DENTONS

myna PARTNERS

SUNRISE PRIVACY

Privacy + Security Forum

OOPS All Opt-Outs! Bringing Universal Privacy Preferences to Complex Company Practices

Privacy+ Security Forum

Speakers: Bringing Universal Privacy Preferences to Complex Company Practices

Kyle W. Miller
Partner
Dentons

Dave Cohen
Director
Myna Partners

Ashley Haynes
Senior Director-
Privacy and Trust
Ericsson
Founder/CEO
Sunrise Privacy

Privacy+ Security Forum

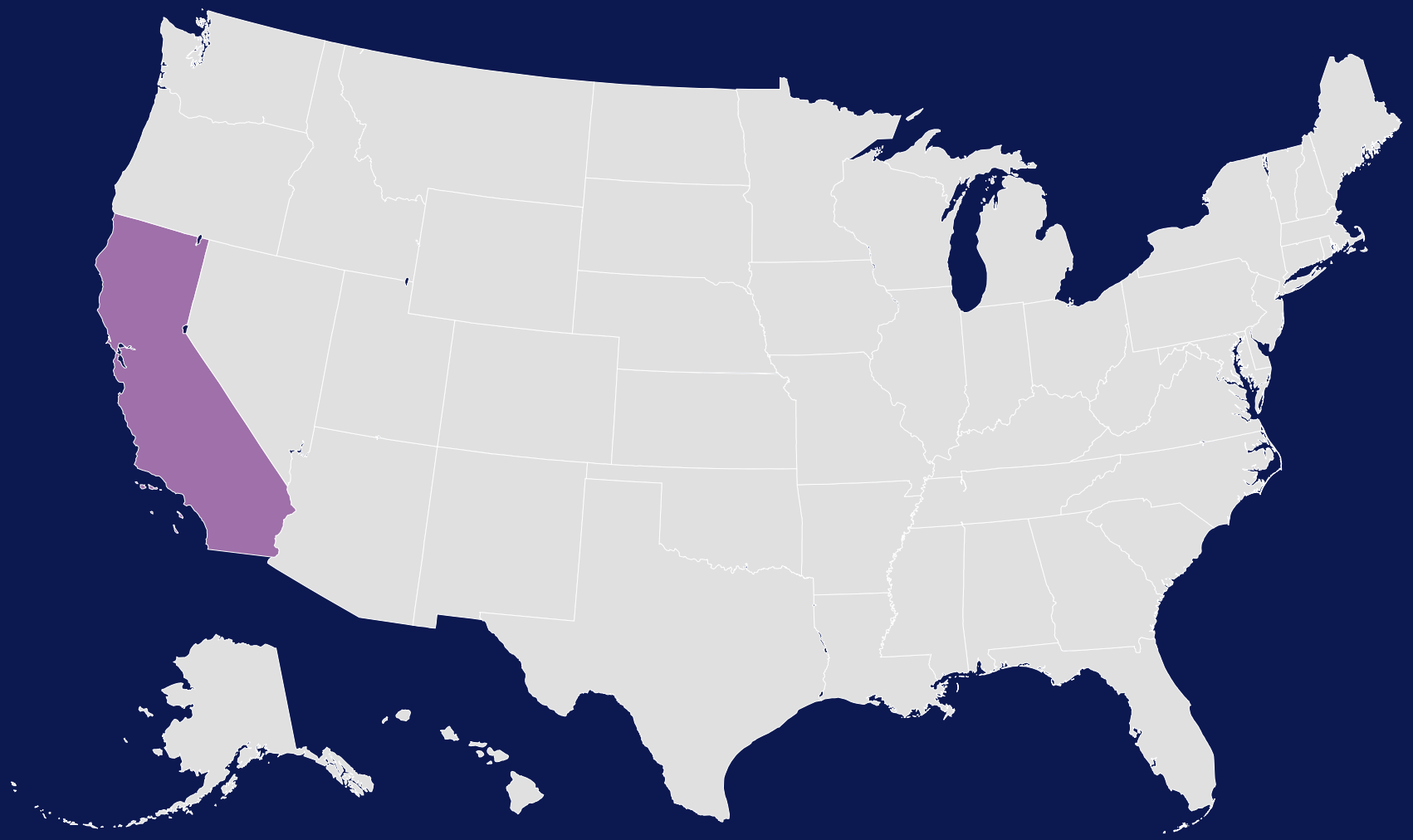
Session: Bringing Universal Privacy Preferences to Complex Company Practices

Session Agenda

- Opt-Out Frameworks
- OOPS, UOoMs, and the Global Privacy Control
- Business Obligations
- Complex Organizational Challenges
- Best Practices

