January 31, 2024

Chair Julie Slama
Nebraska Committee on Banking, Commerce and Insurance
Nebraska Legislature
Room 1507
1445 K Street
Lincoln, NE 68508

Re: Nebraska L.B. 1294, Nebraska Consumer Privacy Legislation — OPPOSE UNLESS AMENDED

Dear Chair Slama,

Consumer Reports[1] writes in respectful opposition to L.B. 1294. The bill seeks to provide to Nebraska 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 Nebraska 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.

Consumers currently possess very limited power to protect their personal information in the digital economy, while online businesses operate with virtually no limitations as to how they collect and process that information (so long as they note their behavior somewhere in their privacy policy). As a result, consumers' every move is constantly tracked and often combined with offline activities to provide detailed insights into their most personal characteristics, including health conditions, political affiliations, and sexual preferences. This information is sold as a matter of course, is used to deliver targeted advertising, facilitates differential pricing, and enables opaque algorithmic scoring—all of which can lead to disparate outcomes along racial and ethnic lines.

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

At the same time, spending time online has become integral to modern life, with many individuals required to sign-up for accounts with tech companies because of school, work, or simply out of a desire to connect with distant family and friends. Consumers are offered the illusory "choice" to consent to company data processing activities, but in reality this is an all or nothing decision; if you do not approve of any one of a company's practices, you can either forgo the service altogether or acquiesce completely.

As such, privacy laws should set strong limits on the data that companies can collect and share so that consumers can use online services or apps safely without having to take any action, such as opting in or opting out.[2] We recommend including a strong data minimization requirement that limits data collection and sharing to what is reasonably necessary to provide the service requested by the consumer, as outlined in our model bill.[3] A strong default prohibition on 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.

To that point, we do appreciate that this legislation includes a provision for universal opt-out, which empowers consumers by making it easier to manage the otherwise untenably complicated ecosystem of privacy notices, opt-out requests, and verification. Measures largely based on an opt-out model with no universal opt-out, like the Virginia Consumer Data Protection Act, require consumers to contact hundreds, if not thousands, of different companies in order to fully protect their privacy. Making matters worse, Consumer Reports has documented that some companies' opt-out processes are so onerous that they have the effect of preventing consumers from stopping the sale of their information.[4]

While we appreciate this bill's thoughtful approach to opt-outs, the legislation still contains significant loopholes that would hinder its overall effectiveness. We offer several suggestions to strengthen the bill to provide the level of protection that Nebraska consumers deserve:

- *Remove the small business carveout.* Section 3(1)(c) of the bill currently exempts from coverage entities defined as small businesses by the United States Small Business Administration. However, in the modern digital marketplace, size is a poor proxy for an entity's capacity to collect and process large amounts of consumer data, and, by extension, create significant privacy risks. Moreover, the Small Business Administration's definition is pegged to NAICS codes, meaning the threshold qualifying an entity for the exemption will

---

[2] Section 12(1)(a) of the bill ostensibly includes data minimization language; however, because data processing is limited to any purpose listed by a company in its privacy policy — instead of to what is reasonably necessary to fulfill a transaction — that language will in practice have little effect.

[3] *Model State Privacy Act*, Consumer Reports (Feb. 23, 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/.

[4] 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.

vary by industry. Businesses in some industries may qualify as "small" so long as they employ less than 1,500 employees or bring in under $36.5 million in annual revenue.[5] By contrast, Cambridge Analytica, which illegally harvested the personal information of 87 million people, only employed 107 people when their activities were made public in 2018 and made around $25 million in revenue the previous year.[6]

Nebraska would join Texas as the only states to completely carve-out small businesses from coverage in a comprehensive privacy law. Even the weak Virginia Consumer Data Protection Act applies to smaller entities who nonetheless process consumer data as a core business practice. We urge the drafters to remove this provision and instead include coverage thresholds pegged to the amount of personal data a company processes.

- *Strengthen non-discrimination provisions.* Consumers should not be retaliated against for exercising their privacy rights—otherwise, those rights are functionally meaningless. Unfortunately, Section 12(3) of this bill could allow companies to deny service or charge consumers a different price if they opt out of the sale of their information. We urge you to adopt consensus language from the Washington Privacy Act that clarifies that consumers cannot be discriminated against for declining to sell their information (subsequently replicated in the majority of state privacy laws), and limits the disclosure of information to third parties pursuant to loyalty programs:

> *A controller may not discriminate against a consumer for exercising any of the rights contained in this chapter, including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to the consumer. This bill shall not prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program. If a consumer exercises their rights pursuant under Section 7 this act, a controller may not sell personal data to a third-party controller as part of such a program unless: (a) The sale is reasonably necessary to enable the third party to provide a benefit to which the consumer is entitled; (b) the sale of personal data to third parties is clearly disclosed in the terms of the program; and (c) the third party uses the personal data only for purposes of facilitating such a benefit to which the consumer is entitled and does not retain or otherwise use or disclose the personal data for any other purpose.*

---

[5] U.S. Small Business Administration, Table of Small Business Size Standards Matched to North American Industry Classification System Codes, (February 2016), https://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf

[6] Peg Brickley, "Cambridge Analytica Revenue Fell as Questions About Data Tactics Surfaced," Wall Street Journal, (June 1, 2018) https://www.wsj.com/articles/cambridge-analytica-revenue-fell-as-questions-about-data-tactics-surfaced-1527883000; Pitch Book, Cambridge Analytica Overview, (May 2018), https://pitchbook.com/profiles/company/226886-68

- *Narrow the loyalty program exemption*. Relatedly, 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 12(3)) 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.[7] 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.[8] 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.[9] 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.[10]

- *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 opens a loophole for data collected on a single site; it only includes ads based on a

---

[7] 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

[8] ibid.

