January 5, 2024

The Honorable Whitney Westerfield
702 Capital Ave
Annex Room 228
Frankfort, KY 40601

Re: S.B. 15, An Act Relating to Consumer Data Privacy - *AMEND*

Dear Senator Westerfield,

Consumer Reports sincerely thanks you for your work to advance consumer privacy in Kentucky. S.B. 15 would extend to Kentucky 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 tracking.

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, however vaguely, 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 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) or that at least restricts certain types of unexpected secondary uses of consumers' data (sales, targeted advertising, and profiling), we appreciate that S.B. 15 creates a framework for universal opt-out through universal controls and authorized agents.

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.[1] Measures largely based on an opt-out model with no universal opt-out, like the

[1] 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

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.[2]

Aside from universal-opt outs, this bill also includes several other important protections that should be retained in any future version of this legislation:

- *Controls over targeted advertising*. We appreciate that S.B.15 has an opt out of sharing, of tracking, and a strong definition of targeted advertising—providing key consumer controls over ad tracking. In California, many companies have sought to avoid the CCPA's opt-out by claiming that much online data sharing is not technically a "sale"[3] (appropriately, the California Privacy Rights Act [CPRA] expanded the scope of California's opt-out to include all data sharing and clarifies that targeted ads are clearly covered by this opt out).[4] This bill closes such loopholes to better ensure that consumers have a choice over whether internet giants like Google, Facebook, and Amazon serve targeted ads based on their own vast data stores on other websites.

  We also appreciate that the definition of targeted advertising clearly covers retargeting (targeting ads based on a consumer's interaction with another, single site). Finally, the bill's flat prohibition against controllers "knowingly or intentionally" targeting advertising or tracking children under 13 is also a much needed protection to reign in excessive surveillance and monetization of a vulnerable population.

- *Authorized agent rights*. We also appreciate that S.B.15 allows consumers to delegate to third parties the ability to submit consumer rights requests on their behalf — allowing for a practical option for consumers to exercise their privacy rights in an opt-out framework. Consumer Reports's Permission Slip app is one such service that can submit opt-out requests on consumers' behalf, with their permission, through authorized agent provisions. We've found that consumers are enthusiastic about this option, submitting more than 1 million rights requests so far.[5]

---

[2] 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-Consumers-Digital-Rights-Protected_092020_vf.pdf .

[3] Maureen Mahoney, Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs To Act, Digital Lab at Consumer Reports (Jan. 9, 2020), https://medium.com/cr-digitallab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb; The State of Authorized Agent Opt Outs, supra note 7, at 16.

[4] Maureen Mahoney, Consumer Reports Urges Californians to Vote Yes on Proposition 24, Digital Lab at Consumer Reports (Oct. 23, 2020), https://medium.com/cr-digital-lab/consumer-reports-urges-californians-to-vote-yes-onproposition-24-693c26c8b4bd.

[5] Ginny Fahs, "Milestone: One Million Data Rights Requests Initiated in Permission Slip", Consumer Reports, (October 12, 2023), https://innovation.consumerreports.org/milestone-1m-data-rights-requests-initiated-in-permission-slip/#:~:text=Today%2C%20we're%20excited%20to,of%20their%20data%20from%20companies.

While we appreciate this bill's thoughtful approach to the above-mentioned issues, 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 Kentucky consumers deserve:

- *Definition of pseudonymous data.* The bill currently excludes from the definition of personal data so-called "pseudonymous data." Yet the definition of pseudonymous data is broad enough to cover common identifiers, such as mobile advertising identifiers, that advertisers use to track individuals' devices around the internet. This loophole renders the opt-out rights otherwise available through the bill largely meaningless in the mobile space, dramatically undercutting their overall utility for consumers.

- *Private right of action*. One major difference between last session's introduced version of S.B. 15 and the current one is the lack of a private right of action. 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. A private right of action should be restored in this legislation.

- *Right to cure*. 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.[6] 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.

- *Non-discrimination.* Consumers should not be charged or denied service for exercising their privacy rights—otherwise, those rights are only extended to those who can afford to pay for them. Unfortunately, the bill's current language seems to imply that consumers can be discriminated against if they use their opt-out rights under the bill. We urge you to adopt consensus language from the Washington Privacy Act that clarifies that consumers cannot be charged for declining to allow controllers to sell their information, 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 subsection does 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 to Chapter 3 of this act, a*

[6] At the very least, the provisions should sunset as they do under Connecticut's privacy law, see Public Act No. 22-15, Section 11(b), https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF

*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.*

Otherwise, the exception to the anti-discrimination provision when a consumer voluntarily participates in a "bona fide reward, club card or loyalty program" (Section 4(1)(b)) 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.

Loyalty programs take advantage of the exact type of informational asymmetry that privacy law 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 go 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 of loyalty program data 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.

---

[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.

- *Changes to processing purposes.* Previous versions of this legislation included a provision that forbade controllers from processing personal data in a manner incompatible with the purposes that were specified to the consumer when they originally consented without notification and additional consent for those new purposes. This provision should be restored to the legislation. Consumers should not be surprised to find out, for example, that a teleconferencing company has changed its processing purposes to allow itself to train artificial intelligence models using consumers' voice data, as was recently alleged of Zoom.[10]

- *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 or crosses the threshold into providing traditional healthcare services, a line many of them are already currently skirting.[11] The draft already carves out from coverage *information* that is collected pursuant to those laws, so the need to exempt entire entities is unnecessary.

- *Authentication.* Section 3(6) provides that a "controller shall not be required to comply with a request to exercise any of the rights under this section if the controller is unable to authenticate the request using commercially reasonable efforts." 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.[12] If every website in Kentucky responded to an opt-out signal or authorized agent with such a request, in practice these tools would be practically unusable and ineffective. Today, companies generally comply with state and national privacy laws by approximating geolocation based on IP address.[13] The legislation should be revised 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 Kentucky resident or is otherwise illegitimate.

---

[10] Jay Peters, Zoom says its new AI tools aren't stealing ownership of your content, The Verge, (August 7, 2023), https://www.theverge.com/2023/8/7/23822907/zoom-train-ai-models-user-data-customer-consent
[11] 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
[12] Ibid.
[13] 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/.

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

Thank you again for advancing this important legislation. We look forward to working with you to ensure that Kentucky consumers have the strongest possible privacy protections.

Sincerely,

Consumer Reports

[14] 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

[15] 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