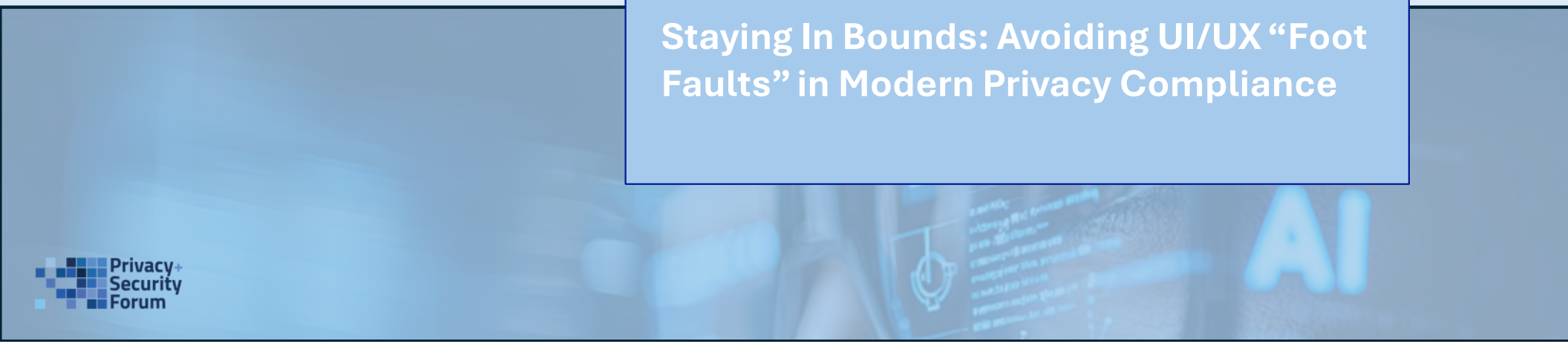
Privacy + Security Forum

Session:

Staying In Bounds: Avoiding UI/UX “Foot Faults” in Modern Privacy Compliance



Privacy+ Security Forum

Speakers: Session Title

Paul Sarkis
Associate General Counsel
Associated Press

Mallory Acheson
Partner
Nelson Mullins

Daniel Lumm
Partner
Nelson Mullins

Privacy+ Security Forum

TODAY'S AGENDA

01

The Compliance Shift

From privacy policies to prescriptive technical standards

02

Enforcement in Focus

Disney, Sephora, Healthline & what regulators are targeting

03

Common Foot Faults

Links, banners, dark patterns, GPC signals & classification

04

Your Practical Playbook

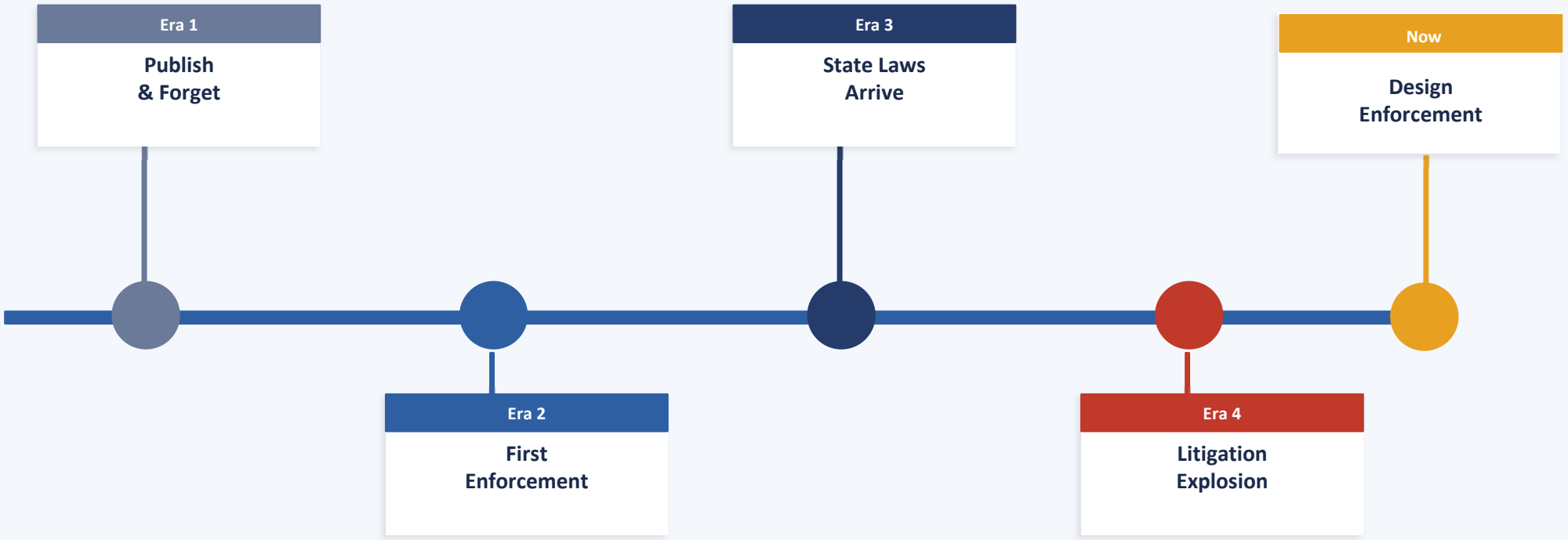
Know your teams, vendors, DPAs & risk assessments

