ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

How to Improve the American Privacy Rights Act

ASH JOHNSON I JUNE 2024

America desperately needs a federal privacy law—but it needs the right federal privacy law. In its current state, APRA is not that law. But with a few important changes, it could be.

KEY TAKEAWAYS

- Congress should remove the data-minimization requirements from APRA and instead focus on giving consumers more control over their data.
- Congress should encourage consumers to take advantage of the diverse data-sharing economy instead of instructing the Federal Trade Commission (FTC) to establish a universal opt-out mechanism.
- Congress should avoid subjective buzzwords like "dark patterns" and instead prohibit objectively harmful practices.
- Congress should treat all online services equally instead of taking a retaliatory approach to "high-impact" social media companies.
- Congress should tailor its prohibition on retaliation against consumers who exercise enumerated privacy rights to prevent actual harms, and not allow freeloaders to take advantage of online services.
- Congress should close the loopholes in APRA's preemption of state privacy laws and include any issues missing from the bill, such as data breach notification.
- Congress should not include a private right of action in APRA, and should leave enforcement to the FTC and state officials.
- Congress should not include language from COPPA 2.0 or any other bill in the text of APRA.

CONTENTS

INTRODUCTION

The American Privacy Rights Act (APRA), Congress' latest attempt at comprehensive federal privacy legislation, passed a House subcommittee vote on May 23, 2024, advancing to a full House Energy and Commerce Committee vote, hopefully soon.[1] As the bill approaches this important milestone, it is crucial for Congress to evaluate provisions that could end up doing more harm than good for American businesses and consumers. America desperately needs a federal privacy law—but more than that, it needs the right federal privacy law. In its current state, APRA is not that law, but with a few important changes, it could be.

NO DATA MINIMIZATION

One of the obligations data holders would face under APRA is data minimization, which requires organizations to collect no more data than is necessary to meet specific needs. These needs include providing or maintaining a product or service the user requested or a communication to the user (other than an advertisement).

Exceptions to APRA's data-minimization requirement include data-security protection, complying with a legal obligation not preempted by APRA, preparing for legal claims, complying with a warrant, fulfilling a product recall or warranty, conducting market research, transferring assets for a merger or acquisition, providing call-location information, providing first-party or contextual advertising, providing targeted advertising to a user who has not opted out, conducting scientific research, or protecting against fraud or harassment, security incidents, public safety incidents, or criminal activity. Data holders also may use de-identified data to develop or enhance a product or service, and they may conduct internal research to improve a product or service.

Data-minimization requirements are popular in privacy legislation. However, they limit innovation by reducing access to data, limiting data sharing, and constraining the use of data. In particular, data minimization negatively impacts organizations that do not know which data will be most valuable when initially deciding what to collect, and it limits organizations' ability to analyze previously collected data as they develop new products and services.

Additionally, APRA's data-minimization requirements go much further than many state privacy laws.[2] For example, Virginia's privacy law limits organizations from collecting data beyond what is "adequate, relevant, and reasonably necessary" for disclosed purposes, unless the organization obtains the user's consent.[3] In contrast, APRA sets a much higher bar because the question is no longer whether an organization has minimized data collection only for disclosed purposes (or else has separately obtained users' consent), but rather whether a government regulator believes the organization's data collection is "necessary, proportionate, and limited" to providing a specific product or service. Tech companies, especially when facing hostile regulators, will likely find their decisions second-guessed on a highly subjective topic.

Many of the benefits that data can generate grow as more parties share data and as data becomes available to more parties. Many of these benefits are public goods, such as the benefits we derive from health research, increased energy efficiency, and smart city applications.[4] These benefits become harder to reach when less data is available, to society's detriment. Rather than viewing data collection and sharing as inherently negative and restricting those practices across the board, Congress should instead focus on giving consumers control over their personal data.

NO UNIVERSAL OPT-OUT MECHANISM

A similarly problematic provision in APRA would instruct the Federal Trade Commission (FTC) to establish within 2 years of the bill's enactment a universal opt-out mechanism that would allow consumers to opt out of all covered data transfers and targeted advertising. The only exceptions are the same as the exceptions to APRA's data-minimization requirement, minus advertising and scientific research. Notably, APRA does not take into account whether such a mechanism is technically feasible, let alone whether it is practical or cost-effective to implement.