[9] ibid.

[10] 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/

"consumer's activities over time and across nonaffiliated **websites**" (plural, emphasis ours). This would 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 the targeting of advertisements to a consumer based on the consumer's activities with one or more businesses, distinctly-branded websites, applications or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts. It does not include advertising: (a) Based on activities within a controller's own commonly-branded websites or online applications; (b) based on the context of a consumer's current search query or visit to a website or online application; or (c) to a consumer in response to the consumer's request for information or feedback.*

- *Strengthen enforcement*. We recommend removing the "right to cure" provision to ensure that companies are incentivized to follow the law.[11] 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 the identity authentication requirement for opting out*. L.B. 1294 gives consumers the right to opt out of certain uses of the consumer's information. But it sets an unacceptably high bar for these requests by subjecting them to identity authentication by the company. Consumers shouldn't have to authenticate their identity, for example by providing a driver's license, in order to opt-out of targeted advertising. Further, much of that data collected online (including for targeted advertising) is tied to a device and not an individual identity; in such cases, authentication may be impossible, rendering opt-out rights illusory. In contrast, the CCPA pointedly does not tether opt out rights to identity verification.[12]

- *Remove entity level carveouts*. The draft 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

---

[11] At the very least, the right to cure should sunset like it does under the Connecticut Data Privacy Act. See Public Act No. 22-15, Section 11(b), https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF

[12] Cal. Civ. Code § 1798.130(a)(2).

or crosses the threshold into providing traditional healthcare services, a line many of them are already currently skirting.[13] 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.

- *Include strong civil rights protections.* A key harm observed in the digital marketplace today is the disparate impact that can occur through processing of personal data for the purpose of creating granularized profiles of individuals based off of data both collected and inferred about them. Therefore a crucial piece of strong privacy legislation is ensuring that a business' processing of personal data does not discriminate against or otherwise makes opportunity or public accommodation unavailable on the basis of protected classes. A number of privacy bills introduced federally in recent years have included such civil rights protections, including the American Data Privacy and Protection Act which overwhelmingly passed the House Energy and Commerce Committee on a 53-2 bipartisan vote. Consumer Reports' Model State Privacy Legislation also contains specific language prohibiting the use of personal information to discriminate against consumers.

- *Remove ambiguities around requirements that the universal opt out mechanism not "unfairly disadvantage" other controllers*. The bill requires controllers to allow consumers to opt out of sales and targeted advertising through an opt-out preference signal (OOPS). However, the bill would also confusingly prohibit OOPSs from "unfairly disadvantag[ing]" other controllers in exercising consumers' opt-out rights. It is unclear what "unfairly disadvantage" might mean in this context, as by their definition mechanisms that facilitate global opt-outs "disadvantage" some segment of controllers by limiting their ability to monetize data. Consumers should be free to utilize OOPSs to opt out from whatever controllers they want. For example, a consumer may want to use a certain OOPS that specifically opts them out from data brokers (or may configure a general purpose mechanism to only target data brokers); in that case, a consumer (and the OOPS) should be empowered to only send opt-out requests to data brokers. The term "unfairly" introduces unnecessary ambiguity and the subsection should be eliminated.

- *Amend prohibitions on default opt-outs*. Currently, the bill states that OOPSs cannot send opt-out requests or signals by default. The bill should be amended to clarify that the selection of a privacy-focused user agent or control should be sufficient to overcome the prohibition on defaults; an OOPS should not be required to specifically invoke Nebraska law when exercising opt-out rights. OOPSs are generally not jurisdiction-specific — they are designed to operate (and exercise relevant legal rights) in hundreds of different jurisdictions. If a consumer selects a privacy-focused browser such as Duck Duck Go or Brave — or a

[13] 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

tracker blocker such as Privacy Badger or Disconnect.me — it should be assumed that they do not want to be tracked across the web, and they should not have to take additional steps to enable the agent to send a Nebraska-specific opt-out signal. Such a clarification would make the Nebraska law consistent with other jurisdictions such as California and Colorado that allow privacy-focused agents to exercise opt-out rights without presenting to users a boilerplate list of all possible legal rights that could be implicated around the world.

- *Clarify that approximating geolocation by IP address is sufficient residency authentication*. The bill provides that an OOPS must "[e]nable the controller to accurately determine whether the consumer is a resident of this state" and has made a legitimate request. Today, companies generally comply with state and national privacy laws by approximating geolocation based on IP address. The drafters should revise the legislation to clearly state that estimating residency based on IP address is generally sufficient for determining residency and legitimacy, unless the company has a good faith basis to determine that a particular device is not associated with a Nebraska resident or is otherwise illegitimate.

We look forward to working with you to ensure that Nebraska consumers have the strongest possible privacy protections.

Sincerely,

Matt Schwartz
Policy Analyst

cc: Senator Eliot Bostar
Members, Banking, Commerce and Insurance Committee