June 17, 2024

Re: Local, State, and National Advocacy Concerns with APRA's Approach to Preemption

Dear Representative:

The undersigned local, state, and national advocacy organizations write to raise our strong opposition to the potentially broad preemption of state and local laws by the American Privacy Rights Act (APRA), as marked up by the Innovation, Data, and Commerce Subcommittee on May 23.[1] APRA preempts certain state and local laws, and concerns have emerged around its impact on state and local protections now and in the future. This letter analyzes the many laws that could be affected by APRA. APRA is a complex bill and has many intersectional equities, including significant anti-discrimination provisions; consequently, many signatory organizations are not taking a stance on APRA at this time. Signatories may also have specific redlines to offer. However, the soundest approach to avoid the harms from preemption is to set the federal standard as a national baseline for privacy protections — and not a ceiling.

APRA's Preemptive Effect Could Be Sweeping, With Unpredictable Consequences
APRA would preempt state and local law on issues that are "covered by" the bill, with exceptions for listed categories of laws. APRA's scope is comprehensive, and consequently the effect of its preemption could be equally sweeping. APRA covers practices across nearly every economic sector and the entirety of the personal information lifecycle. Consequently, its preemptive effect might not only reach state "comprehensive" privacy laws governing personal information but may have less obvious and potentially serious impact on laws governing:

- auditing and assessing artificial intelligence (AI) systems;
- data broker registries and universal deletion mechanisms;
- defining and restricting targeted advertising;
- relief for privacy harms, including state laws with stronger relief than provided under APRA, such as by providing statutory damages;
- design codes, including those focused on age-appropriate design and privacy protections;
- the collection, use, and sale of information about children;
- collection, retention, destruction, disclosure, and sale of personal information, potentially implicating state and local laws requiring private business to retain certain records;
- universal opt-out mechanisms, including state opt-outs for profiling; and,
- cybersecurity requirements.

Preemption under APRA might reach so broadly because personal information is used in every economic sector, industry, and organization — a fact that states and localities have long recognized in promulgating not just comprehensive privacy laws, but laws regulating, for example, the privacy of utility usage. States have also previously regulated privacy regarding credit card transactions, activity on educational platforms, and the books we check out, both physically and electronically. As discussed below, APRA could

[1] This letter references the latest publicly available draft of APRA, available here.

potentially preempt many of these laws — with exceptions — without consideration of their tailoring for the specific needs of the industries, sectors, and activities they regulate.

APRA Could Block Important Future State and Local Responses to New and Emerging Harms

Although APRA's substantive provisions would establish protections for privacy and civil rights, preemption could freeze policy responses to new abuses of people's personal information to what can be enacted by Congress — and largely remove states from the calculus, unless they could fit their policy efforts within APRA's exceptions. This will undermine ongoing policy efforts across the country to respond to both long-standing and emerging harms.

For example, Colorado recently enacted legislation that requires impact assessments of artificial intelligence (AI) systems that make certain "consequential decisions." Other states are considering similar legislation, which could be "covered by" — and ostensibly preempted by — APRA. Similarly, states continue to experiment with approaches to children's use of technology, including through privacy legislation and design codes. Both approaches may include requirements regarding default privacy settings, privacy policies and terms of service, the sale of data, geolocation, and dark patterns — all issues "covered by" APRA.

Recent history has demonstrated that innovation and responsiveness at the state level are crucial in responding to emerging harms from technology. California passed the first U.S. comprehensive privacy law in 2018 and has since been followed by nearly twenty other states. Illinois passed protections for biometric privacy in 2008 and has been followed in dozens of other states, either in biometric-specific laws or comprehensive laws with biometric provisions. States' ability to innovate and iterate expands the menu of tested approaches not only for other states but for Congress as well.