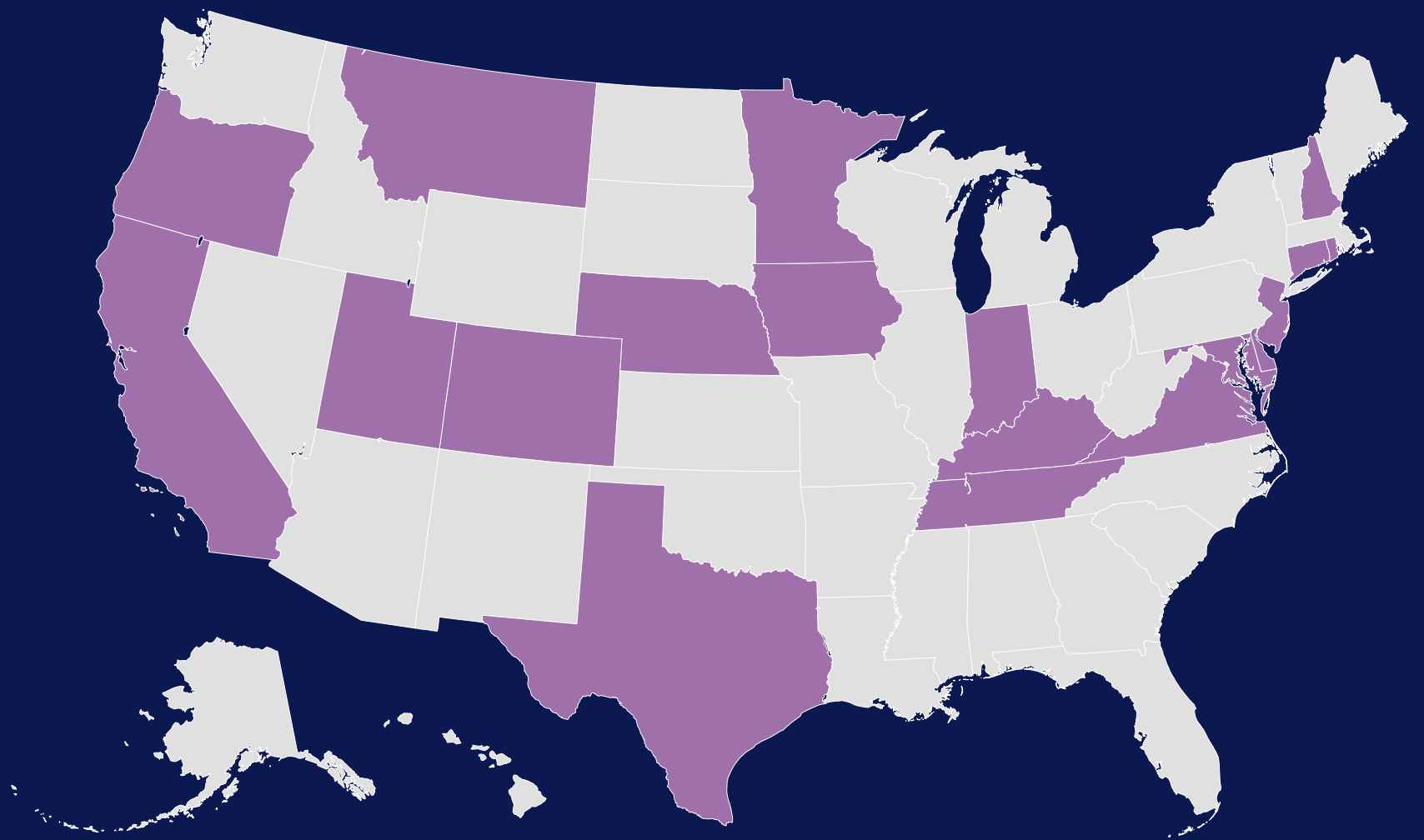
Privacy+ Security Forum

Session: Bringing Universal Privacy Preferences to Complex Company Practices



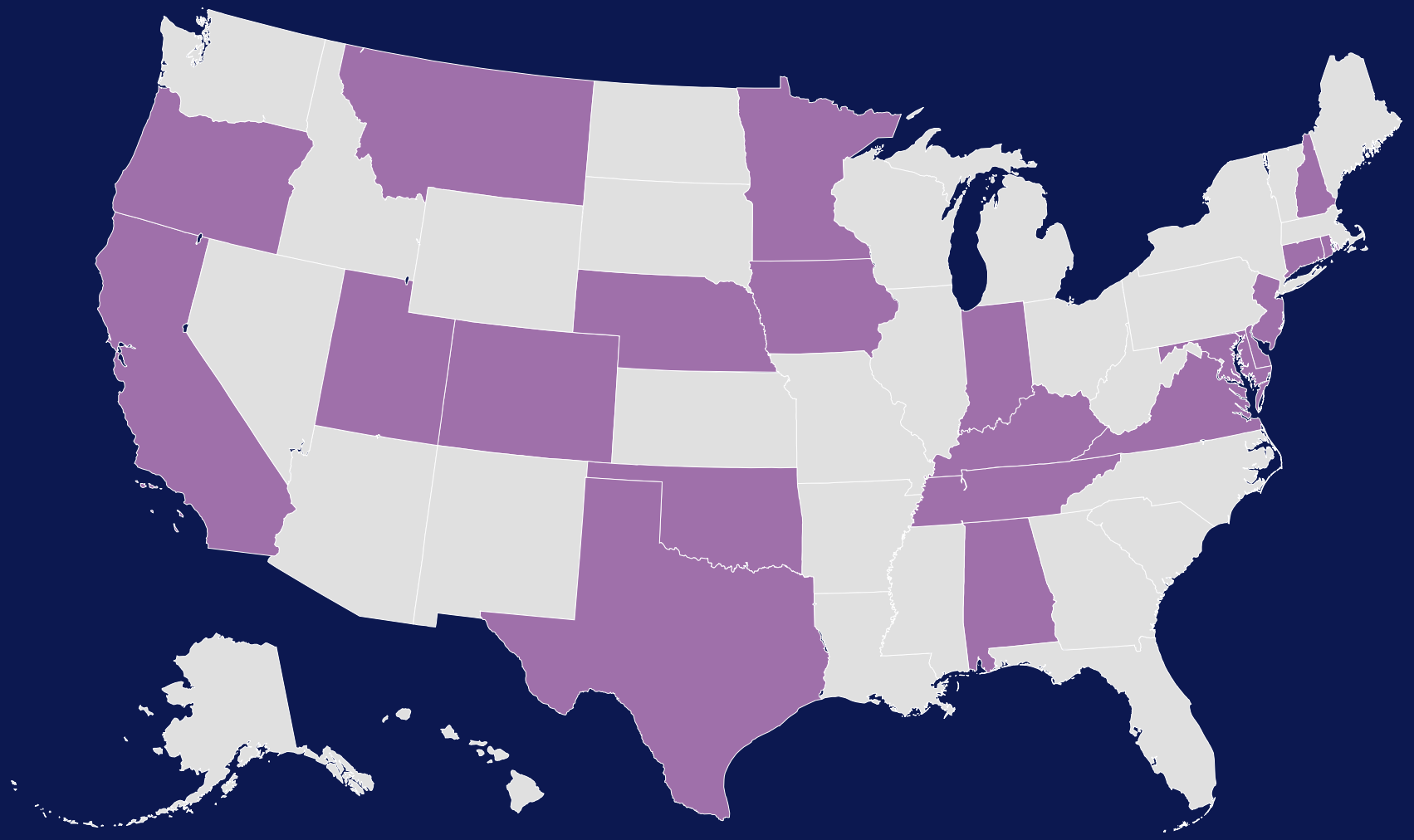
Privacy+ Security Forum