PART 01

The Compliance Shift

How U.S. privacy enforcement evolved from policies to prescriptive technical standards

THE COMPLIANCE EVOLUTION



Key shift: Regulators moved from targeting bad actors → bad designs, bad implementation, bad transparency

THE LITIGATION REALITY: CIPA, VPPA & WIRETAPPING CLAIMS

What's Happening

- Dedicated plaintiffs' firms sending hundreds of demands weekly
- Allegations: cookies, pixels & tracking technologies used without prior consent
- Split court decisions — theories that many expected courts to reject are surviving
- Years of quick settlements fueling continued litigation
- Cookie banners don't end the exposure — they create new theories

If You Added a Cookie Banner...

You may now face new claims around:

- How the banner itself functions
- Cookie classification accuracy ("strictly necessary" vs. advertising)
- Dark patterns violating State Privacy Laws & UDAP
- What "optional" truly means in your consent language

The U.S. is catching up fast — martech and adtech compliance is now a top-tier risk for every company.

PART 02

Enforcement in Focus

Disney · Sephora · Healthline — what regulators are really looking for

CASE STUDY: SEPHORA — GPC Signals Are Legally Binding

What Happened

Sephora failed to treat the Global Privacy Control (GPC) signal as a valid opt-out of sale or sharing of personal data for advertising.

This case established a baseline expectation that still catches companies off guard today.

States Treating GPC as a Valid Opt-Out:

- ✓ California — Ignoring GPC = same as ignoring a direct opt-out request
- ✓ Colorado — Ignoring GPC = same as ignoring a direct opt-out request
- ✓ Connecticut — Ignoring GPC = same as ignoring a direct opt-out request

The Takeaway

Recognizing GPC is no longer optional.

Browser-based signals are not preferences — they are legally binding choices.

Cookie banners and preference centers can't just collect choices — they have to listen to the browser itself.

New CCPA regulations also require a notification informing consumers that their GPC signal was recognized and honored.

CASE STUDY: HEALTHLINE MEDIA — Contextual Sensitivity & Sensitive Data

What Happened

- Health-related search terms shared with ad-tech partners via tracking pixels
- No explicit, affirmative consent obtained
- Regulators focused on the nature of the data — not just the technology

The Risk Multiplier

- Tracking technologies on sensitive pages carry exponentially higher risk
- The same pixel tolerated on a retail homepage may be unlawful on a health article
- Sensitive contexts: health, children's content, financial information

What's Required

- Implied consent is not enough in sensitive contexts
- Clear, opt-in consent required before any data flows to third parties
- Backend behavior must match disclosures and promises

Where enforcement is heading: contextual sensitivity is the next frontier of cookie compliance.

CASE STUDY: DISNEY — Cross-Device Identity & Consent

$2.5M+

California AG Fine

The Key Lesson

Regulators apply a single-user lens — not a single-platform lens.

If you can recognize a user across devices for advertising or analytics, you must recognize them across devices for privacy choices. You cannot silo consent and opt-outs when your data architecture is not siloed.

Technical platform silos are not a legal defense.