Even if such a mechanism was both feasible and practical, this type of universal opt-out would likely encourage consumers to broadly restrict data sharing and opt out of all targeted advertising without considering the societal implications of their decisions, rather than use the more granular controls available to them by different data holders. In addition to restricting the beneficial uses of data, this would shrink ad revenue for online services that consumers get for free or at a low cost today, including news, apps, games, and more. To make up for the loss in revenue, these services would either need to show more ads that are less relevant, or start charging more for their services, or start charging for services that were previously free.

The benefits and risks of data sharing vary greatly depending on who is collecting the data and how they are using it. A universal opt-out mechanism that does not distinguish between different data holders and different uses of data does not accurately reflect the diverse data-sharing economy that exists in the United States. Rather than encouraging consumers to opt out of data sharing entirely, Congress should encourage them to take advantage of this diversity and its numerous immense benefits, both for individuals and for society.

NO PROHIBITION ON DARK PATTERNS

The APRA also includes a prohibition on "dark patterns," defined as a user interface designed to subvert or impair user autonomy.[5] Not only will this vague and subjective definition almost certainly complicate compliance for companies that want to abide by the law and avoid fines or expensive litigation, but the concept of dark patterns is problematic in itself.

The terminology is borrowed from anti-technology activists who accuse tech companies of using behavioral psychology to design products that manipulate people into taking actions that activists believe are contrary to users' best interests, such as consenting to share their personal data with an online service, clicking on an ad, or staying on a platform longer than intended. "Dark patterns" is a convenient label to excuse these inconvenient consumer behaviors, rather than acknowledging that consumers do not always act logically, and they especially do not always act according to anti-technology activists' logic.

In reality, consumers might choose to share their personal data with an online service because they want to use certain features that require data-sharing, or simply because they trust the online service and see no harm in sharing their data. Consumers might click on an ad because they are interested in the product or service being advertised, particularly if the ad has accurately targeted their interests. Finally, consumers might spend longer than anticipated on a certain platform because they had a long day at work and find it relaxing to view online content from their friends or like-minded strangers.

The assumption that consumers only act contrary to anti-technology activists' expectations because of manipulative "dark patterns" leads to paternalistic data privacy laws and regulations, because the assumption itself is paternalistic.[6] It is not an objective descriptor but a loaded term that critics can easily use to label design choices as being nefarious simply because they are effective. Congress should avoid subjective buzzwords like "dark patterns" and stick to prohibiting objectively harmful practices.

NO SEPARATE REQUIREMENTS FOR SOCIAL MEDIA

APRA includes a separate category of data holders, "covered high-impact social media companies," which are defined as any Internet-accessible platform that generates at least $3 billion in global revenue annually, has 300 million or more monthly active users globally, and provides an online service for users to access or share user-generated content. This definition explicitly targets a select few companies, not coincidentally many of the same companies that anti-technology advocates target in their critiques of "Big Tech."[7]

These high-impact social media companies receive different treatment under certain provisions of APRA. For example, the bill's definition of first-party advertising excludes advertising on high-impact social media companies. Likewise, APRA's definition of a loyalty program excludes programs offered by high-impact social media companies. This would functionally ban targeted advertising for popular social media platforms, which is how most of these platforms currently monetize their services instead of charging users.

Furthermore, APRA's definition of the "sensitive covered data" that is subject to opt-in requirements includes information revealing an individual's online activities over time on any online service operated by a high-impact social media company. Finally, the bill's definition of

targeted advertising includes any online advertisement for a third-party product or service by a high-impact social media company based on first-party data.

Large social media companies do not pose a greater privacy risk to users than any other comparable online service. The only reason to include these exceptions and additional requirements for large social media companies is to retaliate against "Big Tech" for perceived offenses.[8] Congress should not take this retaliatory approach in APRA; lawmakers should treat all online services equally.

NO PROHIBITION ON RETALIATION

As a final obligation, the APRA prohibits data holders from "retaliating" against consumers for exercising any of the privacy rights that the bill enumerates by denying products or services, charging different prices or rates, or providing a different level of quality, with the exception of loyalty programs, incentives for participation in market research, or collection and processing of data necessary for the function of a product or service. Calling these actions "retaliation" is loaded language intended to negatively portray standard practices used by businesses to monetize their products and services.

This requirement would create a freeloader problem for online services, wherein users could still reap the benefits of data sharing even if they have opted out of sharing their own data. For example, users would benefit from a free service that uses targeted advertising as a source of revenue even if they have opted out of targeted advertising. Likewise, this requirement would punish users who do not opt out of data sharing. For example, if enough users of a free service opt out of targeted advertising to the point where the service loses an important source of revenue and needs to start charging users, all users would have to start paying the same fee to access the service, even those who did not opt out of targeted advertising.