Session: Bringing Universal Privacy Preferences to Complex Company Practices



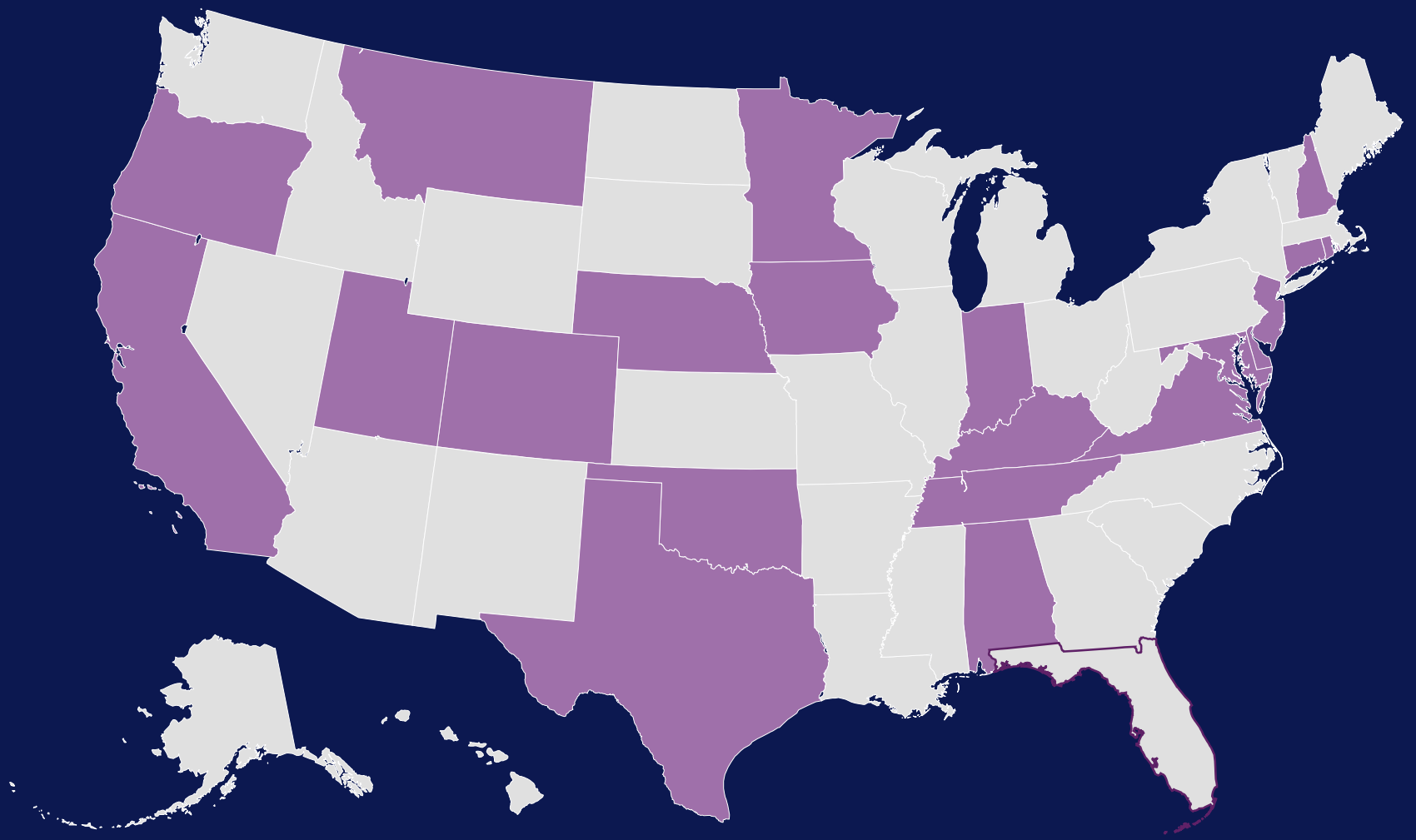
Privacy+ Security Forum

Session: Bringing Universal Privacy Preferences to Complex Company Practices



Privacy+ Security Forum

