June 10, 2024

The Honorable Cathy McMorris Rodgers,
Chairman
U.S. House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone,
Ranking Member
U.S. House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Re: Opposition to the APRA as Drafted

Dear Chairman Rodgers and Ranking Member Pallone:

The undersigned consumer, privacy, civil rights, and advocacy groups write to express our concerns and opposition to the American Privacy Rights Act (APRA) in its current form. While we appreciate that the updated draft of the APRA includes a centralized deletion mechanism, it falls short of the landmark California Delete Act in several critical areas and threatens to undermine future progress for consumers.

Concerns Regarding Data Broker Industry

Data brokers pose a significant and growing threat to privacy, national security, and civil liberties.[1] These entities enable aggressive targeting of vulnerable populations, such as "economically anxious elders," "heavy purchasers of pregnancy tests," and people who are "frequently depressed."[2] In 2022, it cost just $160 to purchase the precise geolocation

[1] Office of the Director of National Intelligence, *Declassified Report on Commercially Available Information (CAI)* January 2022, at 3, 8, https://www.odni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf (last visited March, 2024), stating "(last visited June 10, 2024), stating, "There is today a large and growing amount of [Commercially available information] that is available to the general public, including foreign governments (and their intelligence services) and private-sector entities, as well as the [Intelligence Community]. . . It also raises significant issues related to privacy and civil liberties."

[2] Jon Keegan & Joel Eastwood, *From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You,* The Markup (June 8, 2023), https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you (last visited June 2024).

information of anyone who visited a Planned Parenthood clinic,[3] and criminals have leveraged data brokers to enable and even automate identity theft, stalking, and harassment on a massive scale.[4] As the industry receives increased scrutiny, reports and headlines only continue[5] to surface[6] detailing abusive[7] and concerning[8] data broker practices.[9]

The risks associated with data brokers extend beyond individual privacy violations. President Biden recently issued an executive order to prevent data brokers from selling Americans' sensitive personal information to foreign entities, acknowledging that such sales raise significant national security concerns, including counterintelligence and blackmail risks, particularly for those in the military or intelligence community.[10] In addition, with reproductive rights and gender-affirming healthcare under attack across the country, the threat posed by data brokers has taken on new urgency, as law enforcement agencies have exploited these entities to circumvent Fourth Amendment protections.[11]

Prohibition on Authorized Agents

One major concern with the APRA is that it prohibits authorized agents from accessing or utilizing the centralized deletion mechanism. Section 112(c)(3)(B)(iii) and Section 112(c)(3)(B)(iv) establish

---

[3] Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, Vice (May 3, 2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood (last visited June 2024).

[4] Joseph Cox, *The Secret Weapon Hackers Can Use to Dox Nearly Anyone in America for $15*, 404 Media (Aug. 22, 2023, 8:34 AM), https://www.404media.co/the-secret-weapon-hackers-can-use-to-dox-nearly-anyone-in-america-for-15-tlo-usinfosearch-transunion/ (last visited June 2024).

[5] Ashley Belanger, *Data broker's "staggering" sale of sensitive info exposed in unsealed FTC filing*, Ars Technica (Nov. 7, 2023, 12:59 PM), https://arstechnica.com/tech-policy/2023/11/data-brokers-staggering-sale-of-sensitive-info-exposed-in-unsealed-ftc-filing/ (last visited June 2024).

[6] Zane McNeill, *Data Broker Sold Data From 600 Planned Parenthood Visits to Anti-Abortion Group*, Truthout (Feb. 15, 2024), https://truthout.org/articles/data-broker-sold-data-from-600-planned-parenthood-visits-to-anti-abortion-group/ (last visited June 2024).

[7] Katherine Hamilton, *U.S. Government Buying 'Intimate' Data About Americans, Report Finds*, Forbes (Jun. 12, 2023, 5:33 PM), https://www.forbes.com/sites/katherinehamilton/2023/06/12/us-government-buying-intimate-data-about-americans-report-finds/ (last visited June 2024).

