February 22, 2021

The Honorable Matt Williams
Chairperson, Banking, Commerce, and Insurance Committee
Nebraska Legislature
41050 Road 762
Gothenburg, NE 69138-4036

Re: LB 1188, Uniform Personal Data Protection Act — OPPOSE

Dear Senator Williams,

The undersigned consumer and privacy groups write in respectful opposition to LB 1188, which is based on the Uniform Law Commission's Uniform Personal Data Protection Act. We recognize the challenges in devising legislation that adequately protects consumers without creating unworkable requirements on industry. But enacting this would be worse than doing nothing at all. This bill would do little to reform companies' inappropriate data practices. It explicitly exempts behavioral advertising from the protections in the bill, does not provide data deletion rights, has significant loopholes for data brokers, and doesn't give actionable rights to consumers. It could also forestall future privacy legislation that is more beneficial to consumers and holds companies accountable.

American consumers are subject to constant and intrusive data collection practices and have few legal protections for their personal information online. There is no comprehensive federal privacy law providing baseline protections over data privacy and security. Consumers need a strong privacy law that limits the processing of their personal data to what is reasonably necessary to provide the services they request online. And the law needs strong enforcement to back it up.

This bill doesn't impose meaningful limits or create strong enforcement mechanisms. It vaguely exempts "compatible data practices" — practices that companies believe are consistent with consumers' "ordinary expectations" or from which they are likely to "benefit" — from a consent requirement. We agree that consent should not be required for strictly necessary data processing, so that consumers aren't pummeled with confusing consent pop-ups. But the definition of compatible is too loosely defined to rein in companies. Rather than punt a determination of what is "compatible" to self-interested companies, the law should specify what processing activities are allowable without consent, and what activities are extraneous and prohibited.

Further, the consent provisions in LB 1188 would not be effective because they could allow privacy rights to be waived by boilerplate Terms of Service. Under LB 1188, companies must obtain consumers' consent for "incompatible data practices" — but this process for consent is not specified. In most cases, companies must only offer some ability for consumers to opt out of the processing. For incompatible processing of sensitive data, companies are required to obtain "explicit consent" — but that process is undefined. Potentially, the law would allow for privacy rights to be waived away by boilerplate language in a Terms of Service or End User License Agreement.

Arguably the most striking element of LB 1188 is that it explicitly exempts behavioral advertising from any controls or protections — even though reining in these privacy-invasive practices is generally considered to be a key motivation to enact a new data privacy law. Companies routinely use and transfer consumers' most personal information for targeted advertising. Not only is this harmful to privacy, but ad targeting based on this data can perpetuate historic patterns of discrimination and unequal outcomes among protected classes.[1] For example, the Department of Housing and Urban Development has charged Facebook for targeting housing advertisements based on protected categories like race and religion.[2]

Other problems with this bill include:

- **No deletion rights.** The bill offers consumers no right to deletion for any data for any company. Deletion rights have been a core element of European privacy law dating back to the Data Protection Directive, and have been reinforced by the enactment of the Global Data Protection Regulation. The California Consumer Privacy Act, Virginia Consumer Data Protection Act, and the Colorado Privacy Act all include deletion provisions. Consumers are at risk to data exposure or misuse so long as it remains saved.

[1] *See Letter from Lawyers' Committee for Civil Rights Under the Law et al. to Chair Lina Khan and Commissioners Chopra, Slaughter, Phillips, and Wilson,* Fed. Trade Comm'n (Aug. 4, 2021), https://www.lawyerscommittee.org/wp-content/uploads/2021/08/FTC-civil-rights-and-privacy-letter-Final-1.pdf.
[2] *Sec'y of Hous. & Urban Dev. v. Facebook, Inc.*, No 01-18-0323-8, 1, Charge of Discrimination, FHEO No. 01- 18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.

- **Loopholes for third-party data brokers and facial recognition technologies.** In addition to the general exemption for targeted advertising, the bill also exempts data brokers from the law's access provisions, perversely limiting those rights to companies with which consumers have a direct relationship. The bill would also broadly exempt facial recognition through its expansive definition of publicly available information. In addition, the bill has a weak definition of "deidentified data" that could offer further loopholes to companies.

- **Consumers can be penalized for exercising their privacy rights.** Under this bill, companies are permitted to charge consumers for declining to consent to incompatible practices. Consumers should not be penalized for exercising their privacy rights — otherwise those rights would only apply to those who could afford them. While privacy rules should not inhibit true loyalty programs that keep track of consumer purchases in order to incentivize repeat business, companies should not be permitted to provide discounts in exchange for building a profile for targeting offers, or for selling information about customer habits to third-party data brokers. That behavior does nothing to reward consumer loyalty, and runs counter to what participating consumers would reasonably expect.

- **Unlimited safe harbor.** Under this bill, compliance with voluntary consensus standards or another federal or state privacy framework would satisfy the requirements of the law, if that approach is approved by the attorney general. This gives an attorney general overly broad authority to limit the scope of the bill's already weak protections by blessing a weaker industry self-regulatory program. A better approach would be to clearly outline the rules that companies must follow to respect consumers' privacy, and provide enforcement provisions that are strong enough to incentivize companies to comply.

LB 1188 reflects the concerns of businesses over the interests of consumers. Many privacy groups objected to the framework as it was being developed by the ULC, but those concerns were ignored.[3] We welcome continued discussions with state privacy stakeholders to hammer out a framework that protects consumers without creating unduly onerous compliance costs. We look forward to working with you to help ensure that consumers have the strongest possible legal protections to safeguard their personal data.

[3] See, e.g. Letter from Common Sense Media, Consumer Federation of America, Electronic Frontier Foundation, and Privacy Rights Clearinghouse to Harvey Perlman (Oct. 16, 2020); Letter from Consumer Reports to Harvey Perlman (Oct. 16, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2021/07/CR-Comments-on-ULC-CUPIDA-Oct.-12.pdf.

Sincerely,

Consumer Federation of America
Consumer Reports
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
U.S. PIRG

cc: Members, Banking, Commerce, and Insurance Committee
The Honorable Mike Flood