Session: Bringing Universal Privacy Preferences to Complex Company Practices



Privacy+ Security Forum

Session: Bringing Universal Privacy Preferences to Complex Company Practices

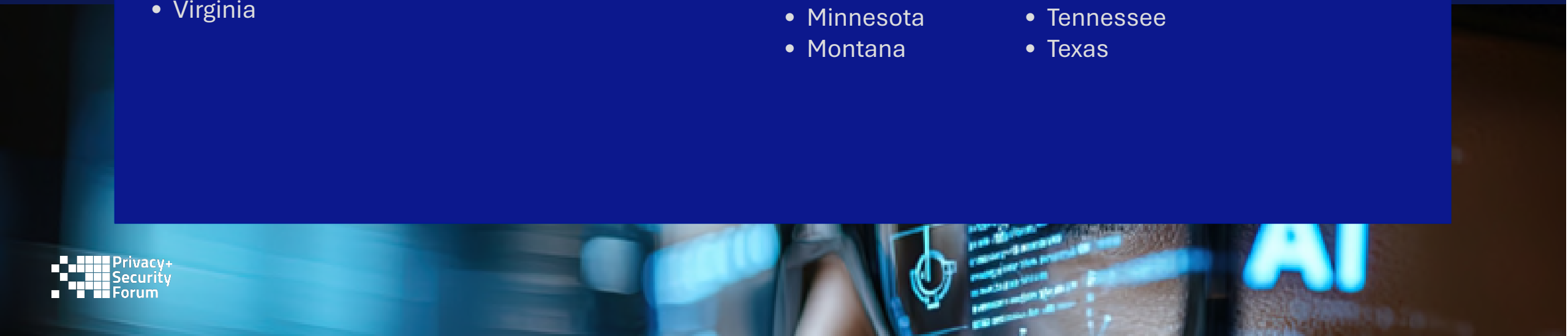
“Sale of Data”