[8] Jessica Lyons, *96% of US hospital websites share visitor info with Meta, Google, data brokers*, The Register (Apr. 11, 2024, 3:00 PM UTC), https://www.theregister.com/2024/04/11/hospital_website_data_sharing/ (last visited June 2024).

[9] Suzanne Smalley, *Data brokers are selling US service members' secrets, researchers find*, The Record (Nov. 6, 2023), https://therecord.media/data-brokers-are-selling-military-secrets (last visited June 2024).

[10] *FACT SHEET: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data*, https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/ (last visited Mar. 2024).

[11] Lauren Sarkesian & Spandana Singh, *How Data Brokers and Phone Apps Are Helping Police Surveil Citizens without Warrants*, Issues in Science and Technology (Jan. 6, 2021), https://www.newamerica.org/oti/articles/how-data-brokers-and-phone-apps-are-helping-police-surveil-citizens-without-warrants/ (last visited June 2024).

a "do not collect" and “delete my data” mechanism for consumers to use, but explicitly state that requests must come from "an individual...and not a third party on behalf of the individual."

This language echoes a provision in California Senate Bill 1076, introduced earlier this year, which sought to undermine the Delete Act by introducing restrictions that all but barred authorized agents from making use of the deletion mechanism central to the Act.[12] Following significant backlash, the author pulled the bill prior to its first committee hearing. The resurfacing of this language in the APRA raises concerns that data broker industry representatives are attempting to shape federal policy after being rebuffed at the state level.

The prohibition disproportionately impacts vulnerable populations such as elderly people, non-native English speakers, victims of crime, domestic violence survivors, and individuals targeted by stalking or harassment. These individuals may lack the technical knowledge, time, or resources to navigate the complex process of submitting deletion requests to numerous data brokers and may also have heightened privacy concerns that make them reluctant to engage directly with data brokers. Many rely on trusted third parties to assist them in exercising their privacy rights, such as adult children helping their elderly parents, parents protecting their minor children, or nonprofit organizations serving communities with language barriers, disabilities, or specific privacy needs. By denying people the choice to work with an authorized agent, the APRA creates an inconsistent model where authorized agents can assist with exercising APRA rights but not with the centralized deletion and do-not-collect mechanism, effectively limiting access to this critical privacy protection for those who need it most.

Lack of Robust Reporting and Transparency Requirements

The APRA lacks the robust reporting and transparency requirements found in the California Delete Act. While we appreciate the APRA requirement for data brokers to provide a "description of the categories of covered data the data broker collects, processes, retains, or transfers" (Sec. 112(c)(2)(B)(ii)), the California Delete Act goes further by setting clear requirements to specifically disclose sensitive information practices such as selling reproductive healthcare data, minors' data, and precise geolocation data, and requires brokers to disclose any broad exemptions they may be claiming.

Moreover, the Delete Act mandates that data brokers share precise metrics about the CCPA requests they received and responded to in the previous year. Going further, the Delete Act sets regular audit requirements to ensure that data broker practices line up with their reporting.

[12] *California S.B. 1076, Data brokers: accessible deletion mechanism*, 2023-2024 Leg., Reg. Sess. (Cal. 2023), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB1076 (last visited June 2024).

These granular transparency provisions are absent in the APRA, risking that data brokers will continue to obfuscate their practices, leaving consumers unaware of the extent to which their sensitive information is being bought and sold without their knowledge or consent.

Removal of Stipulated Fines

The updated draft of the APRA removed the already insufficient stipulated fines present in the earlier version, further weakening enforcement and accountability. The previous fines, capped at a mere $10,000 per year and $100 per day, paled in comparison to the more robust penalties in the California Delete Act, which imposes a $200 per day fine for non-registration, a $200 fine for every instance of non-deletion and has no annual cap.

Section 112(d) now states that data brokers shall be liable for civil penalties under the FTC Act, rather than specifying fine amounts. This change places an undue burden on regulators to determine appropriate penalties on a case-by-case basis, potentially leading to inconsistent enforcement and weaker deterrence against violations.

