July 17, 2022

By email

The Honorable Frank Pallone, Chair
The Honorable Cathy McMorris Rodgers, Ranking Member
House Committee on Energy & Commerce
Washington, DC 20515

Re: American Data Privacy and Protection Act ("ADPPA")

Dear Chairman Pallone and Ranking Member McMorris Rodgers,

Consumer Reports[1] writes to commend the work of this committee in trying to enact federal privacy legislation and to recommend improvements to the text to make sure the bill works as intended. We appreciate the constructive dialogue we have had with the Committee both about the initial draft bill released on June 3rd as well as about the Amendment in the Nature of a Substitute ("AINS") passed by the Subcommittee on Consumer Protection and Commerce on June 23rd. Consumer Reports has long argued that federal privacy protections are long overdue, and we support the bipartisan negotiations to develop a consensus solution to these pressing issues. The bill includes important protections for consumers — including new civil rights protections to safeguard consumers from discrimination — that are desperately needed in a society where every click and footstep can be recorded, analyzed, and sold without any consumer awareness or control.

We also want to express our appreciation for the fact that this bill is fundamentally based upon the principle of data minimization — data processing should be limited to what is functionally necessary to deliver the products or services requested by an individual, with specific and limited exceptions for certain processes such as first-party analytics and product

[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.

improvement. This is the approach recommended by the Consumer Reports model privacy bill,[2] and is reflected in § 101(a) (restricting data processing to fulfill consumer requests) and § 101(b) (articulating the exclusive list of exceptions to §101(a)). This approach protects consumers' privacy by default instead of forcing consumers to constantly micromanage their privacy, either by shunting consumers through constant opt-in choices or by forcing consumers to find and navigate hundreds of heterogenous privacy opt-out controls and settings.

However, the structure of the bill raises questions about how effective the data minimization standard will be in practice. While Section 101(b) purports to limit secondary sharing by default, Section 206 provides for a data broker registry which consumers can visit to delete unnecessary data stores and to stop brokers from collecting their information going forward. If Section 101 truly limited data processing to what is functionally necessary, a data broker registry and opt-out list would not be necessary.

Moreover, the text of the AINS specifically calls out targeted advertising as an exempted purpose under the bill, relying instead on opt-outs — including global opt-outs — to empower consumers to advertising and sharing for advertising-related purposes (which is the considerable majority of online data sharing). We have supported the use of global opt-outs as a fall back option both in a recent white paper we co-authored with the Electronic Privacy Information Center on FTC rulemaking and in our advocacy on state legislation;[3] Consumer Reports is also a founding member of the Global Privacy Control project, an open-source effort to create a standardized browser-based signal to let consumers exercise opt-out rights at scale when online.[4] However, we would prefer a more straightforward prohibition — as has been proposed for example in the Ban Surveillance Advertising legislation introduced by Representatives Eshoo and Schakowsky — and it is worth noting that relying upon global opt-opts to address advertising-related sharing has not to date been effective in California in comprehensively reining in advertising-related data sharing, as the largest platforms have yet to roll the tools out to their user base.

However, taking for granted the negotiators' decision to address targeted advertising and related data sharing through opt-out mechanisms instead of a prohibition, we urge the negotiators to address the following issues to strengthen the bill to provide the comprehensive privacy protections that American consumers have lacked for far too long:

---

[2] Model State Privacy Act, Consumer Reports, (February 2021) https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.

[3] Consumer Reports and the Electronic Privacy Information Center, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, (Jan. 26, 2022), https://advocacy.consumerreports.org/press_release/consumer-reports-and-epic-release-paper-calling-on-the-federal-trade-commission-to-pursue-a-privacy-rulemaking/; *e.g.*, Letter from Consumer Reports to The Honorable Reuven Carlyle re S. 5062, The Washington Privacy Act (2021), (Jan. 24, 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/01/CR-Letter-S.-5062-WPA-1.14.21-FINAL.pdf.

[4] Global Privacy Control — Take Control of Your Privacy, https://globalprivacycontrol.org/.