Only Monetary Consideration

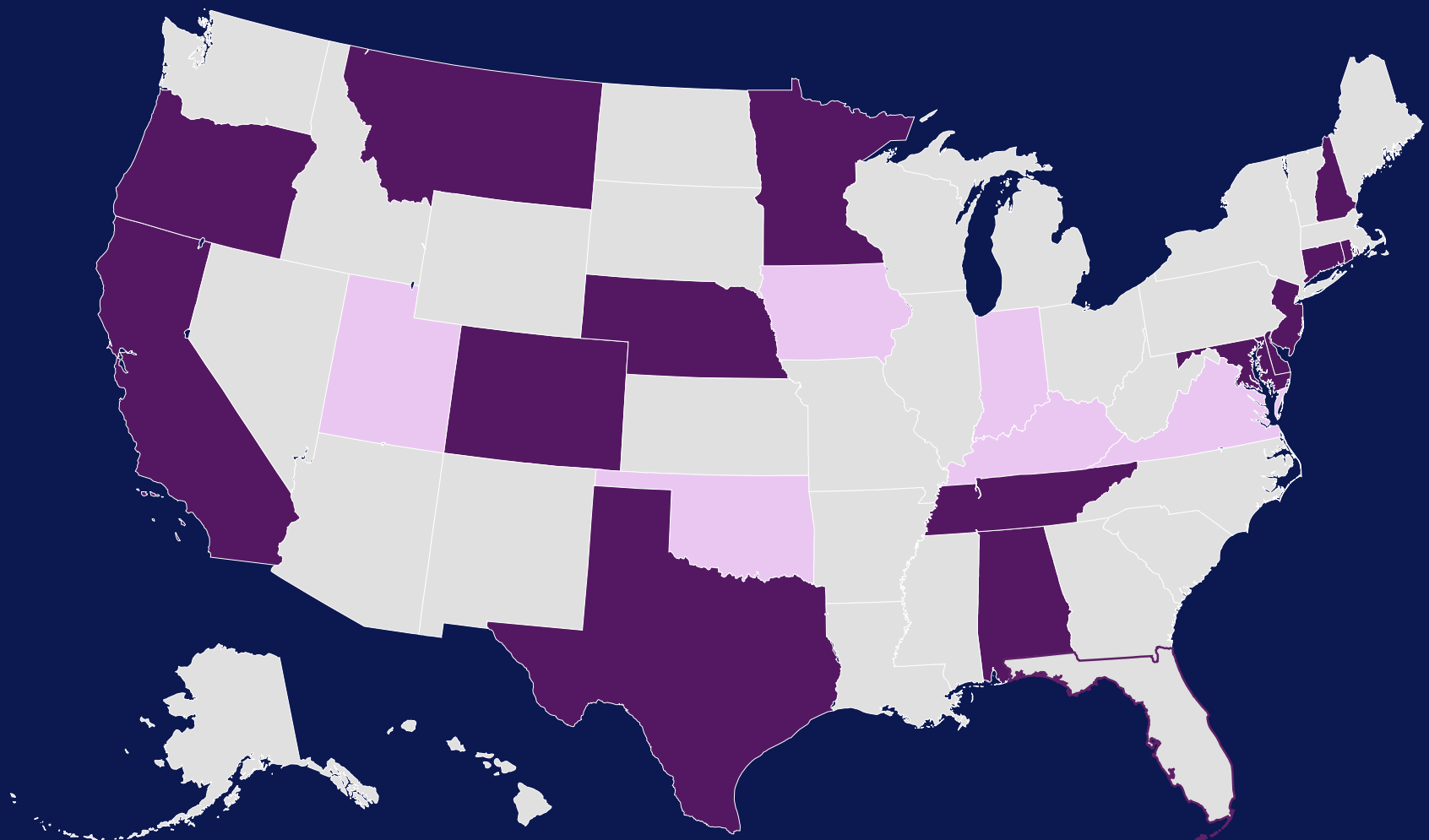
- Alabama
- Indiana
- Iowa
- Kentucky
- Utah
- Virginia

Monetary “or other valuable consideration”

- California
- Colorado
- Connecticut
- Delaware
- Maryland
- Minnesota
- Montana
- Nebraska
- New Jersey
- Oklahoma
- Oregon
- Rhode Island
- Tennessee
- Texas