Clear, substantial and stipulated fines in privacy legislation are crucial for ensuring compliance and holding bad actors accountable. By removing stipulated fines, the APRA risks emboldening data brokers to continue engaging in harmful practices without fear of significant financial consequences. The absence of a strong enforcement mechanism undermines the effectiveness of the law and leaves consumers vulnerable to ongoing privacy violations.

Preemption of the California Delete Act and State Privacy Laws Generally

The APRA's preemption of state privacy laws is a significant concern that undermines the ability of states to protect their residents' privacy. The California Delete Act, passed in 2023, represents only one of the recent groundbreaking state efforts to empower consumers and hold data brokers accountable.[13] Notably, the Delete Act's reporting requirements have already taken effect—revealing, for instance, that nearly 90 registered brokers are selling location data and dozens of brokers sell reproductive data or data on minors.[14] The deletion mechanism, set to

[13] Angelika Munger, ONE, TWO PUNCH: Maryland Signs into Law Consumer Data Privacy, While Vermont's BEAST of a Bill Awaits Signature, TCPAWorld (Troutman Amin, LLP), Nat'l L. Rev., https://natlawreview.com/article/one-two-punch-maryland-signs-law-consumer-data-privacy-while-vermonts-beast-bill (last visited June 2024).

Peter Hirschfeld, Vermont Legislature passes data privacy bill that could shape national efforts, Vermont Public (May 13, 2024), https://www.vermontpublic.org/local-news/2024-05-13/vermont-legislature-passes-data-privacy-bill-that-could-shape-national-efforts (last visited June 2024).

[14] California Privacy Protection Agency, Data Broker Registry, https://cppa.ca.gov/data_broker_registry/ (last visited June 2024).

provide consumers a free, easy-to-use, “one-click” mechanism to delete their information from data brokers, will take effect in 2026. By overriding this law, the APRA would not only strip away the benefits Californians are already experiencing from the increased transparency but also prevent the full realization of the Delete Act's potential before it even has a chance to be implemented.

The broad preemption provision in the APRA would effectively freeze privacy standards at the federal level, leading to the ossification of laws that fail to keep pace with evolving technologies and threats, such as the increasing use of artificial intelligence by data brokers to analyze and exploit consumer data.

Centralized deletion mechanisms were proposed and rejected multiple times at the federal level before the California Delete Act passed. The success of the Delete Act in California fundamentally shifted the conversation, making centralized deletion from data brokers not just a possibility, but a necessity. Had a broadly preemptive federal privacy law, such as the American Data Privacy and Protection Act (ADPPA) of 2023, been enacted as intended, it would have prevented the passage of the Delete Act in California and there would be no centralized data broker deletion mechanism (even the limited mechanism currently proposed in the APRA). This demonstrates the critical role that states play in driving innovation and positive change in consumer protection. By stifling future state-level efforts, the APRA risks leaving consumers with a one-size-fits-all approach that may not adequately address the diverse privacy concerns of individuals across the country.

In its current form, the APRA encourages a race to the bottom approach that puts American consumers at a disadvantage from the outset. The APRA must establish a strong baseline for privacy rights—a federal floor, not a ceiling—while allowing states the freedom to build upon these protections and address the unique needs of their constituents.

While the APRA purports to enhance consumer privacy rights, its current form falls short of providing the comprehensive protections that individuals need in the face of an increasingly invasive data broker industry. By prohibiting authorized agents, omitting robust transparency and audit requirements, removing stipulated fines, and, fundamentally, preempting stronger state laws, the APRA risks leaving consumers vulnerable to ongoing privacy violations and undermining the progress made by trailblazing legislation like the California Delete Act. For these reasons we must oppose the current draft of the American Privacy Rights Act, unless amended, and urge you to address these deficiencies to work towards a federal privacy law that truly puts consumers first.

Sincerely,

Lee Tien, Directing, Senior Staff Attorney
Electronic Frontier Foundation

Emory Roane, Associate Director of Policy
Privacy Rights Clearinghouse

Tracy Rosenberg, Executive Director
Media Alliance

Mike Katz-Lacabe, Research Director
Oakland Privacy

Sean Taketa McLaughlin, Executive Director
Access Humboldt