January 19, 2024

Representative Steve Elkins
Minnesota House of Representatives
100 Rev. Dr. Martin Luther King Jr. Blvd.
Saint Paul, MN 55155

Re: H.F. 2309, Minnesota Consumer Privacy Legislation - OPPOSE UNLESS AMENDED

Dear Representative Elkins,

Consumer Reports[1] sincerely thanks you for your work to advance consumer privacy in Minnesota. H.F. 2309 would extend to Minnesota 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 ability to require businesses to honor universal opt-out signals and authorized agent requests to opt out of sales, targeted advertising, and profiling.

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 are constantly tracked online and their behaviors are 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 erode individuals' basic expectation of privacy and can lead to disparate outcomes along racial and ethnic lines.

While we prefer privacy legislation that limits 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

[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.

[2] Section 8(2)(b) 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.

restricts certain types of unexpected secondary data processing (sales, targeted advertising, and profiling), we appreciate that H.F. 2309 creates a framework for universal opt-out through universal controls. Privacy legislation with universal opt-outs empowers consumers by making it easier to manage the otherwise untenably complicated ecosystem of privacy notices, opt-out requests, and verification.[3] 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.

Privacy legislation with universal opt-outs 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 Minnesota consumers deserve:

- *Remove the pseudonymous data exemption.* Section 7(b) of the bill currently provides that all consumer rights under the bill, including opt-outs, do not apply to so-called "pseudonymous" data. This represents a major loophole that would essentially exempt the majority of the online advertising ecosystem from the most substantive aspects of this bill's coverage. Online platforms and advertisers use pseudonymous identifiers (often mobile ad IDs or MAIDs) to track users across websites and apps, collecting extremely granular data about a user's search history, usage, personal characteristics, and interests in order to serve them targeted advertisements or to create a profile they can sell to other interested third-parties. Though this is precisely the type of online tracking this bill ostensibly seeks to grant consumers more control over, this exemption would allow vast swaths of it to continue unabated. We presume that the intention of this provision is to minimize unnecessary data linkage as a result of a rights request. However, given the inclusion of the provision that restricts businesses from attempting to re-identify pseudonymous data (Section 7(e)), we question why Section 7(b) is necessary at all.

- *Broaden opt-out rights to include all data sharing and ensure targeted advertising is adequately covered.* H.F. 2309's opt-out should cover all data transfers to a third party

[3] 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

[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.

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).[5] We recommend including "sharing" in H.F. 2309's opt-out right and using 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.*

We also 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 "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.

- *Eliminate entity level carveouts*. The bill currently exempts from coverage covered entities and business associates under the Health Insurance Portability and Accountability Act. This 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 crosses the threshold into providing traditional healthcare services, a line many of them are already currently skirting.[6] The bill already carves out from

[5] Id.
[6] 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

coverage *information* that is collected pursuant to that law, so the need to exempt entire entities is unnecessary.

- *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. 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. 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.

- *Allow authorized agents to send rights requests on behalf of consumers.* While we appreciate this bill's inclusion of universal opt-out controls, it currently does not allow authorized agents to effectuate rights requests on behalf of consumers. Authorized agent provisions are now baseline consumer provisions in state privacy laws,[7] allowing for a practical option for consumers to exercise their privacy rights in a consent-based framework. Consumer Reports has already begun to experiment with submitting opt-out requests on consumers' behalf, with their permission, through the authorized agent provisions.[8] Authorized agent services will be an important supplement to platform-level global opt outs. For example, an authorized agent could process offline opt-outs that are beyond the reach of a browser signal. An authorized agent could also perform access and deletion requests on behalf of consumers, for which there is not an analogous tool similar to the GPC.

- *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

---

[7] Authorized Agent provisions are included in the California, Connecticut, Colorado, Delaware, New Hampshire, New Jersey, Montana, Oregon and Texas laws.

[8] Ginny Fahs, Putting the CCPA into Practice: Piloting a CR Authorized Agent, Digital Lab at Consumer Reports (Oct. 19, 2020), https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8.

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 Minnesota 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 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 Minnesota-specific opt-out signal. Such a clarification would make the Minnesota 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 Minnesota resident or is otherwise illegitimate.

- *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.[9] Consumer Reports’ Model State Privacy Legislation also contains

[9] 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.[10]

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

Sincerely,
Matt Schwartz
Policy Analyst

[10] 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