CR Consumer Reports®

March 7, 2023

By email

Chairman Floyd Prozanski
Vice Chair Kim Thatcher
Committee on Judiciary
Oregon Senate
900 Court St. NE, S-413
Salem, OR 97440

Re: S.B. 619, Oregon consumer privacy legislation - SUPPORT IF AMENDED

Chair Prozanski, Vice Chair Thatcher, and Members of the Senate Judiciary Committee,

Consumer Reports[1] sincerely thanks you for your work to advance consumer privacy in Oregon. S.B. 619 would extend to Oregon 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 authorized agents' browser privacy signals as an opt out of sale, targeted advertising, and profiling.

While the aforementioned protections would provide real improvements for the personal privacy of Oregon citizens, we are concerned with the ambiguous authentication and other requirements tethered to the authorized agent and global opt-out signal provisions, potential loopholes created by the nondiscrimination exception related to undefined "bona fide loyalty programs", as well as with this bill's definition of sale. As such, the bill needs to be significantly strengthened before we can offer our full support.

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 or 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

[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.

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.

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.

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 restricts certain types of processing (sales, targeted advertising, and profiling), we appreciate that with this legislation, the drafters chose the next best option by creating a framework for universal opt-out through universal controls and authorized agents. Strong data minimization provisions are our first choice because they prevent consumers from constantly operating from a defensive position where they must determine whether each company that they interact with performs processing activities they consider acceptable or not. However, 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.[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.

Measures largely based on an opt-out model with no universal opt-out, like the original interpretation of the California Consumer Privacy Act (CCPA), 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 CCPA opt-out processes are so onerous that they have the effect of preventing consumers from stopping the sale of their information.[4]

Section 3(1)(d) of the act requires that covered businesses allow consumers or their authorized agents to opt-out from a controller's processing of personal data for the purpose of targeted advertising, sales, and profiling. Privacy researchers, advocates, and publishers have already

[2] Section 5(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.
[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, 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.

created multiple technologies that would fit the bill for an authorized agent under this bill, including the Global Privacy Control (GPC)[5] and Consumer Reports' own Permission Slip[6], both of which could help make the opt-out model more workable for consumers.

We also appreciate that the authorized agent provisions join the California Privacy Rights Act (CPRA) in going further than most existing state privacy proposals and laws, since they also apply to all the consumer rights created through the legislation, such as the right to access, correct, and delete, in addition to the right to opt out. While access, correction, and deletion rights are important on their own, it is important to supplement them with authorized agent provisions so that consumers can actually use them at scale, especially when the law otherwise allows businesses to ask for onerous documentation to complete a rights request.

We also applaud you for including a private right of action in the bill. Given the AG's limited resources, a private right of action is key to incentivizing companies to comply. Further, it's appropriate that consumers are able to hold companies accountable in some way for violating their rights. We would prefer a private right that would also afford consumers monetary relief, but empowering consumers to obtain injunctive relief and costs is a significant step forward.

Section 7 also provides key assurances that controllers truly deidentify data if they are to rely on the "deidentified data" exception to the definition of "personal data." The section requires that controllers commit to maintaining and using deidentified data without attempting to reidentify it later on and that the controller enter into and monitor contracts with any recipient of deidentified data so that the recipient is held to the controller's own obligations under the legislation. Privacy legislation too often allows controllers to shirk their responsibilities through weak definitions of deidentification that fail to truly protect consumer privacy by allowing the trivial reidentification of personal data.

However, 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 Oregonians deserve.

- *Expand opt-out protections to all commercial sharing*. Draft versions of the Oregon Comprehensive Privacy Law allowed consumers to opt out of sharing for any commercial purpose. The bill, as introduced, provides a more limited and vague right to opt out of a data "sale." The new guardrails on opt-out rights could significantly limit the reach of the bill. In response to the California Consumer Privacy Act, many companies have claimed that they do not "sell" data to third parties to avoid complying with the

[5] Global Privacy Control, https://globalprivacycontrol.org.

[6] Ginny Fahs, Introducing Permission Slip, the app to take back control of your data, Consumer Reports (Nov. 16, 2022), https://digital-lab-wp.consumerreports.org/2022/11/16/introducing-permission-slip/

opt-out.[7] While the California Attorney General has adopted a broad definition of sale,[8] the language in this bill is nebulous and invites abuse. In fact, companies' abuse of the term "sale" was a key reason the CCPA was amended by the CPRA — now California law allows consumers to opt out of data "sharing" more broadly. The bill should instead clarify that all data disclosed, made available to, or shared with a third party for a commercial purpose is in the scope of the bill's protections — either by expanding opt-out rights to "sharing" or by defining sale to include any sharing for a commercial purpose.

- *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 reward, 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 drafters 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.

  Relatedly, Section 5(6) of the bill implies that consumers share data with companies "in return" for loyalty rewards and instructs companies to notify consumers when exercising their opt-out rights may interfere with the operation of a loyalty program. In reality, opting out of targeted ads or data sales should *never* interfere with a company's ability to track transactions for loyalty rewards. This section reflects a misunderstanding of how *bona fide* loyalty programs operate and should be removed.

