February 23, 2024

Representative Josh Branscum
702 Capital Ave
Annex Room 357B
Frankfort, KY 40601

Re: H.B. 15, Consumer Privacy Legislation - *OPPOSE UNLESS AMENDED*

Dear Representative Branscum,

Consumer Reports writes in respectful opposition to H.B. 15. The bill seeks to provide to Kentucky 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 Kentucky 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.

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. 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. 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.

Measures largely based on an opt-out model with no universal opt-out, like this bill, require consumers to contact hundreds, if not thousands, of different companies in order to fully protect their privacy. Consumer Reports recently conducted a study that found that, on average, more than 2,000 companies shared participants' consumer data with Facebook.[1] 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]

However, even within the parameters of an opt-out based bill, we make the following recommendations to improve the privacy provisions of H.B. 15:

- *Require companies to honor browser privacy signals as opt outs*. In the absence of strong data minimization requirements, at the very least, consumers need tools to ensure that they can better exercise their rights, such as a global opt out. CCPA regulations require companies to honor browser privacy signals as a "Do Not Sell" signal; the California Privacy Rights Act (CPRA) added the global opt-out requirement to the statute. The majority of comprehensive state privacy laws, such as those recently passed in Texas and Montana require it as well.[3] Privacy researchers, advocates, and publishers have already created a "Do Not Sell" specification, the Global Privacy Control (GPC), designed to work with the CCPA/CPRA, CPA, and CTDPA.[4] This could help make the opt-out model more workable for consumers, but unless companies are required to comply, it is unlikely that consumers will benefit.[5] We recommend using the following language:

---

[1] Jon Keegan, Each Facebook User Is Monitored by Thousands of Companies, Consumer Reports, (January 17, 2024), https://www.consumerreports.org/electronics/privacy/each-facebook-user-is-monitored-by-thousands-of-companies-a5824207467/

[2] 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.

[3] HuschBlackwell, State Privacy Comparison Chart, (January 9, 2024); CA, CO, CT, DE, MT, NJ, OR, TX all require controllers to respect universal opt-out requests. https://www.bytebacklaw.com/wp-content/uploads/sites/631/2024/01/New-Jersey-Chart.pdf

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

[5] Press release, Announcing Global Privacy Control: Making it Easy for Consumers to Exercise Their Privacy Rights, Global Privacy Control (Oct. 7, 2020), https://globalprivacycontrol.org/press-release/20201007.html.

> *Consumers or a consumer's authorized agent may exercise the rights set forth in Section 3 of this act by submitting a request, at any time, to a business specifying which rights the individual wishes to exercise. Consumers may exercise their rights under Section 3 via user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt out.*

Notably, the "authorized agent" provision mentioned above would allow a consumer to designate a third party to perform requests on their behalf — allowing for a practical option for consumers to exercise their privacy rights in an opt-out framework. Consumer Reports has already successfully implemented such a service that works to submit opt-out requests on consumers' behalf, with their permission, through the authorized agent provisions under state laws.[6] Authorized agent services are 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.

- *Broaden opt-out rights to include all data sharing and ensure targeted advertising is adequately covered.* H.B. 15'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).[7] 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.*

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

---

[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/

[7] 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.

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.*

- *Strengthen non-discrimination provisions*. Consumers should not be charged for exercising their privacy rights—otherwise, those rights are only extended to those who can afford to pay for them. Unfortunately, language in this bill could allow companies to 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 charged for declining 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 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.*

- *Clarify the authentication requirements*. 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.[8] If every website in Kentucky responded to an opt-out request in this way, in practice these rights (limited as they already are) would be practically unusable and ineffective. Today companies generally comply with state and national privacy laws by approximating geolocation based on IP address.[9] 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.

- *Strengthen enforcement.* We recommend removing the "right to cure" provision to ensure that companies are incentivized to follow the law. 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 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.[10] 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.

---

[8] Ibid.
[9] 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/.
[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

- *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.

- *Narrow the loyalty program exemption*. 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 4(1)(d)) 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.[11] 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.[12] This information is used to

[11] 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
[12] ibid.

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.[13] 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.[14]

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

Sincerely,

Matt Schwartz
Policy Analyst
Consumer Reports

cc: Members, Kentucky Senate Judiciary Committee

[13] ibid.
[14] 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/