September 22, 2020

The Honorable Roger Wicker, Chair
The Honorable Maria Cantwell, Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate
Washington, D.C. 20510

Dear Chairman Wicker and Ranking Member Cantwell,

Consumer Reports[1] appreciates your leadership in exploring the need for regulations on the collection, use, and disclosure of consumer's personal information through the upcoming Commerce Committee hearing, "Revisiting the Need for Federal Data Privacy Legislation."[2] Now more than ever, consumers need effective protections over the unauthorized use of their data. Consumers are constantly tracked: online, through apps, and in the physical world. Without protections over the sharing of data, our personal information can be sold without our permission or awareness, or otherwise disseminated in ways that could mean getting charged more for insurance, or even facing job discrimination.[3] This information is often widely traded as a matter of course. As just one example, a recent study found that 10 apps, including dating and period-tracking apps, together sent sensitive personal information on consumers (such as location data) to at least 135 companies involved in advertising and behavioral profiling.[4]

---

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to helping expand online privacy protections, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

[2] *Revisiting the Need for Federal Privacy Legislation*, U.S. Senate Committee on Commerce, Science, & Transportation, (Sept. 23, 2020), https://www.commerce.senate.gov/2020/9/revisiting-the-need-for-federal-data-privacy-legislation.

[3] Donna Rosato, *What Your Period Tracker App Knows About You*, CONSUMER REPORTS (Jan. 28, 2020), https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you/.

[4] *Out of Control: How Consumers are Exploited by the Online Advertising Industry*, NORWEGIAN CONSUMERS COUNCIL at 5-6 (Jan. 14, 2020), https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf.

Additionally, in light of the COVID-19 crisis, consumers working from home are increasingly relying on their internet service providers, Google platforms, and teleconferencing services to work and attend school. Recently, Consumer Reports found that Zoom allowed itself to share details including instant messages and the names of call participants with third parties, even for advertising.[5] In response to this and further investigations from press outlets like *Motherboard*, Zoom quickly changed its policies to curtail these uses, and removed Facebook tracking software from its mobile app.[6] But this highlights that it's largely up to the company to decide whether to provide privacy protections to their customers. Clearly, consumers need effective, mandatory privacy protections.

We appreciate Chairman Wicker's work to help establish privacy protections by introducing new privacy legislation, Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA Act).[7] The bill would advance key baseline privacy protections: the right to access, delete, correct, and opt out of the sale of personal information, and additional protections for sensitive data. We particularly appreciate that the bill includes a data security requirement and that the definition of covered data applies to individuals as well as devices. We also approve of new efforts in this version of the bill to improve transparency into algorithmic data processing and to combat the use of dark patterns to coerce consumer consent. However, we cannot support the bill as written. We urge the Chairman to consider a number of adjustments to ensure that the bill is workable for consumers and to eliminate inadvertent loopholes that companies could exploit to avoid reforming their data practices. This is particularly important in light of early bad faith responses to similar legislation, the California Consumer Privacy Act (CCPA).

And bad faith CCPA compliance is a serious problem. Many tech companies are adopting disingenuous legal interpretations to avoid complying with their responsibilities under the CCPA to honor consumers' explicit requests to opt out of the sale of their information. For example, the Interactive Advertising Bureau (IAB), a trade group that represents the ad tech industry, developed a framework for companies to evade the opt-out by abusing the "service provider"

---

[5] Allen St. John, *Zoom Calls Aren't as Private as You May Think. Here's What You Should Know*, CONSUMER REPORTS (Mar. 24, 2020), https://www.consumerreports.org/telecommunications/zoom-teleconferencing-privacy-concerns/.

[6] Allen St. John, *At Zoom, New Privacy and Security Problems Keep Emerging*, CONSUMER REPORTS (Apr. 2, 2020), https://www.consumerreports.org/privacy/at-zoom-new-privacy-and-security-problems-keep-emerging/.

[7] SAFE DATA Act (2020), https://www.commerce.senate.gov/services/files/BD190421-F67C-4E37-A25E-5D522B1053C7.

provision in the CCPA.[8] Google announced that it will follow IAB's lead,[9] and Facebook has announced that its "like" buttons, which allow the company to track users' behavior across the web — even if they are not logged in — is outside of the consumer opt-out clause.[10] Grindr has sought to ignore "do not sell" instructions by claiming that consumers have assented to sale in long-form contracts they almost certainly have never read.[11]

Consumer Reports has been active in efforts to advance privacy protections in the states, and these experiences inform our feedback on this bill. For example, we were involved in negotiations over CCPA clean-up bills in the 2019 legislative session[12] and have closely observed consumers' experiences as they have tried to exercise their rights under the CCPA.[13] We have also helped shape the pending Washington Privacy Act, helping to transform it from a weak privacy bill, which nearly passed the Washington State legislature over the objections of privacy advocates,[14] to a much-improved 2020 version.[15] It is from this perspective that we offer recommendations to make the SAFE DATA Act more workable for consumers.

