See here: https://olis.oregonlegislature.gov/liz/2025R1/Measures/Overview/HB2008
[2] Maryland's recent comprehensive privacy law includes the concept of data minimization, discussed in the first bullet below.
[3] Montana's SB 297 amended the Montana Consumer Data Privacy Act to significantly narrow the law's exemption for financial institutions. https://dojmt.gov/office-of-consumer-protection/montana-consumer-data-privacy/

a number of areas to close loopholes that are hindering their enforcement efforts.[4] As such, A.B. 172/S.B. 166 would require several strengthening amendments to match these recent improvements and provide the level of protection that Wisconsin consumers deserve, including:

- *Include meaningful data minimization provisions.* Privacy laws should set strong default limits on the data that companies can collect and use so that consumers can use online services or apps safely by default. For this reason, we recommend that privacy laws include a strong data minimization requirement that limits data collection and use to what is reasonably necessary to provide the service requested by the consumer, as outlined in Consumer Reports and EPIC's model bill.[5] A strong default prohibition on unwanted data sharing is preferable to an opt-out based regime which relies on users to hunt down and navigate divergent opt-out processes for potentially thousands of different companies.

  By contrast, the notice-and-choice framework adopted by A.B. 172/S.B. 166 offloads all of the burden of consumer protection onto consumers themselves, while absolving companies of the responsibility to engage in responsible data collection. This very dynamic was highlighted by the Connecticut Office of the Attorney General in its recent enforcement report, where it recommended legislative amendments to strengthen the CTDPA, stating that the: "notice-and-consent model sets an exploitable standard— businesses can seek to justify unnecessary data collection by deeming such collection 'adequate, relevant and reasonably necessary' to the purposes disclosed to consumers."[6]

  The weaknesses in the notice-and-choice framework present in most state privacy laws and A.B. 172/S.B. 166 became apparent to many consumers last week when TikTok's transfer to a U.S. entity prompted a new pop-up notice for TikTok users. Upon opening the app, users were presented with a notice that TikTok was updating its Terms of Service and Privacy Policy to reflect changes including "new types of location information (including device geolocation) we may collect from you, with your permission" as well as changes to advertising practices. There was no "disagree" button—instead users had to agree or simply delete the app.[7] That's not a real choice, particularly for other apps that may be required for work, school, or other life necessities.

---

[4] Connecticut Office of the Attorney General, Updated Enforcement Report Pursuant To Connecticut Data Privacy Act, Conn. Gen. Stat. § 42-515, Et Seq, (April 17, 2025), https://portal.ct.gov/-/media/ag/press_releases/2025/updated-enforcement-report-pursuant-to-connecticut-data-privacy-act-conn-gen-stat--42515-et-seq.pdf

[5] Consumer Reports and the Electronic Privacy Information Center unveil new model legislation to protect the privacy of American consumers, (September 24, 2024), https://advocacy.consumerreports.org/press_release/consumer-reports-and-the-electronic-privacy-information-center-unveil-new-model-legislation-to-protect-the-privacy-of-american-consumers/

[6] Connecticut Office of the Attorney General, Updated Enforcement Report Pursuant To Connecticut Data Privacy Act, Conn. Gen. Stat. § 42-515, Et Seq, (April 17, 2025), https://portal.ct.gov/-/media/ag/press_releases/2025/updated-enforcement-report-pursuant-to-connecticut-data-privacy-act-conn-gen-stat--42515-et-seq.pdf

[7] Aimee Picchi, *TikTok's new privacy policy is sparking a backlash. Here's what to know,* CBS News (Jan. 28, 2026), https://www.cbsnews.com/news/tiktok-new-terms-of-service-privacy-geolocation-personal-information/?intcid=CNM-00-10abd1h.

Though the current legislation is far too reliant on opt-outs, we do appreciate that it at least includes recognition of tools, like universal opt out mechanisms (UOOMs), to ensure that consumers can exercise their rights in a more tenable fashion. UOOMs allow consumers to broadcast to businesses they interact with online their preference to opt out from their personal information being sold or shared with third parties through a simple toggle. Covered businesses are then expected to comply with the signal as if the consumer individually contacted them. The majority of state comprehensive privacy laws now include such a provision, including recently passed laws in Montana, Nebraska, and Texas.[8]

- *Ensure targeted advertising is adequately covered.* We recommend refining the definition of "targeted advertising" to better match consumer expectations of the term. The drafted definition potentially opens a loophole for data collected on a single site; it only includes ads based on a "consumer's activities over time and across nonaffiliated **websites**" (plural, emphasis ours). This may exempt "retargeted" ads from the scope of the bill's protections — ads based on one particular product you may have considered purchasing on another site. Such advertising — such as a pair of shoes that follows you all over the internet after you had left a merchant's site — are the stereotypical example of targeted advertising; the law's opt-out provisions should certainly apply to it. We suggest a shift toward the following definition:

  > *"Targeted advertising" means displaying or presenting an online advertisement to a consumer or to a device identified by a unique persistent identifier (or to a group of consumers or devices identified by unique persistent identifiers), if the advertisement is selected based, in whole or in part, on known or predicted preferences, characteristics, behavior, or interests associated with the consumer or a device identified by a unique persistent identifier.*
  >
  > *"Targeted advertising" includes displaying or presenting an online advertisement for a product or service based on the previous interaction of a consumer or a device identified by a unique persistent identifier with such product or service on a website or online service that does not share common branding with the website or online service displaying or presenting the advertisement, and marketing measurement related to such advertisements.*
  >
  > *"Targeted advertising" does not include:*
  > *(A) first-party advertising; or*
  > *(B) contextual advertising.*