Congress should avoid creating these problems by tailoring the prohibition on retaliation to prevent actual harm to consumers, and should prevent freeloaders from taking advantage of online services that rely on data sharing or targeted advertising.

FULL STATE PREEMPTION

An important feature of any effective federal privacy law is preempting the growing patchwork of state privacy laws that pose costly and complicated compliance challenges for data holders and replacing it with a single national standard.[9] APRA would preempt state privacy laws, including the comprehensive data privacy laws passed so far in 18 states, but it includes a long list of exceptions to this preemption, such as for state laws governing consumer protection, civil rights, privacy rights of employees, privacy rights of students, data breach notification, nonconsensual pornography, child sexual abuse material, financial information, electronic surveillance, spam, health information, and more.[10]

This Swiss cheese approach to preemption fundamentally undermines the purpose of keeping compliance costs low, reducing confusion, and ensuring all Americans have equal data privacy protections. Allowing states to legislate on niche data-privacy and security issues instead of addressing those issues in a federal law will, in fact, do the opposite, increasing costs and confusion. Congress should close these loopholes in APRA's preemption provision, and include any issues missing from the bill, such as data-breach notification.

APRA also includes provisions from California's Consumer Privacy Act (CCPA) and Consumer Privacy Rights Act (CPRA), and Illinois' Biometric Information Privacy Act (BIPA). No other states are included in these special carve-outs, which are clearly an attempt at compromise with key lawmakers stemming from backroom dealing. This gives two states an unfair advantage over 48 others. Congress should remove these provisions, both in the name of fairness and in the name of reducing costs, as California and Illinois' laws are some of the most expensive in the country.[11]

NO PRIVATE RIGHT OF ACTION

Notably, APRA includes a private right of action, allowing individuals to sue for violations of certain provisions, mostly those regarding consumers' privacy rights. A court may award injunctive and declaratory relief, as well as the sum of actual damages, attorney's fees, and litigation costs. Data holders have a 30-day opportunity to cure, except in cases involving alleged substantial privacy harm. In other words, within 30 days of receiving written notice of an alleged violation, data holders will be able to address the violation and ensure such violations will no longer occur, and thus avoid a lawsuit. Pre-dispute arbitration agreements would also not be valid in cases of alleged substantial privacy harm or alleged privacy harm to minors.

APRA's limitations on why an individual can sue and how much they can sue for will hopefully deter expensive, frivolous lawsuits. However, APRA's private right of action is still likely to be the bill's most expensive provision, especially since it includes a carveout for BIPA violations, which have led to multiple multimillion-dollar lawsuits, and the CPRA's private right of action for data breaches, which will drive costs up even higher.[12]

To reduce the huge burden of litigation on companies, Congress should remove APRA's private right of action and leave enforcement to the FTC and states. Combined, federal and state authorities are more than capable of enforcing APRA and protecting consumers in a far less costly way. Moreover, once again, California and Illinois do not deserve special treatment, and that includes having their private rights of action included in a federal privacy law to the exclusion of all other states.

DO NOT INCLUDE COPPA 2.0

Finally, a recent change to APRA included language from another bill, the Children and Teens' Online Privacy Protection Act (COPPA 2.0).[13] This bill would amend existing federal children's privacy legislation, the Children's Online Privacy Protection Act (COPPA), originally passed in 1998.[14] Currently, COPPA applies to users under 13, prohibiting online services from collecting their personal information without parental consent. COPPA rules apply when an online service is directed toward children and has "actual knowledge" that a minor under 13 is using their service.

COPPA 2.0 would expand children's privacy protections to users aged 13 to 16 and change the standard for online services, requiring them to comply if they have actual knowledge or "knowledge fairly implied on the basis of objective circumstances" that a minor under 17 is using their service. This will create a costly minefield of potential liability for online services, which will take away resources from innovating new products, services, and safety features, and funnel them into compliance efforts. It may also require online services to collect more personal

information about their users to determine who is an adult and who is a child, which runs contrary to APRA's intended purpose.

COPPA 2.0 would also ban targeted advertising to children and teens. Because much of the Internet relies on targeted advertising to pay for services that are free or lower-cost than would otherwise be possible, this ban would likely result in fewer online services designed for children, and particularly fewer free online services designed for children, including educational content and wholesome entertainment that many families rely on to keep kids engaged and learning.