- *Advertising loopholes.* The original draft bill was extremely confusing on the issue of targeted advertising — targeted ads were simultaneously banned (§ 101(a)), subject to an opt-in (§ 204(a))), and subject to an opt-out (§ 204(c)-(d)). The AINS is at least clearer and now specifically identifies as permissible purposes both targeting advertising (subject to an opt-out) and first-party advertising (not subject to an opt-out).

  However, the exception for first-party advertising is overbroad and would encompass some of the most common forms of targeted advertising in practice today. Section 101(b)(11) exempts:

  > With respect to covered data previously collected in accordance with this Act, notwithstanding this exception, to process such data as necessary to provide first party marketing or advertising of products or services provided by the covered entity.

  The term "first-party marketing or advertising" is undefined. However, in response to increasing privacy scrutiny and regulation around the world, many companies are adopting very expansive claims about what can be done with "first-party data," including using first-party data on other services' sites.[5] Notably, § 204(b)(2) of the AINS presupposes that data can be shared with third parties for "first-party marketing or advertising" and specifically *exempts* from consumer opt-out rights data shared for these purposes.

  The prototypical example of targeted advertising is "retargeting," where a product that a user has viewed on the web or in an app then proceeds to follow that user around in display advertisements on other websites or apps, and potentially even on other devices. A user considers buying a pair of Nikes and decides not to — later they see an ad for the same shoes on ESPN. From Nike's perspective, this might be "first-party advertising" — it's advertising based on data it previously collected to market products that it provides. If they use an ad tech provider as a "service provider" to show ads on their behalf around the web, that behavior could fall within the scope of first-party advertising.

  Similarly, many businesses upload customer lists to services such as Google and Facebook with an instruction to those businesses to target visitors based on prior purchasing behavior. Under the language in the AINS, this use of "custom audiences" too could potentially fall outside consumers' opt-out rights under the bill. As a result,

[5] *E.g.*, Raja Rajan, *How e-commerce stores can use first-party data for Facebook retargeting*, Customer Labs, (Jan. 19, 2022), https://www.customerlabs.com/blog/how-ecommerce-stores-can-use-first-party-data-for-facebook-retargeting/.

consumers could continue to receive online ads based on what they (or potentially family members) purchased in online physical stores, even if they had specifically tried to opt out.

In designing this bill's protections, it is useful to keep in mind how many companies have adopted tendentious interpretations of the GDPR and CCPA to make only performative behavioral changes while failing to reform the fundamental business that those laws were designed to rein in. For example, in response to CCPA, many companies and trade associations adopted a narrow interpretation of the term "sale" and an expansive interpretation of the term "service provider" in order to categorize their data sharing practices as falling outside the statute's opt-out rights.[6]

Of course, even with true first-party advertising of first-party services on a first-party site, consumers should still have the ability to turn off personalized recommendations if they so desire. While it may be appropriate to exempt such advertising from the global opt-out controls defined in § 210, a consumer should always have the right to opt out of first-party targeting, even if only on a service-by-service basis.

- *Non-retaliation.* One bedrock principle of privacy law is that companies shouldn't punish consumers for making privacy choices. Privacy should be recognized as an inalienable and fundamental right, not merely an asset to be bartered away. Charging consumers for privacy would also have a disparate impact on the economically disadvantaged and members of protected classes who may not be able to afford the luxury of paying for fundamental privacy rights.

  The original draft bill prohibited differential pricing — but not differential treatment — of consumers who opted out (or did not agree to opt into) secondary uses of their data. Section 104(a) of the AINS weakened that language to only prohibit companies from denying service entirely to consumers who exercise privacy rights. This provision should be revised to clearly prohibit denial of service, differential pricing, and differential treatment for persons exercising privacy rights or withholding consent for secondary use.[7]

- *Deidentification.* The definition of "de-identified data" in § 2(10) appears to be based on the three-part test articulated in the FTC in its seminal 2012 Privacy Report: (1) the company must take reasonable measures to ensure that the data is de-identified, (2) the

[6] Wendy Davis, "Some Advertisers See Loopholes In California Privacy Law," MediaPost, (October 29, 2019), https://www.mediapost.com/publications/article/342338/some-advertisers-see-loopholes-in-california-priva.html?edition=115828.

