April 16, 2024

Chair Cathy McMorris Rodgers
Ranking Member Frank Pallone
House Committee on Energy and Commerce
Washington, D.C. 20515

Re: Discussion Draft of the American Privacy Rights Act (APRA)

Dear Chair McMorris Rodgers and Vice Pallone,

Consumer Reports[1] writes to share our initial thoughts on the committee's recently announced discussion draft of the American Privacy Rights Act (APRA). We commend the continued work of this committee in trying to enact federal privacy legislation and for its outreach to stakeholders to solicit feedback to ensure the bill works as intended. Consumer Reports has long argued in favor of federal privacy protections, and we support the bipartisan negotiations to develop a consensus solution to these pressing issues. However, as currently written, we believe the bill's privacy protections are not robust enough to justify the bill's preemption provisions that would undo important and evolving state and federal privacy laws.

The bill does include important protections for consumers, many of which have been carried over from the committee's last bipartisan proposal, the American Data Privacy and Protection Act (ADPPA). These include baseline consumer rights like the right to access, correct, and delete personal information held by companies, strong civil rights protections to safeguard consumers from discriminatory uses of data, and special protections relating to data brokers and large data holders.

That said, the bill's core protections relating to targeted advertising and online tracking — those tethered to the bill's data minimization, opt-in, and opt-out provisions — are too unclear and contradictory to support in their current form. To share one key example, under the current draft, information used to track consumers across apps and websites (the type of information commonly used for targeted advertising) is deemed as sensitive information (subject to both data minimization and opt-in consent), and the practice of targeting advertising using non-sensitive data is listed as an exception to the data minimization standard. Does that mean

[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.

that targeted advertising using sensitive data is prohibited by default? If so, then why is there a separate opt-out for targeted advertising later in the bill? If not, the bill takes a step back from ADPPA, which clearly prohibited as a matter of law the use of online behavioral data for targeted advertising. The text of the bill raises several other similar questions that are difficult to answer based on its current language.

Offering these ambiguous and sometimes contradictory protections at the expense of the developing body of state privacy law — many of which contain provisions that are considerably stronger than APRA — would be a bad deal for consumers at this time. For more detailed thoughts on these issues, please see the attached op-ed, “Unclear Protections in the American Privacy Rights Act Not Worth Broad Preemption.” We plan to follow-up with the committee with suggested language to address these and other concerns.

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

Sincerely,

Justin Brookman, Director, Technology Policy
Matt Schwartz, Policy Analyst
Consumer Reports

Unclear Protections in the American Privacy Rights Act Not Worth Broad Preemption

JUSTIN BROOKMAN / APR 11, 2024

Justin Brookman is the Director of Technology Policy for Consumer Reports.

Shutterstock

I am very torn on the subject of federal privacy legislation. On the one hand, it's something I've fought for for years, and American consumers deserve to have strong and comprehensive protections over what happens to their personal information. On the other hand, I am very worried about enacting and cementing imperfect privacy protections in place, undoing the substantial progress that has been made at the state level, and prohibiting states from iterating on protections over time. Federal privacy

law could be monumental if it gets the substance right, but it could also be disastrous if it preempts the states with a weak or unworkable standard.

Over the weekend, Senator Cantwell (Democratic Chair of the Senate Commerce Committee) and Representative McMorris Rodgers (Republican Chair of the House Energy & Commerce Committee) unveiled the text of American Privacy Rights Act of 2024 — the latest effort in a long-standing slog to enact federal privacy legislation. APRA is a carefully balanced compromise that will necessarily frustrate both sides, but which offers everyone something — companies get one standard that preempts states from enacting additional protections, and advocates get a nationwide law that includes novel protections as well as a private right of action.

The landscape has changed

One thing that's important to note at the beginning of this discussion is that the landscape at the state level is very different than it was even two years ago when Congress considered the American Data Privacy and Protection Act (or ADPPA) — the last major bipartisan effort at federal privacy legislation. Sixteen states have now enacted comprehensive privacy laws, most recently Maryland which enacted arguably the strongest yet, mandating companies only collect data as is necessary to provide the service requested by the consumer. California has refined and strengthened its privacy laws since enacting the California Consumer Privacy Act (CCPA) in 2018, adding strong new protections for mental health and sexuality data, enacting the DELETE Act to give consumers more control over data broker records — all while the California Privacy Protection Agency has initiated rulemaking on protections around automated decision making. Dozens of other states are considering similar protections around algorithmic decision making and AI in addition to their own comprehensive and sectoral privacy bills. Washington state passed the My Health, My Data Act strictly limiting secondary use of personal health information, while Massachusetts is considering legislation to prohibit the sharing of geolocation data with third parties.