Session: Bringing Universal Privacy Preferences to Complex Company Practices



Privacy+ Security Forum

Session: Bringing Universal Privacy Preferences to Complex Company Practices

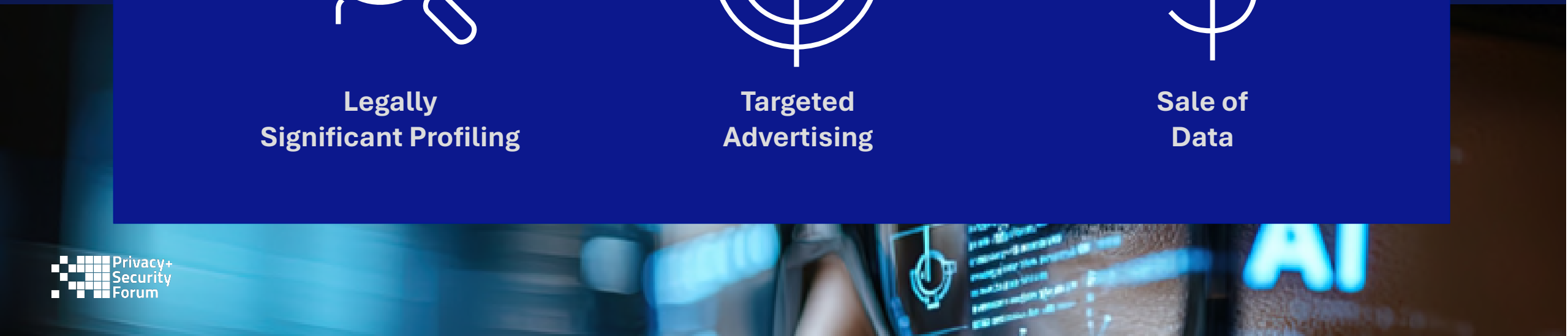
Key Responsibilities

Data Subject Rights: Data Subject Requests

Legally Significant Profiling

Targeted Advertising

Sale of Data



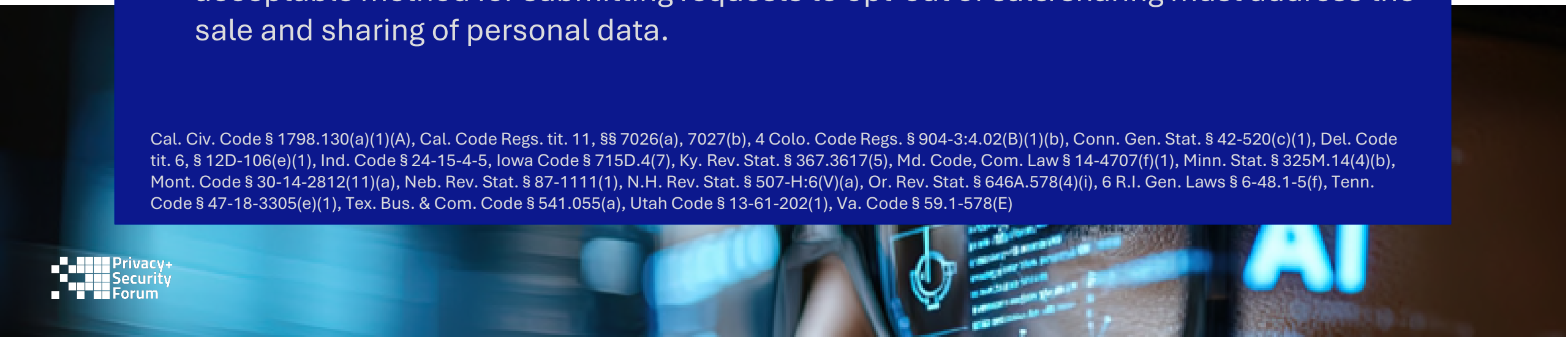
Privacy+ Security Forum

Session: Bringing Universal Privacy Preferences to Complex Company Practices

Honoring Opt-Outs

- Acceptable Data Subject Right Mechanisms include a dedicated email address, toll-free number, a digital webform, a form filled out in-person, or a form submitted through the mail.
- A cookie banner or consent management platform is not, by itself, an acceptable method for submitting requests to Opt-Out of Sale/Sharing because "cookies concern the collection of personal data and not the sale or sharing of personal data," and "an acceptable method for submitting requests to opt-out of sale/sharing must address the sale and sharing of personal data.

Cal. Civ. Code § 1798.130(a)(1)(A), Cal. Code Regs. tit. 11, §§ 7026(a), 7027(b), 4 Colo. Code Regs. § 904-3:4.02(B)(1)(b), Conn. Gen. Stat. § 42-520(c)(1), Del. Code tit. 6, § 12D-106(e)(1), Ind. Code § 24-15-4-5, Iowa Code § 715D.4(7), Ky. Rev. Stat. § 367.3617(5), Md. Code, Com. Law § 14-4707(f)(1), Minn. Stat. § 325M.14(4)(b), Mont. Code § 30-14-2812(11)(a), Neb. Rev. Stat. § 87-1111(1), N.H. Rev. Stat. § 507-H:6(V)(a), Or. Rev. Stat. § 646A.578(4)(i), 6 R.I. Gen. Laws § 6-48.1-5(f), Tenn. Code § 47-18-3305(e)(1), Tex. Bus. & Com. Code § 541.055(a), Utah Code § 13-61-202(1), Va. Code § 59.1-578(E)