[7] However, Consumer Reports has no objection to data processing necessary to maintain loyalty programs, so long as the data is simply used to track engagement for loyalty rewards, and the data is not shared or sold to third parties for unrelated purposes.

company must publicly commit to not try to reidentify the data, and (3) the company must contractually mandate any recipient of the data to not attempt reidentification.[8]

This definition was weakened in the AINS to include "administrative" and "physical" measures as possible ways to fulfill the first prong of the test. This is contrary to the purpose of the first prong of the test — the goal is for the company to believe that the data *could not be identified* even if the company was motivated to try. Administrative and physical measures are reversible. If a company simply encrypts data and keeps the decryption key next door with a policy against opening the door, that data should not be considered de-identified. Administrative measures to limit de-identification are provided for in the second and third prongs of the test.

- *Enforcement.* The FTC is already woefully underfunded.[9] ADPPA gives the FTC considerable new enforcement responsibilities, as well as new rulemaking powers, an obligation to assess and approve safe harbor requests, and a mandate to set up an "Office of Business Mentorship" to provide informal guidance and education. While § 407 of the bill authorizes new monies to the FTC to fulfill its new mission, we are unaware of any specific commitment of resources or proposed funding amounts to empower the FTC to enforce ADPPA. In Europe, the GDPR has been hampered by insufficient enforcement.[10] Given that private enforcement of the law is delayed several years and even then is subject to numerous constraints that will limit its use, we are concerned that insufficient enforcement could also blunt the effectiveness of ADPPA.

- *Preemption.* Finally, we have serious concerns about the scope of preemption in the current version of ADPPA. Over the past twenty years, the states have been the leaders in the United States on privacy protection, starting with data breach notification laws in 2002 and continuing with the passage of comprehensive privacy and security laws in states like California, Colorado, and Connecticut.

  The California Privacy Rights Act contains a provision that prohibits the legislature from ever weakening it in the future; as such, the law today provides a solid floor below which

[8] Federal Trade Commission Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[9] Letter from Consumer Reports and 26 other civil rights, civil liberties, and consumer protection organizations to The Honorable Chuck Schumer, Majority Leader *et al.*, (Sep. 23, 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/09/Group-letter-in-support-of-FTC-privacy-funding.pdf.

[10] Access Now, *Access Now raises the alarm over weak enforcement of the EU GDPR on the two-year anniversary*, (May 25, 2020), https://www.accessnow.org/alarm-over-weak-enforcement-of-gdpr-on-two-year-anniversary/.

privacy protections cannot sink.[11] Obviously, ADPPA does not and cannot provide a similar guarantee, but if it preempts the CPRA, it would also eliminate the CPRA's guaranteed baseline of protections.

The text of ADPPA has only been public for only a few weeks, and has evolved significantly even during that short time — there are dramatic differences between the initial draft and the AINS released on June 22nd. Especially given the fast timeline upon which this bill is being developed, it is inevitable that there will be inadvertent loopholes and gaps in the bill's protection. As discussed above, the California Consumer Privacy Act — which was also drafted and enacted in a very short legislative window — contained a number of loopholes that companies were able to exploit to largely evade the bill's protections. The California Privacy Rights Act was enacted just two years after the passage of CCPA to address some of the problems that became evident as the law became applied in practice.

Moreover, technology continues to evolve, and legislators, no matter how prescient, will not be able to account for every privacy threat that will develop in the coming years. Despite several efforts, Congress has failed to enact privacy legislation in response to concerns about online tracking for the past twenty-two years.[12] If ADPPA passes, consumers cannot wait for twenty-two years for those protections to be updated. The states must have the flexibility to iterate on ADPPA's protections in order to plug unintended holes and to respond to new threats.

Thank you again for your diligent efforts to bring new privacy and civil rights protections to American consumers. Despite our concerns and the narrow legislative window, we remain supportive of this process and hopeful that the issues we identify can be resolved.

Sincerely,

Justin Brookman
Director, Technology Policy
Consumer Reports

[11] CPRA § 25. *See also* Letter from Maureen Mahoney, Deputy Director of Policy and Legislation, California Privacy Protection Agency to Speaker Nancy Pelosi, (Jul. 1, 2022), https://aboutbgov.com/3XA.
[12] "Senate Eyes Net Privacy," CNN Money, (May 23, 2000), https://money.cnn.com/2000/05/23/technology/ftc_privacy/.