- *Clarify there are no authentication requirements for opt-outs.* Section 4(5)(e) provides that a business may not require authentication for the purpose of responding to an opt-out, however Section 5(5)(c) seemingly allows for authentication for any rights requests, including opt-outs.[9] In the past, businesses have used authentication clauses

[7] Wendy Davis, "Some Advertisers See Loopholes in California Privacy Law," MediaPost, (Oct. 22, 2019), https://www.mediapost.com/publications/article/342338/some-advertisers-see-loopholes-in-california-priva.html

[8] E.g., California Attorney General's Office, Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act, (Aug, 24 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement

[9] The language in Section 5(5)(c) is especially confusing since to find out what rights are being referenced, readers of the statute must cross-reference Section 5(4)(i), then Section 4(1), then Section 3.

to stymie rights requests by insisting on receiving onerous documentation.[10] We request that you clarify that the authentication in Section 5(5)(c) only applies to access, correction, and deletion requests.

- *Remove ambiguities around requirements that the authorized agent not "unfairly disadvantage" other controllers.* Section 5(5)(e)(A) confusingly prohibits agents 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 authorized agents that facilitate global opt-outs are "disadvantaging" some segment of controllers by limiting their processing of data. Consumers should be free to utilize agents to opt out from whatever controllers they want. For example, a consumer may want to use a certain authorized agent that specifically opt-outs them from data brokers (or may configure a general purpose authorized agent to only target data brokers); in that case, a consumer (and their agent) should be empowered to only send opt-out requests to data brokers. The term "unfairly" introduces unnecessary ambiguity and Section 5(5)(e)(A) should be eliminated.

- *Amend prohibitions on default opt-outs*. Currently, Section 5(5)(e)(B) states that agents cannot send opt-out requests or signals by default. However, 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 authorized agent should not be required to specifically invoke the Oregon Privacy Act when exercising opt-out rights. Agents 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 an Oregon-specific opt-out signal. Such a clarification would make the Oregon 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.* Section 5(5)(e)(E) provides that if a consumer or authorized agent sends an opt-out signal, the controller must be able to "accurately determine whether the consumer is a resident of this state and has made a legitimate request under section 4 of this 2023 Act." 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

[10] Maureen Mahoney, California Consumer Privacy Act: Are Consumers' Digital Rights Protected?, Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf2.pdf

rights.[11] If every website in Oregon responded to a universal opt-out signal with such a request, in practice global opt-outs would be practically unusable and ineffective. Today companies generally comply with state and national privacy laws by approximating geolocation based on IP address.[12] 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 an Oregon resident or is otherwise illegitimate.

- *Clarify that companies cannot hound consumers for consent to disregard a global opt-out or other opt-out request*. The bill is ambiguous as to whether companies can respond to opt-out requests by pestering users for consent to process data notwithstanding the request. If the functional result of using an agent to opt out is simply that every site or app will then harass you for permission to ignore, the controls will end up being ineffective failures for Oregon consumers. For this reason, there is a strong policy argument to prohibit "re-opt-in" to ignore opt-outs, since the costs of re-opt-in (hassle, user experience, inadvertently granting consent) will almost certainly outweigh the benefits to the narrow slice of consumers who want to make targeted exceptions to a universal opt-out choice though such a prohibition. We recommend inclusion of language similar to Section 1102(2)(d) in the New York Privacy Act clarifying that companies cannot pester users for consent for functionally non-necessary tracking after they have exercised their opt-out rights.[13] At the very least, the law should impose stringent requirements upon such requests for consent and limit the frequency with which they appear.

- *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.[14] 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.

- *Limit exceptions.* Section 2(3) provides that various processing behaviors, such as for fraud prevention or for identifying defects, fall outside the scope of certain obligations of the law. These exceptions should be constrained to processing that is necessary,

[11] Ibid.

[12] E.g., Press Release, OneTrust Cookie Consent Upgraded with Recent ICO, CNIL and Country- and State-Specific Guidance Built-in, (Aug. 15, 2019), OneTrust, https://www.onetrust.com/news/onetrust-updates-cookie-consent-ico-cnil/.

[13] See Section 1102(2)(d), New York Privacy Act, https://legiscan.com/NY/text/S00365/id/2622257/New_York-2023-S00365-Introduced.html

[14] 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

proportionate, and limited to those particular purposes to prevent these exceptions from swallowing the law's protections.

- *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.[15] Consumer Reports' Model State Privacy Legislation also contains specific language prohibiting the use of personal information to discriminate against consumers.[16]

- *Eliminate the entity-level financial institution carveout.* The bill currently exempts from coverage any financial institution or an affiliate of a financial institution, as defined in the Gramm-Leach-Bliley Act. This carveout makes it so that large tech companies (Apple, Amazon, Google, Facebook, and Microsoft) would be exempted from the entire bill if they receive enough financial information from banks or cross the threshold into providing traditional financial products, a line many of them are already currently skirting.[17] The bill already carves out from coverage *information* that is collected, processed, sold or disclosed under and in accordance with the Gramm-Leach Bliley Act, so the need to additionally carve out entire financial institutions is unnecessary.

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

Sincerely,
Matt Schwartz
Policy Analyst

[15] See Section 207, 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

[16] 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

[17] 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