SQUIRE PATTON BOGGS

Evolving Privacy Challenges for Advertising

June 26, 2024

Agenda

I. Introductions

II. U.S. State Privacy Laws

III. Consumer Health Data Laws
IV. Policy Perspectives on Federal Privacy Lawmaking

V. What's Happening at the Federal Level?

Panel

Julia Jacobson

Partner

Squire Patton Boggs

(New York)

Faye Ricci

Associate General Counsel

Boeing Employee Credit Union

(Seattle)

Steve Elkes

President and Co-Founder of Curacity

(New York)

Stacy Swanson

Policy Advisor

Squire Patton Boggs

(Washington D.C.)

The Consent Challenge in Digital Advertising

SQUIRE PATTON BOGGS

Transparency requires explaining to consumers in advance why and how their personal information is collected and processed and the consequences of the processing.

A privacy notice (e.g., privacy policy) is transparent when it is clear, conspicuous and proximate to the point at which personal information is collected.

A privacy notice is context specific. *What works in one context does not automatically work in another*.

- Cookie vs. Non-Cooke Notice

A privacy notice generally must precede privacy consent. If notice is context specific, then consent is context specific.

Consent considerations: 'audience', location, law, information category, etc.

- **Age of privacy consent** varies, e.g., for certain digital advertising (see Section III).
- Age of privacy consent is not necessarily the same as the age of legal consent.

What’s up with Digital Advertising in the 19 State Consumer Privacy Laws

U.S. State Privacy Laws – 2023

SQUIRE PATTON BOGGS

Law	Right to Opt-Out of Sale	Right to Opt-Out of Targeted Advertising	Right to Opt-Out of Profiling	Choice Required for Processing Sensitive Personal Data	Assessments for Targeted Advertising
California Privacy Rights Act	✓	✓	**	Opt-Out	**
Virginia Consumer Data Protection Act	✓	✓	✓	Opt-In	✓
Colorado Privacy Act	✓	✓	✓	Opt-In	✓
Connecticut Public Act No. 22-15	✓	✓	✓	Opt-In	✓
Utah Consumer Privacy Act	✓	✓	X	Clear notice and opportunity to Opt-Out	X

U.S. State Privacy Laws – 2024

SQUIRE PATTON BOGGS

Law	Effective Date	Right to Opt-Out of Sale	Right to Opt-Out of Targeted Advertising	Right to Opt-Out of Profiling	Choice Required for Processing Sensitive Personal data	Assessments for Targeted Advertising
Texas Data Privacy and Security Act	**7/1/24**	✓	✓	✓	Opt-In	✓
Florida Statutes, Chapter 2023-201	**7/1/24**	✓	✓	✓	Opt-In	✓
Oregon Consumer Privacy Act	**7/1/24**	✓	✓	✓	Opt-In	✓
Montana Consumer Data Privacy Act	**10/1/24**	✓	✓	✓	Opt-In	✓

U.S. State Privacy Laws – 2025

SQUIRE PATTON BOGGS

Law	Effective Date	Right to Opt-Out of Sale	Right to Opt-Out of Targeted Advertising	Right to Opt-Out of Profiling	Choice Required for Processing Sensitive Personal data	Assessments for Targeted Advertising
Delaware Personal Data Privacy Act	1/1/25	✓	✓	✓	Opt-In	✓
Iowa's Act Relating to Consumer Data Protection	1/1/25	✓	✓	X	Clear notice and opportunity to opt-out	X
Nebraska's Data Privacy Act	1/1/25	✓	✓	✓	Opt-In	✓
New Hampshire Act Relative to the Expectation of Privacy	1/1/25	✓	✓	✓	Opt-In	✓
New Jersey Data Protection Act	1/15/25	✓	✓	✓	Opt-In	✓
Tennessee Information Protection Act	7/1/25	✓	✓	✓	Opt-In	✓
Minnesota Consumer Data Privacy Act	7/31/25	✓	✓	✓	Opt-In	✓
Maryland Online Data Privacy Act	10/1/25	✓	✓	✓	Sale prohibited	✓

U.S. State Privacy Laws – 2026

SQUIRE PATTON BOGGS

Law	Effective Date	Right to Opt-Out of Sale	Right to Opt-Out of Targeted Advertising	Right to Opt-Out of Profiling	Choice Required for Processing Sensitive Personal data	Assessments for Targeted Advertising
Indiana Consumer Data Protection Act	**1/1/26**	✓	✓	✓	Opt-In	✓
Kentucky Consumer Data Protection Act	**1/1/26**	✓	✓	✓	Opt-In	✓