So is passing APRA worth reversing all the state level gains? It's not, at least not as it's currently written. The text of the bill is largely borrowed from ADPPA, but it does fold in new elements, and perhaps as a result the overall structure is complicated, and at times contradictory. (To be fair, the bill was consciously distributed as a "discussion draft," and the authors have signaled a willingness to work with stakeholders to address concerns. We will be sharing specific suggestions with lawmakers to address these and other issues.)

Confusing treatment of online advertising

One of the first things I look for in privacy legislation is "how will the bill address targeted advertising and online data sharing?" Concerns about websites sharing your data with Google and Facebook, not

to mention hundreds of other ad-tech companies and data brokers, has fueled much of the drive for enacting privacy legislation, so it's important to know how legislation would try to rein in excessive practices.

Unfortunately, it is *very* difficult to assess what exactly APRA would do on this issue. Section 3(a) of the bill leads with a strong data minimization principle: companies can only collect, use, or share data to provide a specific product or service requested by an individual (with some explicit carveouts for operational administrative uses). This is what consumer advocates have largely asked for, including Consumer Reports (see for example our white paper with EPIC on guidance for FTC privacy rulemaking) — constraining data processing to consumer expectations rather than subjecting consumers to persistent and annoying opt-in requests, or difficult-to-use opt-out controls.

However, the APRA bill text then introduces a number of other exceptions and other intersecting and confusing provisions, leaving the reader unclear as to how different data elements are protected. "Targeted advertising" based on non-sensitive data is exempted from the data minimization requirements, subject only to an opt-out. Separately, Section 3(b) of the bill requires opt-in consent for the transfer of "sensitive" data to third parties (including data about online activities). It is not clear how this provision interacts with 3(a)'s data minimization rules — does the transfer also have to be specifically in service of a consumer request? The text is ambiguous, but it would be strange to treat the sharing of less sensitive data pursuant to a stronger standard (data minimization under 3(a)) than sensitive data (consent requirement under 3(b)). On the other hand, if 3(a) still applies, it's hard to see how targeted advertising based on sensitive data could ever be allowed. I would support that result, but it seems inconsistent with the rest of the bill (such as the definition of "targeted advertising" which includes targeting based on online behavioral data). If instead online targeted advertising is allowed under the bill, that would be a significant retreat from ADPPA, which prohibited most cross-website ad targeting without an opt-out or an opt-in.

There is also ambiguity about what constitutes "sensitive" data. The bill defines "information revealing an individual's online activities over time and across websites and online services" as sensitive, but what if websites share data about online activities one-at-a-time? That's how much online sharing works — you go to a website, and then that website tells dozens of other companies that you're there. Is that one site visit sensitive, requiring consent for transferring? Similarly, is "retargeting" — targeting ads based on just one website (such as a pair of shoes you looked at) — covered by the definition of targeted advertising? And if it isn't, is it completely fair game — not even subject to an opt-out — or is it strictly prohibited? I'm not sure of the answer to any of these questions based on the text of APRA.

While "targeted advertising" and some first-party advertising are carved out as exceptions to the bill's data minimization rule, other ad-tech functions like frequency capping, measurement, and attribution don't seem to be covered by the bill at all. Does that mean they are just prohibited by the bill's default data minimization language?

Or, do those functions fall under the bill's large carveouts for "service providers" who provide functionality on behalf of other companies? Would the bill simply allow companies to engage in most of the same data sharing behaviors they already do by simply designating partners as "service providers" who can then collect and merge data sets across their various customers? In response to state privacy laws — even laws intended to address sensitive data categories like personal health data — we've seen companies adopt aggressive interpretations of loopholes to simply engage in the same behaviors of sharing online behavior with dozens of sites at a time (while maybe passing along instructions limiting use of that data). Perhaps this bill would do no worse than existing state laws in actually reining in excessive data sharing. But it would also stop states from improving on their laws to address these concerns over time.