[8] Julie Rubash, SourcePoint, The Always-Up-To-Date US State Privacy Law Comparison Chart, (July 1, 2024), https://sourcepoint.com/blog/us-state-privacy-laws-comparison-chart/

- *Narrow the loyalty program exemption.* We are concerned that the exception to the anti-discrimination provision when a consumer voluntarily participates in a "bona fide loyalty, rewards, premium features, discounts, or club card program" (Section 3(a)(4)) is too vague and could offer companies wide loopholes to deny or discourage consumer rights by simply labeling any data sale or targeted advertising practice as part of the "bona fide loyalty program." We urge the sponsors to adopt a more precise definition and provide clearer examples of prohibited discrimination that does not fall under this exception. For example, it's reasonable that consumers may be denied participation in a loyalty program if they have chosen to delete information or deny consent for processing that is functionally necessary to operate that loyalty program. That is, if you erase a record of having purchased nine cups of coffee from a vendor, you cannot expect to get the tenth cup for free. However, generally controllers do not need to sell data to others or to engage in cross-context behavior advertising in order to operate a bona fide loyalty program – such behaviors have nothing to do with the tracking of purchases to offer discounts or first-party advertising.

  Loyalty programs take advantage of the exact type of informational asymmetry that privacy laws should strive to eliminate. While consumers typically view loyalty programs as a way to save money or get rewards based on their repeated patronage of a business, they rarely understand the amount of data tracking that can occur through such programs.[9] For example, many grocery store loyalty programs collect information that extends far beyond mere purchasing habits, sometimes going as far as tracking consumer's precise movements within a physical store.[10] This information is used to create detailed user profiles and is regularly sold to other retailers, social media companies, and data brokers, among others. Data sales are extremely profitable for such entities — Kroger estimates that its "alternative profit" business streams, including data sales, could earn it $1 billion annually.[11] At a minimum, businesses should be required to give consumers control over how their information is collected and processed pursuant to loyalty programs, including the ability to participate in the program without allowing the business to sell their personal information to third-parties.[12]

  We recommend the following language:

  Nothing in this subdivision shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain, or to prohibit a controller from offering a different price, rate, level, quality, or

---

[9] Joe Keegan, Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You, The Markup, (February 16, 2023), https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you.
[10] ibid.
[11] ibid.
[12] See Consumer Reports' model State Privacy Act, Section 125(a)(5) for an example of a concise, narrowly-scoped exemption for loyalty programs. https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/.

selection of goods or services to a consumer, including offering goods or services for no fee, if the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program, provided that the selling of personal information is not a condition of participation in the program.

- *Remove authentication requirements for opt-outs.* While authentication requirements may be appropriate when consumers are requesting to access, delete, or correct their information, controllers should not be allowed to authenticate requests to opt-out. Fraudulent access, deletion, or correction requests can pose real consumer harm, such as identity theft or stalking. However, opt-out rights do not carry similar risks to consumers and therefore should not be subjected to this heightened standard. In the past, businesses have used authentication clauses to stymie rights requests by insisting on receiving onerous documentation. For example, in Consumer Reports's investigation into the usability of then-new privacy rights in California, it found examples of companies requiring consumers to fax in copies of their drivers' license in order to verify residency and applicability of CCPA rights.[13] The bill should be amended to clarify that controllers may only authenticate requests to confirm, access, obtain, delete, or correct personal data.

- *Strengthen enforcement.* We recommend removing the "right to cure" provision to ensure that companies are incentivized to follow the law, particularly given that other states have already passed similar provisions, giving companies plenty of time to acclimate to compliance. Already, the AG has limited ability to enforce the law effectively against tech giants with billions of dollars a year in revenue. Forcing them to waste resources building cases that could go nowhere would further weaken their efficacy. In addition, consumers should be able to hold companies accountable in some way for violating their rights—there should be some form of a private right of action.

- *Remove entity level carveouts*. The bill currently exempts from coverage any financial institution or an affiliate of a financial institution, as defined in the Gramm-Leach-Bliley Act, as well as covered entities and business associates under the Health Insurance Portability and Accountability Act. These carveouts arguably make it so that large tech companies (Apple, Amazon, Google, Facebook, and Microsoft) would be exempted from the entire bill if one arm of their business receives enough financial information from banks or crosses the threshold into providing traditional healthcare services, a line many of them are already currently skirting.[14] At most, the bill should exempt *information* that is collected pursuant to those laws, applying its protections to all other personal data collected by such entities that is not currently protected.

---

[13] Maureen Mahoney, Many Companies Are Not Taking the California Consumer Privacy Act Seriously, Medium (January 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb.

[14] See e.g., The Economist, "Big Tech Pushes Further into Finance," (Dec. 15, 2022), https://www.economist.com/business/2022/12/15/big-tech-pushes-further-into-finance; Richard Waters, "Big Tech searches for a way back into healthcare," Financial Times, (May 17, 2020), https://www.ft.com/content/74be707e-6848-11ea-a6ac-9122541af204

Thank you again for your consideration, and for your work on this legislation. We look forward to working with you to ensure that Wisconsin residents have the strongest possible privacy protections.

Sincerely,

Matt Schwartz
Senior Policy Analyst
Consumer Reports

Caitriona Fitzgerald
Deputy Director
Electronic Privacy Information Center (EPIC)

Ben Winters
Director of AI and Privacy
Consumer Federation of America

Vinhcent Le
Director of AI Policy
Tech Equity

Ellen Hengesbach
Associate, Don’t Sell My Data Campaign
Public Interest Research Group (PIRG)

Julius Shieh
Associate
Wisconsin Public Interest Research Group (WISPIRG)

Irene Leech
President
Virginia Citizens Consumer Council