Definitions

SQUIRE PATTON BOGGS

Sale/Sell

- State Consumer Privacy Laws that define a “sale” by exchange of **monetary consideration only**: Indiana, Iowa, Kentucky, Tennessee, **Utah**, and **Virginia.**
- State Consumer Privacy Laws that define a “sale” by exchange of **monetary or other valuable consideration**: **California** (includes third-party cookies), **Colorado**, **Connecticut,** Delaware, **Florida**, Maryland, Minnesota, **Montana**, Nebraska, New Hampshire, New Jersey, **Oregon,** and **Texas**

Targeted Advertising

- Generally, “displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests.” (***CT-DPA***)

Definitions

SQUIRE PATTON BOGGS

Profiling

- Generally, “means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.” (***VA-CDPA***)

Right to opt-out of the processing of personal data for profiling in furtherance of:

- **Automated decisions: Colorado, Florida, Oregon, Texas, Virginia**
- **Solely automated decisions**: **Connecticut, Montana**

Sensitive Personal Data

- Typically, personal data **revealing** racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status; genetic or biometric data processed for the purpose of uniquely identifying an individual; personal data of a known child.
  - Iowa: “’Sensitive data' **means** a category of personal data that includes the following …”
  - Colorado: “Sensitive Data Inferences” means inferences made by a Controller based on Personal Data, alone or in combination with other data, which are used to indicate an individual’s racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status.

Sensitive Personal Data & Digital Advertising

SQUIRE PATTON BOGGS

- Most of the state consumer privacy laws require opt-in consent:
  - Iowa & Utah : A controller must provide consumers with **clear notice and an opportunity to opt out before** processing sensitive data.
  - Texas & Florida: A controller must provide an affirmative statement, clearly and conspicuously given, when a controller/website sells sensitive personal data.
  - Maryland: The sale of sensitive personal data of minors (under the age of 18) is prohibited.
- New sensitive personal data categories:
  - Children's Data [*more on following slide*]
  - Consumer health data - applies to a broader set of personal data or is subject to greater restriction than the CCPA's definition of health data, such as gender-affirming health data and reproductive or sexual health data.
  - Data revealing a person's status as a victim of a crime.
  - Inferences from non-sensitive data that can reveal data that is sensitive data.
  - Transgender or nonbinary status.

Sensitive Data: Children's Data

SQUIRE PATTON BOGGS

- Based on the federal Children's Online Privacy Protection Act ("COPPA"), all state privacy laws treat a minor under the age of 13 as a child subject to parental consent for online personal data collection.
- Unlike COPPA, however, the state privacy laws apply to personal data *about* the child collected *offline* and online.
- Some states limit the processing of children's data regardless of the consent of the minor or his/her parent.
- All of the state consumer privacy laws require verified parental consent to process personal data for **targeted advertising** of children under age 13. California requires consent of a consumer at least age 13 but under age 16 for processing personal data. Other states apply more stringent standards:
  - Consent for targeted advertising, sale and/or profiling: Oregon (under age 16) and New Jersey (under age 17)
  - Consent for processing and/or selling of sensitive personal data: Florida (under age 18)
  - Consent for targeted advertising or sale: Delaware (under age 18)
  - Prohibition of targeted advertising or sale: Maryland (under age 18)

Several states also have online child and teen safety laws that go beyond data privacy, several of which are facing First Amendment challenges.

California's Draft Automated Decisionmaking Technology Regulations

SQUIRE PATTON BOGGS

- "'**Behavioral Advertising'** means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity—both across businesses, distinctly-branded websites, applications, or services, and within the business's own distinctly-branded websites, applications, or services. Behavioral advertising includes cross-context behavioral advertising.
  - Behavioral advertising does ***not*** include nonpersonalized advertising, provided that the consumer's personal information is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business, and is not disclosed to a third party.
- Added Term: "**Extensive profiling**" means work or educational profiling, public profiling, or profiling a consumer **for behavioral advertising.**
  - A business must conduct a risk assessment for extensive profiling
  - Thresholds revised for Pre-use Notice, Opt-Out, and Access requirements for extensive profiling
  - A business that uses physical or biological identification or profiling for extensive profiling must conduct an evaluation that it works as intended and does not discriminate and implement accuracy and nondiscrimination safeguards

Data Minimization

A controller's **collection** of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the "specified" or "disclosed" purposes.

