Ohio House Government Oversight Committee
February 8, 2021
Maureen Mahoney, Senior Policy Analyst, Consumer Reports
Opponent Testimony for HB 376

Chair Wilkin and members of the Government Oversight Committee, my name is Maureen Mahoney, Senior Policy Analyst at Consumer Reports.[1] Thank you for the opportunity to submit written testimony. The Ohio Personal Privacy Act (OPPA) seeks to provide to Ohio consumers the right to know the information companies have collected about them, the right to delete that information, and the right to stop the disclosure of certain information to third parties. However, in its current form it would do little to protect Ohio 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.

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.[2] 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. Consumer Reports has documented that some California Consumer Privacy Act (CCPA) opt-out processes are so onerous that they have the effect of preventing consumers from stopping the sale of their information.[3]

[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] *Model State Privacy Act*, Consumer Reports (Feb. 23, 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/.
[3] *Consumer Reports Study Finds Significant Obstacles to Exercising California Privacy Right*s, Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-significant-obstacles-to-exercising-california-privacy-rights/.

However, within the parameters of an opt-out based bill, we make the following recommendations to improve the Ohio Personal Privacy Act:

- *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; Proposition 24 added the global opt-out requirement to the statute. The new Colorado law requires it as well.[4] Privacy researchers, advocates, and publishers have already created a "Do Not Sell" specification designed to work with the CCPA, the Global Privacy Control (GPC).[5] This could help make the opt-out model more workable for consumers,[6] but unless companies are required to comply, it is unlikely that consumers will benefit. We recommend using the following language:

  > Consumers or a consumer's authorized agent may exercise the rights set forth in Sec. 1355.05-.08 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 Sec. 1355.08 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.

- *Broaden opt-out rights to include all data sharing and ensure targeted advertising is adequately covered.* OPPA'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 by claiming that much online data sharing is not technically a "sale"[7] (appropriately, Prop. 24 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). 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

[4] 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 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.
[5] Global Privacy Control, https://globalprivacycontrol.org.
[6] 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.
[7] 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-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb.

> third party for monetary or other valuable consideration, or otherwise for a commercial purpose.[8]

While we appreciate that this draft 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.

- *Limit exemptions for pseudonymous data.* There are other loopholes in the bill for cross-context targeted advertising that should be addressed. For example, pseudonymous data is fully exempted from the bill. Much of the data involved in ad tracking is associated with a particular device — not an individual name. Consumers should be able to opt out of the sale of this data to ensure that they have control over the disclosure of their data for targeted advertising. Pseudonymous data should be exempted from access and deletion requests, since this information could be associated with more than one person, but not from the opt out.

  Relatedly, the narrow definition of personal data — limited to information attributable to an identifiable consumer, processed for consideration, would have the effect of exempting most online data transfers. We instead recommend the following definition of personal data: "data that identifies or could reasonably be linked, directly or indirectly, with a particular consumer, household, or consumer device."

[8] Further, the definition of "commercial purpose" should be adjusted to reflect the CCPA: "to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. 'Commercial purposes' do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism." (Cal. Civ. Code 1798.140(f).

- *Strengthen definition of deidentified.* Deidentified data is exempted from the protections in this bill, even though research shows that it in many cases it is quite easy to reidentify allegedly "deidentified" or "anonymous" data.[9] We urge you to adopt a strong definition to help ensure that the company cannot reidentify the data, even if they wanted to do so.

  > "Deidentified" means information that cannot reasonably identify, relate to, describe, reasonably be associated with, or reasonably be linked, directly or indirectly, to a particular consumer or device, provided that the business: (1) Takes reasonable measures to ensure that the data could not be re-identified; (2) Publicly commits to maintain and use the data in a de-identified fashion and not to attempt to reidentify the data; and (3) Contractually prohibits downstream recipients from attempting to re-identify the data.[10]

- *Remove the verification requirement for opting out*. OPPA gives consumers the right to opt out of certain uses of the consumer's information. But it sets an unacceptably high bar for these requests by subjecting them to verification by the company. Thus, companies could require that consumers set up accounts in order to exercise their rights under the law — and hand over even more personal information. Consumers shouldn't have to verify their identity, for example by providing a driver's license, in order to opt-out of targeted advertising. Further, much of that data collected online (including for targeted advertising) is tied to a device and not an individual identity; in such cases, verification may be impossible, rendering opt-out rights illusory. In contrast, the CCPA pointedly does not tether opt out rights to identity verification.[11]

- *Remove the safe harbor for reasonable compliance with the NIST privacy framework.* The safe harbor in enforcement for companies that reasonably comply with the NIST privacy framework should be removed. The NIST framework was designed as a voluntary risk-management tool; it was not designed as an alternative to privacy rules. While potentially useful as an internal protocol for assessing privacy issues within a company, the framework does not provide clear guidance as to what companies can or cannot do with personal data, and as such is inappropriate as a safe harbor from legislative protections. Companies instead should be required to adhere to specific, enforceable requirements.

---

[9] Natasha Lomas, *Researchers Spotlight the Lie of 'Anonymous' Data*, TechCrunch (July 24, 2019), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/.

[10] This definition is similar to that in CPRA and tracks the Federal Trade Commission's definition of deidentified: that a company cannot reidentify the information, even if they wanted to. See, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Fed. Trade Comm'n at 21 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[11] Cal. Civ. Code § 1798.130(a)(2).

- *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 declining to sell their information, and limits the disclosure of information to third parties pursuant to loyalty programs:

  > A [business] 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 [business] 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 Sec. 1355.08 of this act, a [business] may not sell personal data to a third-party [business] 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.

- *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.

We ask that you pause to consider these improvements before advancing the bill. Thank you again for your consideration, and for your work on this legislation. We look forward to working with you to ensure that Ohioans have the strongest possible privacy protections.