In contrast, policymaking within Congress usually moves at a more deliberate pace, by constitutional design. Building sufficient, enduring consensus across both chambers to span ideological differences and overcome procedural hurdles can often take years, if not more than a decade. By way of illustration, Congress passed the Electronic Communications Privacy Act, which was originally enacted in 1986[2] — before the advent of the internet, the cell phone, the smartphone, cloud computing, and ChatGPT, to name a few technologies — and it has not been substantively updated since. Stripping states of their critical role in developing policy will not only deprive Americans of critical protections as technologies evolve but it will also deprive Congress of key models for legislation.

APRA Could Eviscerate Numerous Existing Stronger State and Local Protections for Privacy

In addition to undermining future policy responses, APRA could potentially preempt dozens of state laws already on the books that are stronger than APRA. And even if APRA does not ultimately preempt some of these provisions, preemption will be determined in case-by-case litigation, creating uncertainty around millions of peoples' privacy protections. The list below of potentially preempted state laws is only a handful of examples, and as described below, APRA's exceptions to preemption may be inapplicable to these examples. In many

[2] Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510 *et seq*., 2701 *et seq.*, 3121 *et seq.*).

cases, the state laws have fewer exceptions than APRA or provide bright-line rules that APRA does not. For example:

California

- **Constitutional right to privacy:** The California constitution guarantees "all people" the "inalienable" right to privacy.[3] This obligation applies not only to the California government, but to all private entities operating in California as well. The constitutional guarantee of privacy has been instrumental in holding major tech companies accountable for abuses of our data, including the Cambridge Analytica scandal.[4] California's constitutional protection has not only proven effective in countering data-driven harms but also flexible in adapting to changing data practices.[5]
- **Privacy for lawful healthcare:** California law prohibits California companies that provide communications services from complying with "an out of state subpoena, warrant," or other legal process unless the request is not connected to a prosecution of reproductive healthcare or gender affirming care.[6] In contrast, APRA would permit such disclosures; and because APRA covers private entities' disclosure of information pursuant to subpoenas, California's laws could potentially be preempted.
- **Communications privacy:** California, like other states, has passed laws protecting the privacy of our communications, including location data, from being obtained by governmental entities.[7] California, like other states, requires governmental entities to meet heightened requirements for warrants or specialized orders to compel the disclosure of our communications. APRA already exempts wiretap laws — a related but distinct area of law — from preemption; it should also exempt electronic communications privacy laws specifically or laws or rules governing regarding evidence, criminal and civil procedure, and discovery more generally.
- **Regulation of AI:** The California Privacy Protection Agency is currently considering draft regulations that would impose obligations on companies that use personal information in "automated decisionmaking technology" (ADMT) to make decisions about access to financial services, housing, education, employment and more. Companies would be required to provide notice of the ADMT's use, to allow for opt-out, and to access the personal information used by the ADMT.[8] Those rights may not be viewed as "traditional" civil rights, but people's rights established by California's comprehensive privacy law, and could potentially be preempted by APRA.

---

[3] Cal. Const. art. I, sec. 1, here.
[4] *E.g.*, *Google Settles $5 Billion Privacy Lawsuit Over Tracking People Using 'Incognito' Mode*, AP News, AP News (Dec. 29, 2023), here; Ashley Ahn, Facebook Parent Meta Will Pay $725M to Settle a Privacy Suit Over Cambridge Analytica, NPR News (Dec. 23, 2022), here.
[5] Adding an exception to preemption for state constitutional provisions would be welcome.
[6] Cal. Penal Code § 1546.5, here; *id.* § 13778.3(f), here. Because California's reproductive healthcare privacy laws extend to *any* information, we are concerned they will not be preserved by APRA's exception to preemption for "health information" privacy laws.
[7] Cal. Penal Code § 1546 *et seq.*, here.
[8] California Privacy Protection Agency, Fact Sheet: Draft Automated Decisionmaking Technology (ADMT) Regulations (2024), here.