- **California**
  - The purpose(s) for which the personal information was **collected or processed** shall be consistent with the reasonable expectations of the consumer. 11 CCR § 7002(b) (five factor test).
- **Maryland**
  - A controller shall…limit the **collection** of personal data to what is reasonably necessary and proportionate **to provide or maintain a specific product or service requested by the consumer** to whom the data pertains. § 14-4606(B)(1)(I).
  - A controller may not…unless the controller obtains the consumer's consent, **process** personal data for a purpose that is neither reasonably necessary nor compatible with the disclosed purposes for which the personal data is processed, as disclosed to the consumer. §14-4606(A)(8).

New Uses of Collected Personal Data

- A controller is not permitted to, except as otherwise provided, process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent. (CT)
- A controller may not process personal data for purposes that are not reasonably necessary for and compatible with the purposes the controller specified in the privacy notice unless the controller obtains the consumer’s consent. (OR)

Common Exempt/Permitted Uses

SQUIRE PATTON BOGGS

- Comply with federal, state, or local laws, rules, or regulations
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities
- Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local law
- Investigate, exercise, prepare for, or defend actual or anticipated legal claims
- Conduct internal research to improve, repair, or develop products, services, or technology
- Identify and repair technical errors that impair existing or intended functionality
- Perform internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller
- Provide a product or service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract
- Protect the vital interests of the consumer or of another individual
- Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, or malicious, deceptive, or illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action

Colorado AI Law & Digital Advertising

SQUIRE PATTON BOGGS

"Concerning Consumer Protections In Interactions With Artificial Intelligence Systems" (*Colorado AI Law*)

- **When is the Colorado AI Law in force?**
  Enacted May 17, 2024 and in force February 1, 2026

- **What organizations are regulated?**
  - Applies to a legal and natural person (per Colo. Rev. Stat. § 6-1-102)
  - Operating in Colorado
  - That/who is a "developer" and/or user (aka "deployer") of "High-Risk Artificial Intelligence Systems" (HAIS) [*see next slide*]

- **Who or what is a developer and deployer?**
  - a "Deployer" uses a HAIS (Colo. Rev. Stat. § 6-1-1701(6))
  - a "Developer" develops or "intentionally and substantially modifies" an "Artificial Intelligence System."

Colorado AI Law & Digital Advertising

SQUIRE PATTON BOGGS

What is a HAIS?

- *High-risk Artificial Intelligence Systems* is defined as any **Artificial Intelligence System** "that, when deployed, makes or is a **Substantial Factor** in making a **Consequential Decision**."

- *Artificial Intelligence System means* "any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions or recommendations, that can influence physical or virtual environments."

- *Substantial Factor* means a factor that (i) assists in making a Consequential Decision; (ii) is capable of altering the outcome of a Consequential Decision; and (iii) is generated by an Artificial Intelligence System (Colo. Rev. Stat. § 6-1-1701(11).)

- *Consequential Decision means* a "decision that has a material legal or similarly significant effect on the provision or denial to any Consumer [any Colorado resident] of, or the cost or terms of: (a) educational enrollment or an educational opportunity; (b) employment or an employment opportunity; (c) a financial or lending service; (d) an essential government service; (e) health-care services; (f) housing; (g) insurance; or (h) a legal service."

Colorado AI Law & Digital Advertising

SQUIRE PATTON BOGGS

A HAIS does **not** include:

- An Artificial Intelligence System that is intended to perform narrow procedural tasks or to detect a decision-making pattern or deviation from a prior decision-making pattern and does not replace or influence prior human decisions without sufficient human review (Colo. Rev. Stat. § 6-1-1701(9).)

- 17 types of common technology, as long as the outputs are not a Substantial Factor in making a Consequential Decision. These technologies are fraud detection that does not use facial recognition, anti-malware, anti-virus, video games, calculators, cybersecurity, databases, data storage, firewalls, internet domain registration, internet website loading, networking, spam and robocall filtering, spell checking, spreadsheets, web caching, web hosting, and natural language generative AI that is subject to an "acceptable use policy" prohibiting generation of content that is discriminatory or harmful.
  - The terms "discriminatory" and "harmful" are not defined.
  - *Algorithmic Discrimination* occurs when use of an artificial intelligence system results in "an unlawful differential treatment or impact that disfavors an individual or group of individuals on the basis of their actual or perceived age, color, disability, ethnicity, genetic information, limited proficiency in the English language, national origin, race, religion, reproductive health, sex, veteran status, or other classification protected under the laws of this state or federal law" (Colo. Rev. Stat. § 6-1-1701(1).)

