February 6, 2023

The Honorable Nicholas P. Scutari
President
New Jersey State Senate
67 Walnut Ave.
Clark, NJ 07066

Re: New Jersey S. 332, Data Privacy - Consumer Reports OPPOSITION

Dear President Scutari,

Consumer Reports[1] writes in respectful opposition to S. 332. The bill seeks to provide to New Jersey consumers the right to know the information companies have collected about them, the right to "change" 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 New Jersey 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 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.

[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.

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.[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.

Opt-out bills, like S. 332, 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 CCPA's opt-out provision. In our study, hundreds of volunteers tested the opt-out provision of the CCPA, by submitting DNS requests to companies listed on the data broker registry. About 14% of the time, burdensome or broken DNS processes prevented consumers from exercising their rights under the CCPA.[3] Unfortunately, S. 332 lacks provisions, like a global opt-out and authorized agent rights, that helps make the California Privacy Rights Act (CPRA), which builds upon the CCPA, more workable for consumers.

However, within the parameters of an opt-out based bill, we make the following recommendations to improve S. 332:

- *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.[4] Privacy researchers, advocates, and publishers have already created a "Do Not

---

[2] *Model State Privacy Act*, Consumer Reports (Feb. 23, 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/.

[3] *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/.

[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 Connecticut Law, see Public Act No. 22-15, § 5, https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF. For

Sell" specification, the Global Privacy Control (GPC), designed to work with the CCPA/CPRA, CPA, and CTDPA.[5] 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.[6] We recommend using the following language::

> Consumers or a consumer's authorized agent may exercise the rights set forth in Section 4 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 4 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.[7] 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.

- *Include a right to delete.* Every comprehensive privacy law in effect today requires that covered entities delete the personal information they maintain regarding a consumer upon request. Businesses should not be able to retain personal information of consumers indefinitely just because the consumer interacted with them in the past. For example, a woman who previously interacted with a reproductive health application who no longer wishes for that application to maintain her sensitive information should be able to simply request that the application delete it. Including a right to delete also helps reduce the risk of unwanted disclosure, including through a data breach. To make this right more practicable, authorized agents should be permitted to send requests to delete on behalf of consumers, upon request.

---

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] 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.

- *Broaden the applicability.* S. 332 currently only applies to "operators", which are defined as any "person or entity that operates a commercial Internet website or an online service and includes any third party that tracks or collects any information concerning a customer's usage of a commercial Internet website, regardless of whether the third party owns or operates the website." This is much narrower than existing comprehensive privacy laws, which typically apply to *any* business in the state that determines the purposes for which and the means by which personal data are processed and meets the thresholds for applicability, regardless of whether the data collection occurs online or not. The reality of our increasingly connected world is that data collection happens throughout our daily lives, not just when we log-on to the internet or use our smartphones. For instance, retail stores collect all sorts of personal information about our buying habits that can reveal sensitive information about us and that can be sold or shared later on with data brokers, online platforms, and advertisers. S. 332 should be amended to apply to any business that collects personally identifiable information and otherwise meets the requirements set by the bill.

- *Broaden opt-out rights to include all data sharing and targeted advertising.* S. 332's opt out should cover all data transfers to a third party for a commercial purpose (with narrowly tailored exceptions), and include a right to opt out of targeted advertising. Currently, S. 332's opt-out language seemingly only contemplates the scenario when operators sell information to data brokers, since the definition of sale is limited to "the exchange of personally identifiable information for monetary consideration by the operator to a third party *for purposes of licensing or selling personally identifiable information at the third party's discretion to additional third parties*" [emphasis added]. This completely ignores the massive industry of controller-to-controller data sales that endanger individual privacy, leaving consumers' every last byte of personal information, from browsing habits, sensitive health information, and even precise geolocation, vulnerable to sale on the open market.

  Opt-out rights under this bill should be expanded beyond the data broker context and include the concept of sharing. 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"[8] (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). 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

[8] Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously, supra* note 3.

third party for monetary or other valuable consideration, or otherwise for a commercial purpose.

Consumers should also be allowed to specifically opt out of targeted advertising. We recommend including a right to opt out of targeted advertising in Section 4(a) and 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.

- *Include stronger non-discrimination language.* 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 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 Section 4 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.

- *Remove the verification requirement for opting out*. 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. If every website in New Jersey responded to an opt-out request in that way, in practice 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. 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 New Jersey resident or is otherwise illegitimate.

- *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 make 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.[9] Consumer Reports' Model State Privacy Legislation also contains specific language prohibiting the use of personal information to discriminate against consumers.[10]

- *Eliminate the entity-level financial institution carveout.* 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. 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.[11] 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.

---

[9] 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
[10] 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
[11] 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

- *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 look forward to working with you to ensure that New Jersey consumers have the strongest possible privacy protections.

Sincerely,

Matt Schwartz
Policy Analyst

cc: Majority Leader Ruiz
Chair Nellie Pou
Senator Troy Singleton
Senator Richard Codey