Including COPPA 2.0 in APRA introduces all of these flaws into the bill.[15] If Congress wants to pass amendments to COPPA, it should do so separately, rather than further complicating the already fraught path toward passing a much-needed comprehensive federal privacy law.

CONCLUSION

While APRA is far from perfect, there are specific adjustments Congress can make to strike the right compromise for America. These include removing data-minimization requirements, the universal opt-out mechanism, and the prohibitions on dark patterns and retaliation. Above all, Congress should ensure APRA fully preempts state laws, contains neither a private right of action nor language from COPPA 2.0 or any other children's privacy legislation that is still under debate. With these changes, APRA would transform from a flawed draft into an effective, targeted national privacy law that addresses actual harms while reducing costs that hinder innovation.

About the Author

Ash Johnson is a senior policy analyst at ITIF. She researches and writes about Internet policy issues such as privacy, security, and platform regulation. She was previously at Software.org: the BSA Foundation and holds a master's degree in security policy from The George Washington University and a bachelor's degree in sociology from Brigham Young University.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute that has been recognized repeatedly as the world's leading think tank for science and technology policy. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit itif.org/about.

ENDNOTES

1. "American Privacy Rights Act [Discussion Draft]," Congress, accessed June 6, 2024, https://d1dth6e84htgma.cloudfront.net/PRIVACY_04_xml_d1d6b82f10.pdf; Ashley Johnson, "Privacy and Children's Online Safety Bills Still Contain Serious Flaws, Says ITIF," ITIF news release, May 23, 2024, https://itif.org/publications/2024/05/23/privacy-and-childrens-online-safety-bills-still-contain-serious-flaws/.
2. Jordan Francis, "Unpacking the shift toward substantive data minimization rules in proposed legislation," International Association of Privacy Professionals, May 22, 2024, https://iapp.org/news/a/unpacking-the-shift-towards-substantive-data-minimization-rules-in-proposed-legislation.
3. Code of Virginia Title 59.1, Chapter 53.
4. Colin Cunliff, Ashley Johnson, and Hodan Omaar, "How Congress and the Biden Administration Could Jumpstart Smart Cities With AI" (ITIF, March 2021), https://www2.itif.org/2021-smart-cities-ai.pdf.
5. Daniel Castro, "The FTC's Efforts to Label Practices 'Dark Patterns' Is an Attempt at Regulatory Overreach That Will Ultimately Hurt Consumers," ITIF *Innovation Files* commentary, January 4, 2023, https://itif.org/publications/2023/01/04/the-ftcs-efforts-to-label-practices-dark-patterns-is-an-attempt-at-regulatory-overreach-that-will-hurt-consumers/.
6. Daniel Castro, "Trust Us, We Know Best: The Steady Rise of Privacy Paternalism," ITIF *Innovation Files* commentary, June 24, 2021, https://itif.org/publications/2021/06/24/trust-us-we-know-best-steady-rise-privacy-paternalism/.
7. Daniel Ku, "Which Social Media Platforms Make The Most Revenue?" *PostBeyond*, August 3, 2021, https://www.postbeyond.com/blog/revenue-per-social-media-user/.
8. Robert D. Atkinson et al., "A Policymaker's Guide to the 'Techlash'—What It Is and Why It's a Threat to Growth and Progress" (ITIF, October 2019), https://itif.org/publications/2019/10/28/policymakers-guide-techlash/.
9. Daniel Castro, Luke Dascoli, and Gillian Diebold, "The Looming Cost of a Patchwork of State Privacy Laws" (ITIF, January 2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/.
10. Andrew Folks, "US State Privacy Legislation Tracker," International Association of Privacy Professionals, updated May 28, 2024, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
11. Daniel Castro and Ash Johnson, "Why Can't Congress Pass Federal Data Privacy Legislation? Blame California," ITIF *Innovation Files* commentary, December 13, 2019, https://itif.org/publications/2019/12/13/why-cant-congress-pass-federal-data-privacy-legislation-blame-california/.
12. Castro, Dascoli, and Diebold, "The Looming Cost."
13. "S. 1418 – Children and Teens' Online Privacy Protection Act," Office of Senator Ed Markey, accessed June 6, 2024, https://www.markey.senate.gov/imo/media/doc/coppa_20billtext.pdf.
14. 15 U.S.C. 6501.
15. Ash Johnson, "Updated Children's Safety Bills Still Contain Serious Flaws," ITIF *Innovation Files* commentary, March 6, 2024, https://itif.org/publications/2024/03/06/updated-childrens-safety-bills-still-contain-serious-flaws/.