Colorado AI Law & Digital Advertising

SQUIRE PATTON BOGGS

What obligations apply to developers and deployers?

- Developer obligations include (inter alia) (i) for High-Risk Artificial Intelligence System, exercise a duty of care to avoid algorithmic discrimination and make certain disclosures to deployers and the Attorney General, (ii) for Artificial Intelligence System, maintain records of content used to train the model, provide information for deployers about capabilities and limitations, (iii) make available information of the HAIS sufficient to conduct an impact assessment, and (iv) publish statement on Developer's website containing information about the type of HAIS and how the Developer manages known or reasonably foreseeable risks of algorithmic discrimination.
- Deployer obligations include (inter alia) disclosures to an affected consumer:
  - about use of a High-Risk Artificial Intelligence System to make a consequential decision, before the decision is made, and if the resulting decision is adverse, notification thereof along with an explanation of the degree to which the system contributed to the decision, the data processed and the sources of that data, and, excepting where "not in the best interest of the consumer" (e.g., risk of harm from delay), an opportunity to correct any personal data that may have been a substantial factor in the decision and an ability to appeal the decision, which must, if feasible, allow for human review.
  - that the consumer is interacting with an Artificial Intelligence System unless that would be obvious to a reasonable consumer.
  - whether any content provided to them was synthetically generated.

Consumers have the right to correct data used to make certain decisions and, subject to narrow exceptions, the right of appeal to a human reviewer (among other transparency rights).

Washington's My Health My Data Act

SQUIRE PATTON BOGGS

When: effective **March 31, 2024**

Applies to:

- A legal entity conducting business in Washington or targeting Washington residents, subject to processing or revenue thresholds
- Consumer health data (CHD) - "personal information that is linked or reasonably linkable to a consumer and that identifies [or infers] a consumer's past, present, or future physical or mental health"
- Consumers - WA residents and non-residents from whom CHD is collected while they are physically in WA, both categories of which "act only in an individual or household context"

Key requirements:

- Privacy Policy for CHD;
- Consent for CHD "Collection" and CHD "Sharing"
- Signed Authorization for CHD "Sale" (monetary or other valuable consideration) – not the same as consent
- Consumer rights requests
- No geofencing for tracking consumers seeking health care services, for collecting consumer health data from consumers; or for sending messages or advertisements to consumers related to their consumer health data or health care services

Private right of action - actual damages (discretionary treble damages) up to $25,000 (+ attorney's fees, costs)

Nevada's SB 370 ("NV CHD Law")

When: effective **March 31, 2024**

Applies to:

- A legal entity conducting business in Nevada or targeting Nevada residents, subject to processing or revenue thresholds
- Consumer health data (CHD) - "personally identifiable information that is linked or reasonably capable of being linkable to a consumer and that a regulated entity uses to identify the past, present, or future health status of the consumer"
- Consumers - NV residents and non-residents from whom CHD is collected while they are physically in NV, **who has requested a product or service from a regulated entity,** both categories of which "act only in an individual or household context"

Key requirements:

- Privacy Policy for CHD;
- Consent for CHD "Collection" and CHD "Sharing"
- Signed Authorization for CHD "Sale" (monetary or other valuable consideration) – not the same as consent
- Consumer rights requests
- No geofencing for tracking consumers seeking health care services (not defined), for collecting consumer health data from consumers; or for sending messages or advertisements to consumers related to their consumer health data or health care services

NO Private right of action

Policy Perspectives on Federal Lawmaking

Sausage Making Finish Line Struggles

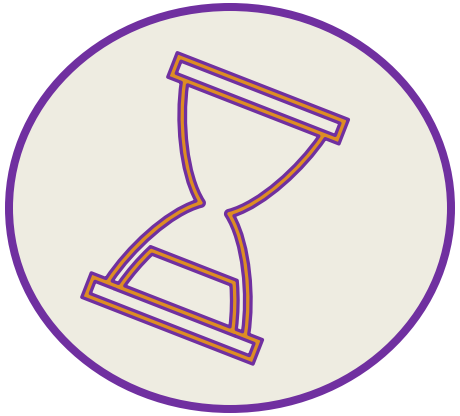
SQUIRE PATTON BOGGS

- ***Comprehensive Federal Policy May Take Years***: For more than a decade, the U.S. Congress has considered comprehensive federal data privacy legislation to fill growing gaps in the current checkerboard of federal and state data privacy rules.
- The **ADDPA** was introduced in 2022; if enacted, ADDPA would have regulated how organizations keep and use consumer data. The bipartisan, bicameral bill was the first American consumer privacy bill to pass a House committee markup, which it did with near unanimity. The bill ultimately did not advance to enactment.
- States filled the void and have enacted data privacy laws. As such, states now have preemptive concerns, believing federal privacy laws should not roll back state privacy protections.
  - The ADDPA would have largely superseded state laws, such as the *California Consumer Privacy Act.*
- With no federal data privacy law, Big Tech and data brokers continue to grapple with the patchwork of state privacy laws.