And in some cases, the bill actually backtracks from existing law. For example, Section 4(e) says that companies can make material changes to their privacy policies after the fact and treat previously collected data pursuant to those new policies so long as they try to let you know about it and give you the opportunity to opt out. That's a weaker standard than existing consumer protection law that says companies can only retroactively change privacy policies with your express permission. Perhaps not the biggest deal in the world since few people actually read policies, but this would render privacy policies even more meaningless, and deprive the FTC of a tool they've used for nearly twenty years to go after companies who've violated promises to consumers as to how they would treat your personal information.

Hazy rules for AI

The bill also tackles algorithmic discrimination, just as a host of bills across the country are purporting to do the same thing. Many of the protections are thoughtful and praiseworthy, but there are loopholes that could constrain their effectiveness. Companies are required to audit their algorithms for potential bias issues and harms to minors but not for other harms. Companies can also withhold not just information that would reveal "trade secrets" but anything it deems to be "confidential." Companies don't have to tell consumers when they lose out on an opportunity because of an algorithmic assessment, nor are they entitled to an explanation for when they do.

The bill also vaguely requires that companies offer an "opt-out" for consequential decision making, but doesn't provide any guidance as to what that means or what the alternative is (the Federal Trade Commission isn't empowered to engage in rulemaking but can offer informal "guidance"). Algorithmic "opt outs" have been an element of various state and international privacy laws for years now, but there is still a ton of uncertainty as to how exactly they do — or should — operate in practice. Some scholars have put a ton of practical thinking into how consumers should be able to opt out, contest, or otherwise appeal decisions made by AI and other algorithmic determinations, but it's a complicated and nuanced subject, and the current text of APRA doesn't offer a ton of clarity. Unlike with privacy

law, where we at least have some useful metrics as to what works and what doesn't, we don't have a lot of data about what effective consumer interventions with regard to algorithmic decision making looks like (apart from the Fair Credit Reporting Act and Equal Credit Opportunity Act, which mandates transparency, explainability, and appeal instead of an "opt out"). Freezing the law around a poorly articulated "opt-out" would constrain state policymakers from coming up with more measured approaches.

Reasons to believe, and work to be done

To be fair, the bill also has a number of novel elements that we haven't seen in a lot of state legislation to date, such as special rules to constrain the power of dominant social media companies, strong language clearly prohibiting retaliation against consumers who exercise privacy rights, and an opportunity for private citizens to enforce the law — a vital provision that understandably must have taken a great deal of negotiation and which has already drawn the ire of critics. Those — and other provisions — would all mark a dramatic improvement over the existing patchwork of state laws, and give consumer advocates reason to be enthusiastic about APRA's enactment.

But there's a huge cost as well if the bill were to invalidate current state laws — some of which have stronger elements than APRA — as well as future laws that could address holes that emerge from the law as well as new technologies. Congress has tried — and failed — to enact privacy legislation since at least the late Senator Fritz Hollings (D-SC) proposed the Online Personal Privacy Act nearly twenty-five years ago. If APRA is enacted, will Congress wait another twenty-five years to address new concerns? Meanwhile, California alone iterates and advances on its own privacy legislation *every year*. If broad preemption is going to be worth the tradeoff, the text of a bill would need to be exceedingly clear and strong — far stronger than existing state protections. APRA isn't there yet — and there's a short legislative window to address its issues — but we will work to hopefully get the bill to a place where its benefits outweigh its downsides for American consumers.

RELATED READING:

- The American Privacy Rights Act of 2024 Explained: What Does the Proposed Legislation Say, and What Will it Do?
- Can the American Privacy Rights Act Accomplish Data Minimization?
- Experts Provide Early Analysis of the American Privacy Rights Act

AUTHORS

JUSTIN BROOKMAN

Justin Brookman is the Director of Technology Policy for Consumer Reports. Justin is responsible for helping the organization continue its groundbreaking work to shape the digital marketplace in a way that empowers consumers and puts their data privacy and security needs first. This work includes us...

TOPICS

Privacy Transparency