Colorado

- **Regulation of AI:** Colorado recently passed a new law requiring developers and deployers of AI for use in "consequential decisions" to create impact assessments for the AI.[9] Consequential decisions grant or restrict access to financial services, housing, education, employment and more. The impact assessments must provide a description of the data used by the AI, its purposes and intended uses, details on the training of the AI, and means of testing performance — all topics covered by APRA.

Illinois

- **Biometric privacy:** APRA permits far more disclosure and retention of biometrics than Illinois's landmark Biometric Information Privacy Act (BIPA).[10] While BIPA limits disclosure to three permissible instances — with consent, for completing a financial transaction authorized by the subject, and as required by law or pursuant to a warrant or judicial subpoena — APRA is much more permissive, allowing transfer of biometrics for *seven* purposes. Those include transfer pursuant to an administrative subpoena or other "lawful process," for a merger or acquisition, or for broad public safety goals. Similarly, BIPA's restrictions on retention are concrete: there is a three-year cap on retention of biometrics. APRA, however, is again much more lenient, permitting retention for *nine* broad purposes.
- **Privacy for lawful healthcare:** Illinois law requires companies served with a subpoena for prosecution of reproductive healthcare or gender-affirming care to *not* comply with the subpoena. It also provides the companies with formal procedures to challenge the subpoena's validity.[11] Illinois similarly precludes disclosure of data collected from automated license plate readers for investigations of reproductive healthcare or immigration status.[12]

Maine

- **Internet privacy:** APRA also permits broader sharing and use of personal information than Maine's first-in-the-nation internet service provider (ISP) privacy law.[13] Maine's ISP privacy law provides robust limitations on the use and disclosure of our browsing history, app usage, geolocation, and the content of our communications. Maine permits disclosure only with consent, pursuant to a judicial order, or for other enumerated purposes — and unlike APRA, it does not permit use or disclosure for targeted advertising or expressly for security and law enforcement purposes. Maine's ISP privacy bill could potentially be preempted by APRA.

Massachusetts

- **Standards for the protection of the personal information of residents:** Massachusetts regulations establish minimum standards to be met by persons who own or license personal information about Massachusetts residents.[14] Massachusetts' regulations include specific, bright-line requirements such as physical security, access controls, disciplinary measures for violations of security policies, firewall protections, user authentication measures, and network monitoring — specific requirements not included in APRA. These protections could potentially be preempted by APRA.

---

[9] Colo. SB 24-205, here.
[10] 740 Ill. Comp. Stat. 14/1 *et seq.*, here.
[11] 735 Ill. Comp. Stat. 35/3.5(d), here; 735 Ill. Comp. Stat. 40/28-5, here.
[12] 625 Ill. Comp. Stat. 5/2-130, here.
[13] Me. Rev. Stat. tit. 35-A, § 9301, here.
[14] 201 Mass. Code Regs. 17.01–17.04, here.

New York

- **Privacy for lawful healthcare:** New York law prohibits New York companies that provide communications services from complying with "a warrant issued by another state" when the company "knows that the warrant relates to an investigation into" reproductive healthcare.[15] As noted above, APRA would permit such disclosures.
- **Privacy for vaccinations:** New York also provides protections for the privacy of vaccinations with bright lines limits on use that are not in APRA. For example, New York generally prohibits "vaccine navigators" — entities that facilitate access to vaccinations — from using, disclosing, or retaining personal information "except as necessary to provide services attendant to the delivery of immunization."[16] That law protects information beyond the fact that someone signs up for a vaccination, including myriad additional information that navigators collect.[17] That law consequently may not fall neatly within APRA's exception to preemption for "health information" privacy laws. New York prohibits providing that information to law enforcement or immigration authorities, which APRA could permit. Similarly, contact tracing information is protected as confidential and is generally prohibited from being disclosed to law enforcement or immigration authorities.[18]
- **Tenant privacy:** New York City also provides bright-line protections not in APRA for tenant privacy in buildings that use keyless access systems, such as keyless fobs, biometrics, or other electronic technologies.[19] Building owners are limited to collecting and utilizing only specific categories of data, must destroy access data after 90 days, and are prohibited from certain activities, such as tracking a tenant's location outside the building. APRA does not provide protections with that degree of specificity.

Many of these laws are "covered by" APRA's provisions governing disclosures to law enforcement, collection of information, the development of impact assessments, and more. Moreover, APRA's exceptions to preemption may not apply to these laws:

- For example, the exception for "health information" does not apply to the broad reproductive health privacy laws in California, New York, and Illinois; those laws protect *all* information and are not limited to "health information" as defined by APRA. A prosecutor might seek travel itineraries, text messages, and internet search history — all of which might be relevant to efforts to research or obtain reproductive or other healthcare, but might be interpreted by a court not to "describe[] or reveal[] the past, present, or future physical health, mental health, disability, diagnosis, or health condition or treatment of an individual" and consequently may not fall within APRA's "health information" exception to preemption. Moreover, the exception for "criminal laws" is likely inapplicable to these reproductive privacy laws because that exception applies only to laws "unrelated to data or data security."[20]
- Similarly, the preemption exception for state "civil rights" laws may not preserve state laws regulating AI. The impact assessments for AI in APRA are not limited to

---

[15] N.Y. Gen. Bus. Law §§ 394-f, here.
[16] N.Y. Pub. Health Law § 2169(2)(a), (c)(i).
[17] Sara Morrison, *You Got a Vaccine. Walgreens Got Your Data.*, Vox (Mar. 4, 2021), here.
[18] N.Y. Pub. Health Law § 2181(1), (6).
[19] N.Y. City Local Law No. 63 (2021), here.
[20] APRA, sec. 120(a)(3)(G).

"civil rights" but instead cover the full spectrum of AI's potential uses and corresponding harms. The same is true of impact assessments required by the law recently passed in Colorado and being considered in other states. A court considering a preemption challenge to a state impact assessment law may consequently consider them outside the scope of APRA's "civil rights" exception.

- APRA's carveout for state laws regarding "electronic surveillance, wiretapping, or telephone monitoring"[21] may not apply to state electronic communications privacy laws, as courts have treated wiretap and similar laws as applying to *real-time* surveillance and consequently distinguished them from state electronic communications privacy laws, which apply to communications that have *already been sent*.[22] At minimum, electronic communications privacy laws should be added to the exception for wiretap and related laws; ideally, the exception should apply to all laws and rules regarding governing regarding evidence, criminal and civil procedure, and discovery.
- Finally, APRA's exception for "consumer protection laws" only applies to "laws of general applicability,"[23] which may exclude sector-specific laws such as many listed here.

Even where ambiguities exist, they are accompanied by corresponding litigation risk. Preemption is usually determined on a case-by-case basis through litigation.[24] APRA could create substantial uncertainty for entities seeking to comply with state laws that may — or may not — be preempted.[25] Further, preemption creates the very real possibility that similar state laws will be treated very differently depending on the court, appellate circuit, or even the facts of the particular case.

Federal Law Should Provide a Floor for Protections, Not a Ceiling

The harms from APRA's approach to preemption — possibly sweeping preemptive effect, potentially undermining ongoing policy response to emerging harms and stronger state laws already on the books — could be avoided by allowing the protections provided by state laws to exceed those provided by APRA.

---

[21] APRA, sec. 120(a)(3)(L).

[22] In re Application for Pen Reg. & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005) (concluding that, while state ECPAs are "inherently retrospective" in capturing information that has already been sent, wiretap and surveillance laws are "inherently prospective"); *accord* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003), as amended (Jan. 20, 2004) (citing United States v. Steiger, 318 F.3d 1039, 1048–49 (11th Cir.2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir.2002); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457 (5th Cir.1994); see also Wesley College v. Pitts, 974 F. Supp. 375 (D.Del.1997), summarily aff'd, 172 F.3d 861 (3d Cir.1998)).

[23] APRA, sec. 120(a)(3)(A).

[24] *Cf.* Mozilla Corp. v. Fed. Commc'ns Comm'n, 940 F.3d 1, 81 (D.C. Cir. 2019) (conflict preemption "is an issue incapable of resolution in the abstract, let alone in gross" (internal quotation marks omitted)).

[25] Although the Supreme Court has applied a canon of statutory interpretation that cautions against interpreting a statute to preempt state law, that canon applies "unless [preemption] was the clear and manifest purpose of Congress." Wyeth v. Levine, 555 U.S. 555, 565 (2009). Where "the statute contains an express pre-emption clause," the canon is inapplicable. Puerto Rico v. Franklin Cal. Tax-Free Tr., 579 U.S. 115, 125 (2016) (internal citation omitted). APRA contains such an express preemption clause. APRA, sec. 120(a)(1).

Existing federal privacy and civil rights laws do not preempt stronger state protections or enforcement efforts. Indeed, federal consumer protection and privacy laws operate as regulatory baselines and do not prevent states from enacting and enforcing stronger state statutes. The Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Cable Communications Privacy Act, the Video Privacy Protection Act, the Employee Polygraph Protection Act, the Telephone Consumer Protection Act, the Driver's Privacy Protection Act, the Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act, and the Health Information Portability and Accountability Act all allow states to craft protections that exceed federal law. For more than six decades, Congress has taken the same approach in enacting federal civil rights laws, allowing states to enact and enforce their own stronger protections. There is no reason for Congress to take a different approach when enacting a new federal consumer privacy bill.

To be clear, we strongly support federal baseline privacy legislation that ensures a basic level of protection for all individuals in the United States. However, such federal legislation should allow state laws to provide stronger protections.

Thank you for your consideration and your continued support for establishing robust protections for our privacy. If you have any questions, please do not hesitate to contact us at cvenzke@aclu.org.

Sincerely,

National Organizations
American Civil Liberties Union
Center for Digital Democracy
Common Sense Media
Consumer Reports
Electronic Frontier Foundation
Grandmothers for Reproductive Rights (GRR!)
It Could Happen To You
Kairos Action
Policing and Social Justice Project
Restore The Fourth
Surveillance Resistance Lab
The Sidewalk Project
U.S. Public Interest Research Group (PIRG)

California
ACLU of Northern California
ACLU of Southern California
Asian Law Alliance
CalPIRG
Communities United for Restorative Youth Justice
Gente Organizada
ICE Out of Marin
Indivisible CA: StateStrong
Indivisible Sausalito

Maryland PIRG
MASSPIRG
Media Alliance
No Ethics In Big Tech
Oakland Privacy
Personal Data Solutions LLC
Privacy Rights Clearinghouse
Racial Justice Committee San Francisco Public Defender
Santa Cruz County Third District Supervisor's Office
Secure Justice
South Bay People Power
TechEquity Action
Together We Will/Indivisible-Los Gatos
UC Berkeley Labor Center
Universidad Popular

Colorado
ACLU of Colorado
CoPIRG

Illinois
ACLU of Illinois
Illinois PIRG
Lucy Parsons Labs

Maine
ACLU of Maine
EqualityMaine
Mabel Wadsworth Center
Maine Family Planning
Safe Abortions For Everyone Maine

Massachusetts
ACLU of Massachusetts
Campaign for Digital Fourth Amendment Rights
Watertown Citizens for Peace, Justice & the Environment

Nebraska
ACLU of Nebraska

New Mexico
ACLU New Mexico

New York
New York Civil Liberties Union (NYCLU)
S.T.O.P. - Surveillance Technology Oversight Project

Oregon
OSPIRG

Washington
ACLU of Washington