ADDPA Challenges: The Clock Runs Out …

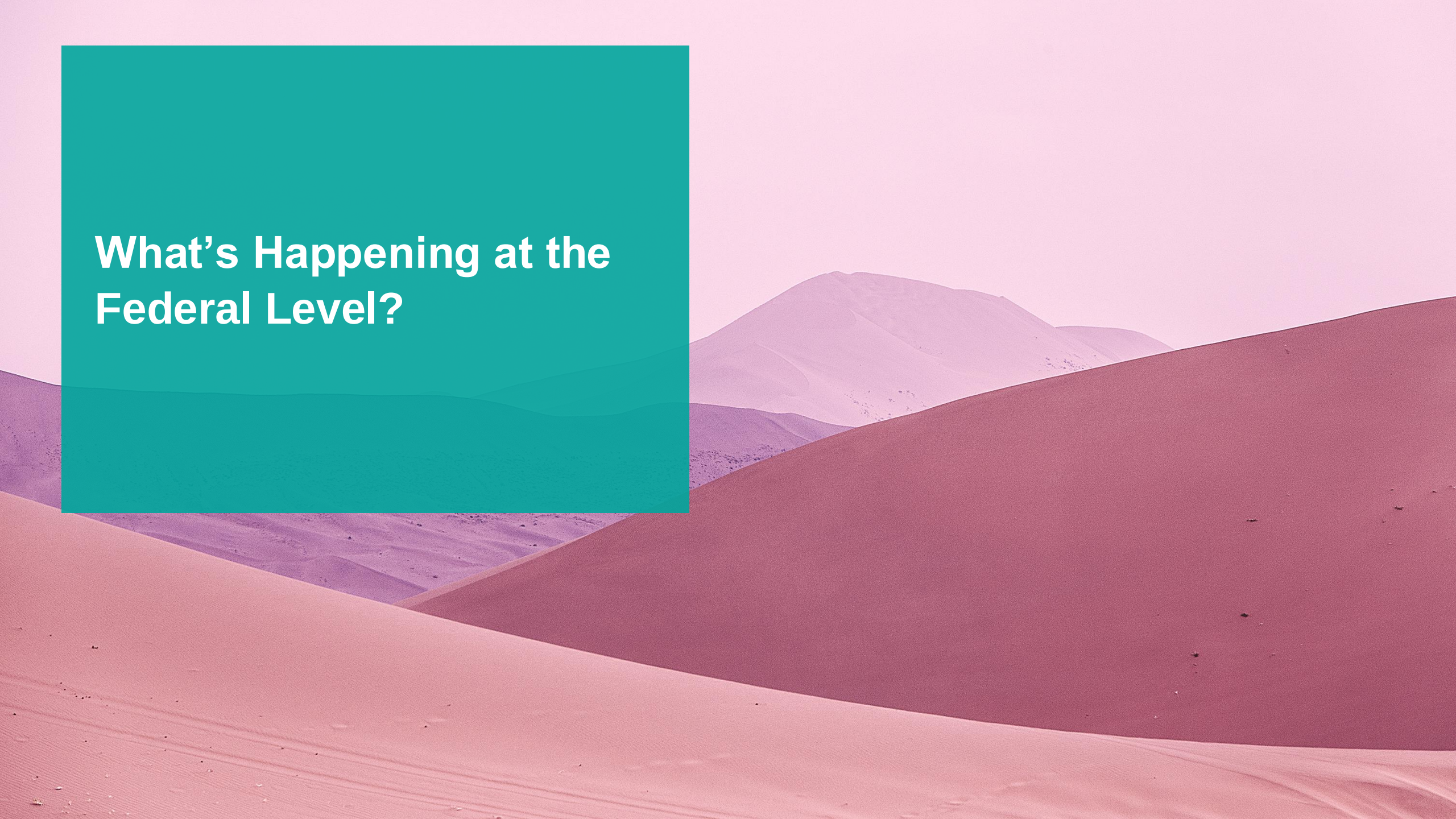
Opposition: Notably, the ADDPA faced opposition from California lawmakers, Senate Democrats, and Big Tech.

- Competing bills – Senate Commerce Committee Chair Maria Cantwell (D-WA) had her own online privacy bill in draft, and declined another bipartisan online privacy bill proposed by Senators Richard Blumenthal (D-CT) and Marsha Blackburn (R-TN).
- Cantwell's primary concern for ADPPA was its enforcement provisions. Her draft bill had also been grappling with a provision that would restrict consumers from creating class-action lawsuits against companies that had harmed them.
- Some stakeholders had also expressed concern about the ADPPA's potential effect on law enforcement efforts to investigate and solve child abduction cases.



Clock Runs Out: **The 117th Congress adjourned on January 3, 2023, and the 118th Congress saw control of the House shift to Republican control. The ADDPA was not been reintroduced in the 118th Congress but …**

What’s Happening at the Federal Level?



American Privacy Rights Act (APRA): The Clock Started

SQUIRE PATTON BOGGS

- In early April, House Energy & Commerce (E&C) Committee Chair Cathy McMorris Rodgers (R-WA) and Senate Commerce, Science, & Transportation Committee Chair Maria Cantwell (D-WA) unveiled the *American Privacy Rights Act* discussion draft (***APRA***)
  - Notably, the bill has not been formally introduced in either chamber.
- On May 23, the House E&C Subcommittee on Innovation held a markup of the APRA, a step intended to help shape the next version.
- The House is pushing to have a full E&C Committee markup of the APRA before the August congressional recess.
- Meanwhile, the Senate is further behind, so time remains for interested parties to weigh-in on the APRA in both chambers.

U.S. Congress | APRA Prospects

- In a divided U.S. Congress – where the Senate is led by a narrow Democratic majority and the House of Representatives is led by a narrow Republican majority – gridlock in Washington, D.C. is the new normal.
- APRA has bicameral, bipartisan support, with many lawmakers recognizing that to help Congress address increasing artificial intelligence (AI) concerns, a federal data privacy law is long overdue.
- After November's Election Day, the 118th Congress will commence its "lame duck" session, where wildcards – such as APRA – could possibly advance to the legislative finish line and the President's desk.

Policy Key Takeaways

- The legislative sausage making machine is neither fast, nor is it easy with 535 Members of Congress – or “CEOs” – seeking to drive the policymaking bus.
- Amid a shortened legislative calendar in an election year, APRA could advance as a standalone measure or be attached to a moving legislative package.
- The legislative vehicles to watch for any possible new data privacy legislative provisions would be either the Fiscal Year 2025 appropriations measures (12 spending bills to fund the Federal Government), or the annual *National Defense Authorization Act*.
  - Alternatively, if Congress can pull together this year on a comprehensive AI bill, APRA could also hitch a ride.
- As a reminder, you (and your clients) can also weigh-in with your congressional representatives and thereby help shape any emerging federal data privacy policy rather than wait and litigate downstream.

American Privacy Rights Act (APRA)

SQUIRE PATTON BOGGS

What data is protected?

- Protects “covered data” defined similarly to personal data in state consumer privacy laws
  - information that “identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals.” (Section 2(9)).
  - Individual is a natural person “residing” in the US but not necessarily a citizen
  - Employees are not expressly excluded but employee information is not covered data
- Personal data collected and processed in B2B context is **not** excluded
- Expansive definition of “sensitive covered data”
  - Typical, such as data that can be used for identity theft, health data, precise geolocation data, data from or about minors (under age 17) and data reflecting immutable personal physiological characteristics (i.e., biometric and genetic information, race).
  - Data generally considered private, such as recorded media intended for “private use” or reflecting a “naked or undergarment-clad private area of an individual,” data about an individual’s video access and use transferred to a third party, and data in or about “private communications” also are sensitive covered data.
  - The Federal Trade Commission (FTC) has the authority to expand the sensitive covered data definition via regulations.

American Privacy Rights Act (APRA)

SQUIRE PATTON BOGGS

What types of entities must comply?

