March 7, 2023

Speaker Matt Regier
Speaker Pro Tem Rhoda Knudsen
Majority Leader Sue Vinton
Minority Leader Kim Abbott
Montana House of Representatives
State Capitol
Helena, MT 59620-0500

Re: S.B. 384, Montana Consumer Privacy Legislation - OPPOSE

Dear Speaker Regier, Speaker Pro Tem Knudsen, Majority Leader Vinton, Minority Leader Abbott and members of the Montana House of Representatives,

Consumer Reports[1] writes in respectful opposition to Montana S.B. 384. The bill seeks to extend to Montana consumers important new protections, including 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 opt out of data sales, targeted advertising, and profiling.

Though the bill largely tracks with the provisions of the Connecticut Data Privacy Act (CDPA), it strips out key protections contained in that law, including the ability for consumers to opt out using an opt-out preference signal, making it a substantially weaker effort. The bill in its current form would not do enough to protect Montana 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 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

[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.

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.

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. Privacy legislation should limit companies' collection, use, and disclosure of data to what is reasonably necessary to operate the service (i.e. data minimization)[2] or that at least restrict certain types of processing (sales, targeted advertising, and profiling). S.B. 384 does neither of these things.

While S.B. 384 does nod toward a framework for universal opt out via authorized agents (Section 6), it strips out language from the CDPA that permits a consumer to designate an authorized agent "by way of, among other things, a technology, including, but not limited to, an Internet link or a browser setting, browser extension or global device setting, indicating such consumer's intent to opt out of such processing."[3] As such, it's unclear how consumers can actually take advantage of their authorized agent rights under this act, including whether such agents can be designated through a technological mechanism. Given the current ambiguity, businesses are likely to construe such allowances as narrowly as possible in order to limit consumer opt outs. S.B. 384 should restore the provision as drafted in the CDPA.

S.B. 384 also differs from the CDPA in that it removes the ability of consumers to opt out of any processing for the purposes of targeted advertising or data sales through an opt-out preference signal. While strong data minimization provisions are the gold standard, privacy legislation with universal opt-outs also empowers consumers by making it easier to manage the otherwise untenably complicated ecosystem of privacy notices, opt-out requests, and verification.[4] The goal of universal opt-out is to create an environment where consumers can set their preference once and feel confident that businesses will honor their choices as if they contacted each business individually.

---

[2] Section 7(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] Public Act No, 22-15, Connecticut Data Privacy Act, Section 5, https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF

[4] Aleecia M. McDonanld and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," I/S: A Journal of Law and Policy for the Information Society, vol. 4, no. 3 (2008), 543-568. https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf?sequence=1&isAllowed=y

Measures largely based on an opt-out model with no universal opt-out, like this bill, would 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.[5] By eliminating the ability for consumers to use opt out preference signals, S.B. 384 would lock-in a status quo that heavily leans in the direction of data collectors.

The legislation also contains several other significant loopholes that would hinder its overall effectiveness. We offer several suggestions to strengthen the bill to provide the level of protection that Montanans deserve.

- *Broaden opt-out rights to include all data sharing and ensure targeted advertising is adequately covered.* S.B. 384's opt out should cover all data transfers to a third party for a commercial purpose (with narrowly tailored exceptions). In California, many companies have sought to avoid the CCPA's opt out requirements by claiming that much online data sharing is not technically a "sale" (appropriately, CPRA expands the scope of California's opt-out to include all data sharing and clarifies that targeted ads are clearly covered by this opt out).[6] We recommend the following definition:

  > *"Share" [or sell] means renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.*

  While we appreciate that this measure has an opt out for targeted advertising, the current definition of targeted advertising is ambiguous, and could allow internet giants like Google, Facebook, and Amazon to serve targeted ads based on their own vast data stores on other websites. This loophole would undermine privacy interests and further entrench dominant players in the online advertising ecosystem. We recommend using 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*

---

[5] Maureen Mahoney, California Consumer Privacy Act: Are Consumers' Rights Protected, CONSUMER REPORTS (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-ConsumersDigital-Rights-Protected_092020_vf.pdf.

[6] Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously, supra* note 3, Medium (January 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb.

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.

- *Tighten the definition and interpretation of bona fide loyalty programs to eliminate loopholes.* We are concerned that the legislation's exception to the anti-discrimination provision when a consumer voluntarily participates in a "bona fide loyalty, rewards, club card or loyalty program" is too vague and could offer companies wide loopholes to deny 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 to provide clearer examples of prohibited behavior 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 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-site targeted 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.

- *Limit authentication requirements to requests to access, correct, and delete*. Section 5(4)(d) allows (though does not require for requests to opt out) controllers to authenticate consumer requests to exercise any of their rights under the act. This may be appropriate when consumers are requesting to access, delete, or correct their information, since fraudulent requests for these rights can pose real consumer harm. 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.[7] For example, in Consumer Reports's investigation into the usability of new privacy rights in California, we found examples of companies requiring consumers to fax in copies of their drivers' license in order to verify residency and applicability of CCPA rights.

- *Apply authorized agent provisions to rights to access, correct, and delete.* S.B. 384 currently only allows authorized agents to send requests to opt out, meaning for all other rights requests consumers must go to each business they interact with one by one and navigate its bespoke system. This means requests to access, correct, and delete are impractical to use at scale, especially when the law allows businesses to ask for onerous documentation to complete the request. The purpose of authorized agents is to cut down on the amount of time that each consumer must spend haggling with individual

[7] Ibid.

businesses to accept their rights requests, ultimately making those rights much more usable for consumers. CPRA and Oregon's SB 619 currently include a similar provision.[8]

- *Remove the right to cure from the Attorney General enforcement section*. The "right to cure" provisions from the administrative enforcement sections of the bill should be removed — as Proposition 24 removed similar provisions from the CCPA.[9] In practice, the "right to cure" is little more than a "get-out-of-jail-free" card that makes it difficult for the AG to enforce the law by signaling that a company won't be punished the first time it's caught breaking the law.

- *Eliminate entity level carveouts*. The draft bill currently exempts from coverage any financial institution or an affiliate of a financial institution, as defined in theFinancial Service Modernization Act of 1999, 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.[10] The bill already carves out from coverage information that is collected pursuant to those laws, so the need to exempt entire entities is unnecessary.

- *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.[11] Consumer Reports' Model State Privacy Legislation also contains

---

[8] See California Civil Code 1798.130 A(3)(a), https://cpra.gtlaw.com/cpra-full-text/

[9] At the very least, the right to cure should be reduced to 30 days and 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

[10] 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

[11] See Section 2076, Amendment in the Nature of a Substitute to the American Data Privacy and Protection Act, https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf

specific language prohibiting the use of personal information to discriminate against consumers.[12]

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

Sincerely,
Matt Schwartz
Policy Analyst

[12] See Sections 125 and 126, Consumer Reports, Model State Privacy Act, (Feb. 2021) https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf