January 25, 2023

Sen. Clyde Perfect, Chairman
Commerce & Technology Committee
Indiana State Senate
200 West Washington Street
Indianapolis, IN 46204-2785

Re: SB 5, Personal information and social media policies – OPPOSITION

Dear Chair Perfect,

The undersigned consumer and privacy groups write in respectful opposition to SB 5. The bill seeks to provide to Indiana consumers the right to know the information companies have collected about them, the right to delete that information, correction rights, and the right to stop the disclosure of certain information to third parties. However, in its current form it would do little to protect Indiana 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.[1] 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.

Opt-out bills, like SB 5, simply shift far too much of the burden onto individual consumers to protect their privacy. Consumer Reports has found that consumers experienced significant difficulty exercising their rights under the California Consumer Privacy Act (CCPA) opt-out provision. In our study, hundreds of volunteers tested the opt-out provision of the CCPA, by submitting "Do Not Sell" requests to companies listed on the data broker registry. About 14% of the time, burdensome or broken "Do Not Sell" processes prevented consumers from exercising their rights under the CCPA.[2] Unfortunately, SB 5 lacks provisions, like a global opt-out and authorized agent rights, that will make it more workable for consumers.

However, within the parameters of an opt-out based bill, we make the following recommendations to improve the privacy provisions of SB 5:

- *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 Colorado Privacy Act (CPA) and Connecticut Data Privacy Act (CTDPA) require it as well.[3] Privacy researchers, advocates, and publishers have already created a "Do Not

[1] Chapter 4, Section 1(1) of the draft bill ostensibly includes data minimization language; however, because data processing is limited to any purpose disclosed 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.
[2] *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?*, Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-significant-obstacles-to-exercising-california-privacy-rights/.
[3] Cal. Code Regs tit. 11 § 999.315(c); CPRA adds this existing regulatory requirement to the statute, going into effect on January 1, 2023, at Cal. Civ. Code § 1798.135(e) https://thecpra.org/#1798.135. For the Connecticut Law,

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:

> *Consumers or a consumer's authorized agent may exercise the rights set forth in Chapter 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 Chapter 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 begun to experiment with submitting opt-out requests on consumers' behalf, with their permission, through the authorized agent provisions of CCPA/CPRA.[6] 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.

- *Broaden opt-out rights to include all data sharing and ensure targeted advertising is adequately covered.* SB 5'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:

---

see Public Act No. 22-15, § 5, https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF. For the Colorado law, see SB 21-190, 6-1-1306(1)(a)(IV)(B), https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.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.

[6] 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.

[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.

"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 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.

- *Non-discrimination*. 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 Indiana 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 Indiana 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.

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

Sincerely,

Consumer Reports

---

[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/.

Electronic Frontier Foundation
Electronic Information Privacy Center (EPIC)

cc: Members, Indiana Senate Committee on Commerce & Technology
The Honorable Liz Brown