- A covered entity determines the purposes and means of processing covered data as well as transferring covered data and a service provider processes or transfers covered data on behalf of, and at the direction of, a covered entity.
  - "transfer" meaning sale or sharing of covered data for consideration or another "commercial purpose." (Section 2(42)).
  - More obligations on service providers than current state consumer privacy laws - e.g., more prescriptive data minimization and security obligations
  - Includes data brokers as covered entities, but not service providers, that meet certain revenue thresholds
  - Includes large data holders (LDH) as covered entities and service providers with at least $250m in gross revenue and that meet certain processing or transferring thresholds that seem targeted to social media platforms
- Notably **not** exempt: "common carriers subject to title II of the Communications Act of 1934" and nonprofit organizations and are thus subject to FTC enforcement in a stark departure from the FTC's Section 5 enforcement powers. (Section 17(b)(3)).
- Does **not** contain *entity-level* exemptions for covered entities subject to existing federal privacy laws, such as for covered entities and their business associates subject to the Health Insurance Portability and Accountability Act (HIPAA) and financial institutions subject to the Gramm-Leach-Bliley Act (GLBA).

American Privacy Rights Act (APRA)

SQUIRE PATTON BOGGS

- **Targeted Advertising –** revised in in the May APRA draft as follows "displaying or presenting an advertisement to an individual or device identified by a unique persistent identifier (or to a group of individuals or devices identified by unique persistent identifiers) ~~an),~~ if the online advertisement is selected based on ~~known or predicted~~ covered data collected or inferred from the online activities of the individual over time and across websites or online services that do not share common branding, or over time on any website or online service operated by a covered high-impact social media company (but not based on a profile created about the individual), to predict the preferences of the individual or interests associated with the individual or a device identified by a unique persistent identifier …"

- **Contextual Advertising –** a new definition in the May APRA draft that means "displaying or presenting an online advertisement that (A) is **not** targeted advertising; (B) does not vary based on the identity of the individual recipient; and (C) is based solely on (i) the content of a webpage or online service; (ii) advertising or marketing content to an individual in response to a specific request of the individual for information or feedback; or (iii) the presence of an individual within a radius no smaller than 10 miles."
- **First Party Advertising & First Party Data –**new definitions in the May APRA draft

American Privacy Rights Act (APRA)

SQUIRE PATTON BOGGS

Targeted Advertising Issues

- Information collected form targeted advertising is “sensitive covered data”
- The right to opt out of covered data transfers has no exceptions and could prevent basic advertising functions like the use of service providers to assist with non-targeted ad serving, measurement and frequency capping.
- The APRA draft is unclear about whether sensitive and previously collected data could be used for purposes of targeted ads. It would prohibit companies from obtaining consent to process covered data for uses that don’t qualify as permitted purposes—unlike the data minimization and secondary use provisions in many state privacy laws.
- Section Eight’s prohibition on different prices or service levels based on exercise of rights, including refusal to give consent, is very broad. the “pay or OK” model (i.e, a consumer can choose to pay or accept targeted ads for free access).

National Security and Cross Border Transfers

February 28, 2024: new data privacy E.O. on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern.

- The U.S. Attorney General and other federal agencies are directed to prevent the large-scale transfer of Americans' personal data by **commercial data brokers** to what the White House calls "countries of concern," (e.g., China, Russia) while erecting safeguards around other activities that can give those countries access to people's sensitive data.
- The Department of Justice also is directed to issue regulations that establish protections for Americans' sensitive personal data, as well as sensitive government-related data, which includes geolocation information on sensitive government sites and members of the military.

National Security and Cross Border Transfers

SQUIRE PATTON BOGGS

- DOJ issued Advance Notice of Proposed Rulemaking (ANPRM)
  - Defines “countries of concern”
  - Focuses on six categories of sensitive personal information
  - Establishes a bulk volume threshold for the regulation of general data transactions
  - Proposes broad prohibition on data brokerage transactions and genomic data transactions
  - Contemplates restrictions on certain vendor agreements for goods and services
- DOJ’s licensing decisions would be made in collaboration with DHS, the Department of State and the Department of Commerce.
- The ANPRM contemplates exemptions for four broad categories of data:
  (1) data incidental to financial services, payment processing and regulatory compliance;
  (2) ancillary business operations within multinational US companies, such as payroll or H.R.
  (3) activities of the US government and its contractors, employees and grantees; and
  (4) transactions otherwise required or authorized by federal law or international agreements

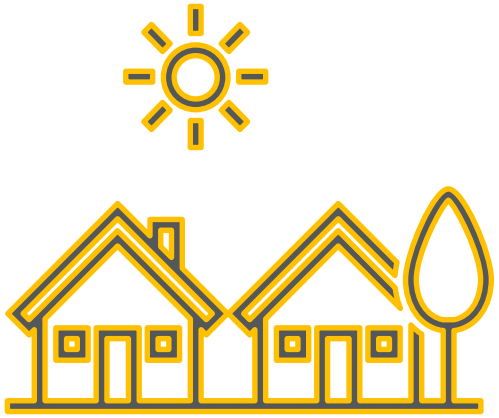
Protecting Kids Privacy Online: Old & New