Below, we outline several suggested improvements for the SAFE DATA Act.

- **Privacy should be protected by default.** Data minimization — limiting the collection, use, sharing, and retention of data to what is reasonably necessary to operate the service requested by the consumer — is a key principle that should be included in any data

---

[8] *IAB CCPA Compliance Framework for Publishers & Technology Companies,* INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2019), https://www.iab.com/wp-content/uploads/2019/12/IAB_CCPA-Compliance-Framework-for-Publishers-Technology-Companies.pdf.

[9] Allison Schiff, *Google Will Integrate With IAB Tech Lab's CCPA Compliance Specs By Jan. 1 Deadline*, ADEXCHANGER (Dec. 4, 2020), https://www.adexchanger.com/privacy/google-will-integrate-with-iab-tech-labs-ccpa-compliance-specs-by-jan-1-deadline/; Google, Helping advertisers comply with CCPA in Google Ads (last visited Feb. 23, 2020), https://support.google.com/google-ads/answer/9614122.

[10] Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, WSJ (Dec. 12, 2019), https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175345.

[11] Natasha Singer and Aaron Krolik, *Grindr and OkCupid Spread Personal Details, Study Says*, N.Y. TIMES (Jan. 13, 2020), https://www.nytimes.com/2020/01/13/technology/grindr-apps-dating-data-tracking.html.

[12] Joint News Release: Privacy Groups Praise CA Legislators for Upholding Privacy Law Against Industry Pressure (Sept. 13, 2019), https://advocacy.consumerreports.org/press_release/joint-news-release-privacy-groups-praise-ca-legislators-for-upholding-privacy-law-against-industry-pressure/.

[13] Maureen Mahoney, *Preliminary Results are In! CCPA Testers Provide Important Insights into the Landmark Privacy Law*, MEDIUM (Jun. 8, 2020), https://medium.com/cr-digital-lab/preliminary-results-are-in-ccpa-testers-provide-important-insights-into-the-landmark-privacy-law-c299f733de09.

[14] Letter from Consumer Reports et al. to The Honorable Christine Rolfes (Feb. 21, 2019), https://advocacy.consumerreports.org/wp-content/uploads/2019/02/SB-5376-Privacy-Coalition-Letter-Oppose.pdf; Letter from Consumer Reports et al. to The Honorable Zach Hudgins (March 25, 2019), https://advocacy.consumerreports.org/wp-content/uploads/2019/03/Privacy-Coalition-Letter-Opposing-ITED-v.-4.pdf.

[15] Maureen Mahoney, *Washington State Fails to Advance Game-Changing Privacy Law*, MORNING CONSULT (Mar. 16, 2020), https://morningconsult.com/opinions/washington-state-fails-to-advance-game-changing-privacy-law/.

privacy law. In this bill, collection and use isn't meaningfully restricted, because the SAFE DATA Act only limits collection and use to the purposes listed in the privacy policy. A company could list any purpose in the privacy policy, emboldened by the fact that most consumers don't read or understand them. The language in this bill also has fairly wide loopholes for data processing "reasonably expected in the context" of the consumer's relationship with the business, and for improving the service — all of which could accommodate a host of purposes that aren't truly necessary.

If data is minimized by default, then empowering consumers to control for secondary use is not necessary. But in the absence of privacy by default, mechanisms to enable consumers to exercise choice have to be scalable and workable**.** Under this bill, the primary way that consumers can control the transfer of their data to third parties is by having them individually opt out of every unwanted data processing behavior. Opt out approaches simply aren't practical — it is too difficult for consumers to opt out of the sale of their data from every company. To put things into perspective, the California data broker registry alone has nearly 400 companies listed.[16] Further, some companies aren't even putting Do Not Sell links on their homepages as required by the CCPA, and of those that do, they're not always easy to spot. Some opt outs involve onerous processes like downloading third-party software. At the very least, a bill should require companies to honor universal opt-out mechanisms like the National "Do Not Call" registry, or universal opt-out signals such as "Do Not Track." The CCPA, for example, requires companies to honor browser privacy signals as universal opt outs, which makes the law far more workable for consumers.[17] While unnecessary data sharing and sales should optimally be prohibited by default, at the very least, global controls must be available to meaningfully empower individuals to exercise agency over their personal information.