Session: Bringing Universal Privacy Preferences to Complex Company Practices

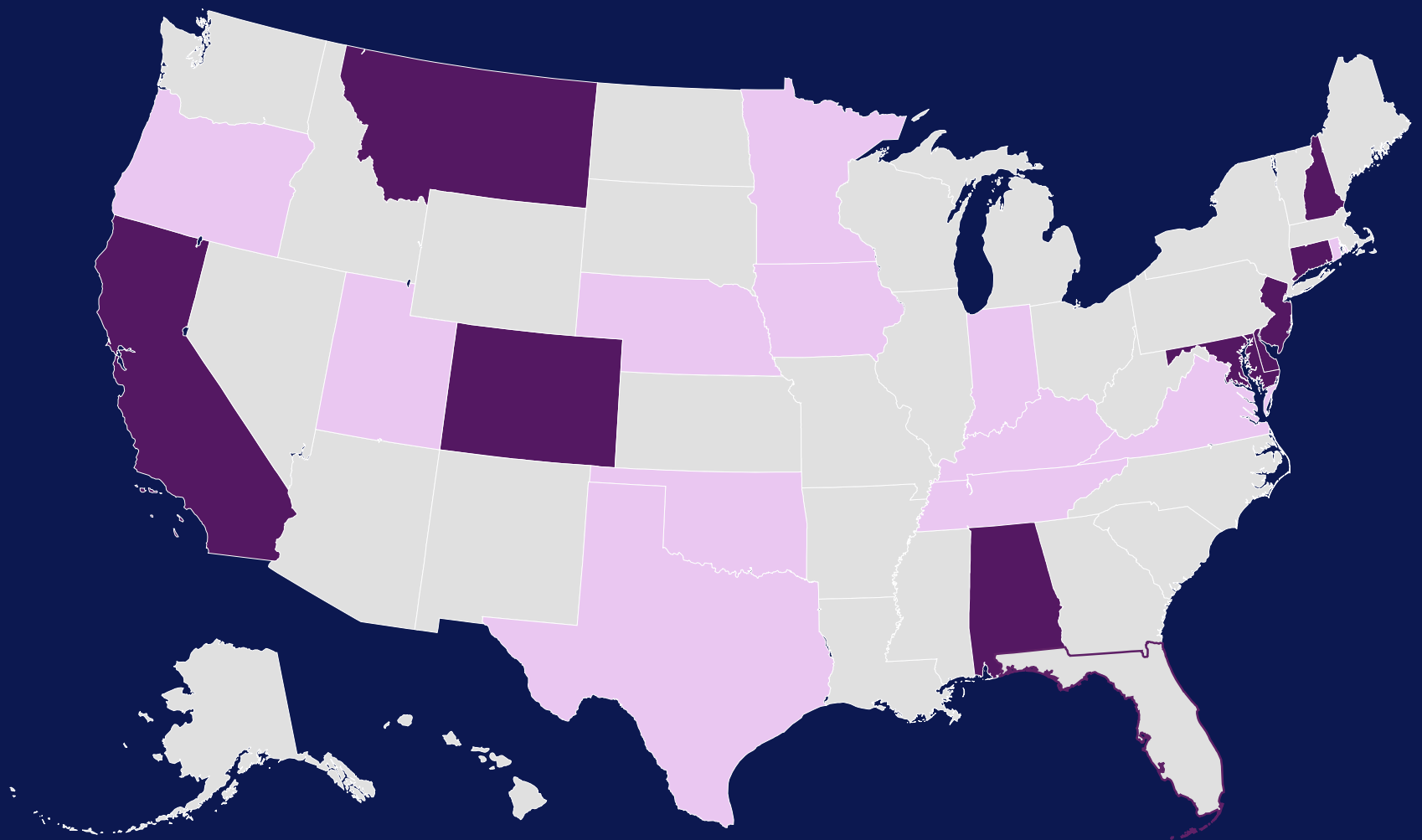
Opt- Out Signals

- Nine states require* the Controller to honor Opt-Out Preference Signals (“OOPS”) or Universal Opt Out Mechanisms (“UOoMs”).

- Md. Code, Com. Law § 14-4707(f)(3) states “A controller ***may*** utilize the following methods . . . (i) Providing a clear and conspicuous link on the controller’s website to a webpage that allows a consumer, or an authorized agent of the consumer, to opt out of the targeted advertising or the sale of the consumer’s personal data; ***or*** allowing a consumer to opt out of . . .targeted advertising, or any sale of personal data, through an opt-out preference signal. . .”

Cal. Civ. Code § 1798.135(e), Cal. Code Regs. tit. 11, § 7025(a), Colo. Rev. Stat. § 6-1-1313, 4 Colo. Code Regs. § 904-3:5.02, Conn. Gen. Stat. § 42-520(c)(1)(A)(ii); Del. Code tit. 6, § 12D-106(e)(1)(a)(2), Md. Code, Com. Law § 14-4707(f)(3), Minn. Stat. § 325M.14(32)(d), Mont. Code § 30-14-2809(c), N.H. Rev. Stat. § 507-H:6(V)(a)(1)(B), N.J. Stat. § 56:8-166.11(b).

Session: Bringing Universal Privacy Preferences to Complex Company Practices



Privacy+ Security Forum

Session: Bringing Universal Privacy Preferences to Complex Company Practices

What is the Global Privacy Control?