COPPA 2.0 proposed February 2024

- Extend to age 13-17
- Teens manage their own consents rather than via VPC
- Broader definition of targeted advertising to children and teens
- Need direct notice for international transfers
- FTC empowered to make regulatory standards for universal consent mechanism

Kids Online Safety Act (KOSA) and Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment Act of 2023 (STOP CSAM Act)

- Common themes:
  - Privacy by default
  - Age verification
  - Additional requirements for targeted advertising



Amended KOSA Bill

SQUIRE PATTON BOGGS

- Advertising to Minors: Amended KOSA does not prohibit advertising to minors if the advertising is age-appropriate and not based on the minor's personal data. If the advertising is "aimed" at known minors, Amended KOSA includes notice and transparency requirements which require a covered platform to provide "easy-to-understand labels and information" about the advertisements (§ 104(c)(1)).
- The notice must include the name of the advertised product or service and disclosure that the content displayed is an advertisement.
- For individual-specific advertising to minors, information about why the advertisement is directed to a specific minor also is required.
  - The term "individual-specific advertising to minors" means advertising that is directed to a specific minor or a device that is linked or reasonably linkable to the minor based on personal data (including a unique device identifier) or "profiling of a minor or group of minors".
  - The term has an exclusion for contextual advertising, among others.
- The covered platform also is prohibited from facilitating alcohol, gambling and tobacco advertising to known minors.
- Many of the details are left to the FTC which is asked with issuing guidance before Amended KOSA's in-force date, making precisely how Amended KOSA will apply to targeted advertising uncertain.

Questions?

Resources

SQUIRE PATTON BOGGS

- Privacy World, “State Privacy Law Patchwork Presents Challenges” (June 10, 2024), available at https://www.privacyworld.blog/2024/06/state-privacy-law-patchwork-presents-challenges/#more-11160
- Privacy World, “All Eyes on AI: Colorado Governor Throws Down the Gauntlet on AI Regulation After Colorado General Assembly Passes the Nation’s First AI Law” (May 21, 2024), available at https://www.privacyworld.blog/2024/05/all-eyes-on-ai-colorado-governor-throws-down-the-gauntlet-on-ai-regulation-after-colorado-general-assembly-passes-the-nations-first-ai-law/
- Privacy World, “Are you Ready for Washington and Nevada’s Consumer Health Data Laws?” (April 17, 2024), available at https://www.privacyworld.blog/2024/04/are-you-ready-for-washington-and-nevadas-consumer-health-data-laws/
- Privacy World, “April’s APRA: Could Draft Privacy Legislation Blossom into Law in 2024?” (April 11, 2024), available at https://www.privacyworld.blog/2024/04/aprils-apra-could-draft-privacy-legislation-blossom-into-law-in-2024/
- Privacy World, In Narrow Vote California Moves Next Generation Privacy Regs Forward” (March 9, 2024), available at “https://www.privacyworld.blog/2024/03/in-narrow-vote-california-moves-next-generation-privacy-regs-forward/#more-10709
- Privacy World, “Protecting Kids Online: Changes in California, Connecticut and Congress – Part I” (February 27, 2024), available at https://www.privacyworld.blog/2024/02/protecting-kids-online-changes-in-california-connecticut-and-congress-part-i/
- Privacy World, “Protecting Kids Online – Part II” (February 27, 2024) available at https://www.privacyworld.blog/2024/02/protecting-kids-online-part-ii/

Global Coverage

SQUIRE PATTON BOGGS

Abu Dhabi
Atlanta
Beijing
Beirut
Berlin
Birmingham
Böblingen
Bratislava
Brussels
Cincinnati
Cleveland
Columbus
Dallas
Denver
Dubai
Dublin
Frankfurt
Hong Kong
Houston
Leeds
London
Los Angeles
Madrid
Manchester
Miami
Milan
New Jersey
New York
Palo Alto
Paris
Perth
Phoenix
Prague
San Francisco
Santo Domingo
Shanghai
Singapore
Sydney
Tampa
Tokyo
Warsaw
Washington DC

Africa
Brazil
Caribbean/Central America
India
Israel
Mexico

Office locations
Regional desks and strategic alliances