- **Disparate treatment for individuals who exercise privacy rights should be prohibited.** The SAFE DATA Act includes language similar to the CCPA that could allow companies to charge consumers for exercising their rights under the law. This language was one of the primary reasons why Consumer Reports could not support the CCPA.[18] Such language could render privacy rights attainable only to those who can afford it. Privacy is a right, and should be available to everyone. The language instead should clarify that companies may not treat consumers differently for opting out of unnecessary data processing, or not agreeing to secondary collection or sharing for data monetization. Consumer Reports would be happy to provide language clarifying that bona fide loyalty programs, that reward consumers for repeated patronage but do not

[16] State of California Department of Justice, Data Broker Registry (last visited Sept. 19, 2020), https://oag.ca.gov/data-brokers.
[17] Cal. Code Regs. tit. 11 § 999 315(c) (2020).
[18] Consumer Reports, Letter to California Legislature Re: AB 375 (Jun. 28, 2018), https://advocacy.consumerreports.org/wp-content/uploads/2018/06/CU-Letter-AB-375-final-1.pdf.

disclose data to third parties pursuant to those programs, are permitted. Additionally, the Washington Privacy Act does a good job of addressing this important issue.[19]

- **Tighten the definition of service provider.** Many companies have exploited loopholes in the service provider definition of the CCPA to continue to deliver targeted advertising outside of the opt out. For example, companies have claimed that hundreds of unknown companies can be considered "service providers" in order to deliver targeted advertising. The SAFE DATA Act likewise has a definition of service provider that could be exploited in bad faith by data brokers. The bill should specify that when the consumer has opted out of the sharing of their information, data cannot be shared — even with a service provider — to target advertising on another site or service. Second, the bill should prohibit companies from combining data across clients. Service providers should be working on behalf of one company at a time. Allowing companies to claim that they're just service providers for everyone swallows the rules and lets third parties amass huge, cross-site data sets. Without clarification, the rights offered by this bill may be rendered largely meaningless, frustrating consumers who wish to limit the widespread dissemination of their personal data to hundreds, if not thousands, of unknown companies.

- **Eliminate loopholes in access, deletion, correction, and portability provisions.** We appreciate that the bill gives consumers the rights to access, delete, and correct their data, with provisions to encourage data portability. But vague loopholes in the provisions significantly undercut their utility. For example, under the bill, companies can deny these requests if it "would require disproportionate effort[.]" That language would give companies unacceptable leeway in denying requests, and it would be difficult to hold companies accountable for failing to extend consumers their rights. Similarly, portability is only required "to the extent that is technically feasible," which could also be exploited to avoid the requirement. While we appreciate the need for reasonable exceptions in edge cases, these open-ended and undefined provisions are too broad and invite abuse.

- **Strengthen enforcement.** Without strong enforcement provisions, companies simply won't comply with the law. In the SAFE DATA Act, enforcement is limited to the FTC and state attorneys general, which does not significantly expand their existing authority under UDAP law to take action against companies for bad privacy and security practices. Strong enforcement, including a private right of action, is essential, a fact that is

[19] Washington Privacy Act, SB 6281 (2019-20), https://app.leg.wa.gov/billsummary?BillNumber=6281&Initiative=false&Year=2019.

highlighted by widespread noncompliance with the CCPA and the GDPR, both of which have inadequate enforcement provisions.[20]

- **Narrow preemption language that would needlessly invalidate stronger state laws.** As written, this bill would upend stronger state-level protections, including the CCPA and the Maine broadband privacy law,[21] and the more expansive data broker registry requirements in Vermont[22] and California.[23] States have been the leaders on privacy in the face of years (if not decades) of inaction on the federal level. States and localities need the flexibility to deal with emerging technologies such as the use of facial recognition in physical spaces — and arguments over difficulties of compliance do not hold up where compliance can be easily segmented based on location. At the very least, federal privacy efforts should not take away protections already available to consumers on the state level.

We thank you again for your leadership on this important issue, and look forward to working with you to ensure that consumers have the strongest possible legal protections to safeguard their personal data.

Sincerely,

Justin Brookman
Director, Privacy and Technology Policy
Consumer Reports

Maureen Mahoney
Policy Analyst
Consumer Reports

cc: Members, Senate Committee on Commerce, Science, and Transportation

[20] Natasha Lomas, *GDPR's Two-Year Review Flags Lack of Vigorous Enforcement,* TECHCRUNCH (Jun. 24, 2020), https://techcrunch.com/2020/06/24/gdprs-two-year-review-flags-lack-of-vigorous-enforcement/.
[21] Sec. 1. 35-A MRSA c. 94 , https://www.mainelegislature.org/legis/bills/bills_128th/billtexts/SP056601.asp.
[22] 9 V.S.A. §§ 2430, 2433, 2446 and 2447,
[23] Cal. Civ. Code § 1798.99.80(d).