The GPC is a browser-level signal that automatically tells websites a consumer visits, "Do not sell or share my personal information."

How It Works

User enables GPC in their browser or installs an extension. On each page load, the browser transmits the signal automatically — no per-site action required.

Multistate Recognition

Connecticut Attorney General, California Attorney General, New Jersey Division of Data Subject Affairs, and CalPrivacy have officially endorsed the GPC as an acceptable OOPS, while the Colorado Attorney General has approved it as a valid OOPS.

Codification

Cal. Civ. Code § 1798.135(e), Cal. Code Regs. tit. 11, § 7025(a), Colo. Rev. Stat. § 6-1-1313, 4 Colo. Code Regs. § 904-3:5.02, Conn. Gen. Stat. § 42-520(c)(1)(A)(ii); Del. Code tit. 6, § 12D-106(e)(1)(a)(2), Md. Code, Com. Law § 14-4707(f)(3), Minn. Stat. § 325M.14(32)(d), Mont. Code § 30-14-2809(c), N.H. Rev. Stat. § 507-H:6(V)(a)(1)(B), N.J. Stat. § 56:8-166.11(b).

Consumer Adoption

GPC does not require a separate opt-out on each website visited. A single toggle sets the user's opt-out across covered sites. Turning it off is not an opt-in.

Session: Bringing Universal Privacy Preferences to Complex Company Practices

Organizational Challenges

Multi-Brand Structures

A single corporate parent may operate multiple consumer-facing brands. Each brand may have separate technical stacks yet share consumer identity. Opt-out must be honored across all brands using the same consumer account.

Multi-Device Complexity

Consumers access services on web browsers, iOS, Android, smart TVs, streaming sticks (Roku, Fire TV, Apple TV). Each platform has different ad SDK integrations. The same consumer signal must reach all of them — including platforms where the vendor has not built an in-app opt-out hook.

Third-Party Ad-Tech Passthrough

Embedded SDKs and server-to-server APIs automatically transmit data to ad-tech partners. The business must instruct these partners to honor the opt-out AND verify they do so. Vendor contracts must include CCPA-required service provider or contractor restrictions. Vendor limitations are not a legal defense.

"Technological Limitation" Defense – Rejected

Media company claimed vendor/tech limitations prevented a comprehensive identity-based opt-out. The AG's position: if you built the tech to link devices for advertising, you must use it to link devices for opt-outs. Technology investment excuses are not acceptable where the capability demonstrably exists.

Privacy+ Security Forum

Session: Bringing Universal Privacy Preferences to Complex Company Practices

Building a Robust GPC Compliance Program

1. Map Your Data Flows

Inventory every pixel, SDK, and API integration that transmits personal information. Identify which of these receive GPC signals and which do not.

2. Implement Account-Level Opt-Out Logic

When a logged-in consumer sends a GPC signal on any device or service, propagate that preference to all devices and services associated with their account — not just the current session.

3. Build In-App Opt-Out Across All Platforms

Do not redirect mobile app users to a web form that has no effect on that app's data flows. Each platform where data is collected needs a functioning opt-out mechanism.

4. Update Vendor Contracts and Verify Compliance

Ensure service provider and contractor agreements prohibit further selling/sharing. Include audit rights. Actively verify that vendors honor opt-out signals passed downstream.

5. Don't Silo Compliance by Opt-Out Method

A single opt-out channel (webform, toggle, or GPC) must stop ALL selling and sharing. These mechanisms should be integrated, not independent silos that each cover only part of the business.

6. Log, Test, and Audit Regularly

Maintain records of opt-out requests and effectuation. Conduct periodic technical testing to confirm the signal is actually stopping data transmission — not just setting a flag.

Session: Bringing Universal Privacy Preferences to Complex Company Practices

Key Takeaways

- GPC is a legally valid opt-out under and is persistent (not session-only), subject to device/browser and identity-linking rules.
- Known consumers get account-wide opt-out protection; one signal must propagate to all linked devices and services.
- If you built the infrastructure to link devices for ads, regulators expect it to link devices for opt-outs.
- Vendor limitations are not a defense; businesses are responsible for their ad-tech partners' reception and honoring of opt-out signals.
- Both Regulatory and Litigation exposure: Deceptive labeling of a non-functional opt-out mechanism increases litigation risk.

Privacy+ Security Forum

Session: Bringing Universal Privacy Preferences to Complex Company Practices

Questions?

Privacy+ Security Forum

Stay in touch: Continue the conversation with us

Kyle W. Miller
Dentons
kyle.miller@
dentons.com

Dave Cohen
Myna Partners
dave.cohen@
myna.com

Ashley Haynes
Ericsson/Sunrise
Privacy Consulting
ashley@
sunriseprivacy.com

Privacy+ Security Forum