PART 03

Common Foot Faults

The small, often unintentional missteps driving disproportionate enforcement & litigation risk

FOOT FAULT #1: BROKEN LINKS & NON-FUNCTIONAL BANNERS

What Regulators & Plaintiffs Look For:

Buried 'Do Not Sell or Share' link

If it's hard to find, regulators may treat it as not providing the right at all

Broken or looping opt-out links

Links that resolve to placeholders or loop back without honoring requests = regulatory failure

Non-functional 'Reject All' buttons

One of the most prevalent arguments in current CIPA/wiretapping demands

Broken banner consent choices

If 'I clicked Reject' but tracking still fires, this is a direct enforcement finding

Audit Checklist

- ☐ Click every opt-out link — does it work?
- ☐ Test banner 'Reject All' — does tracking stop?
- ☐ Verify opt-out requests are honored end-to-end
- ☐ Test in multiple browsers & devices
- ☐ Audit after every tech stack change
- ☐ Document your testing — dates & results

FOOT FAULT #2: DARK PATTERNS — Design Choices Are Now Legal Choices

Pre-Toggled 'Accept'

Consent that defaults to 'on' is not freely given

Extra Clicks to Reject

Opting out must not be harder than opting in

Misleading Button Labels

'Accept All' prominent; 'Reject All' hidden or relabeled

False Functionality Warnings

Implying the site won't work if users decline non-essential cookies

X-Out Without Decision = Consent

Allowing users to dismiss without choosing and counting that as consent is a regulatory red flag

Asymmetric Disclosure

If opt-out is harder than opt-in, or disclosures don't match data flows, that gap is a heightened AG inquiry risk

Even if the underlying tracking is lawful, a coercive interface can render consent invalid. Design choices are legal choices.

FOOT FAULT #3: COOKIE MISCLASSIFICATION — 'We Don't Use Targeted Advertising'

"We don't use any cookies or targeted advertising." — Often said by lawyers and marketing folks whose site fires 80+ cookies on the homepage.

1

Regulators Are Clear

Targeted advertising technologies require a right to opt out. This is settled guidance — not ambiguous.

2

Mislabeling is a Misrepresentation

Calling a cookie 'functional' or 'analytics' when it supports cross-context advertising is a factual misrepresentation. Plaintiffs and regulators can test this easily with technical teams and browser developer tools.

3

Outdated Cookie Scans

New cookies appear through tag updates, A/B testing, or vendor changes. If those cookies aren't disclosed or controlled, you're exposed even if the banner looks compliant.

4

'Optional' vs. 'Strictly Necessary' — A Live Litigation Theory

'Reject All Optional' buttons are a key theory in current demands. What did 'optional' mean? What data sharing applies to 'non-optional'? Even accessibility cookies can carry permissions beyond expected use.

FOOT FAULT #4: GPC BLIND SPOTS & THE 12-MONTH RE-SOLICITATION RULE

GPC Signal Blind Spots

Teams test the banner on first load — but not after a GPC signal fires.

Common failures to test:

- Does the banner still ask for consent after GPC fires?
- Does it silently override preferences?
- Does it show 'accepted' when it shouldn't?

New CCPA regulations also require a banner or notification confirming to the consumer that their GPC signal was recognized and honored — not just silent compliance.

The 12-Month Re-Solicitation Rule

Under CCPA, once a consumer opts out of sale or sharing, you generally must wait 12 months before asking them to opt back in.

Practical challenges include:

- Opt-outs via GPC from anonymous visitors not tied to an account
- Offline opt-outs that don't sync to digital systems
- Cross-device consent reconciliation

Withdrawal of Consent:

Consent must be as easy to withdraw as it is to give.

If withdrawal doesn't actually stop backend tracking, that's a classic enforcement finding.

FOOT FAULT #5: CONSUMER REQUEST PROCESS — Timelines, Verification & Shine the Light

Key Requirements & Common Failures

Response Timelines

CCPA: 45 days (extendable 45 more with notice). Many companies miss these — especially for requests submitted through non-standard channels like email or web form.

Verification Requirements

Too little verification = data breach risk. Too much = a functional denial of rights. Regulators have flagged overly burdensome verification as a de facto refusal to honor requests.

Authorized Agent Requests

Consumers can designate agents to submit requests. Companies cannot ignore these — and cannot impose requirements that make agent requests effectively impossible.

Non-Discrimination

Denying service or charging more to users who exercise privacy rights is prohibited — even subtly.

⚠ Shine the Light: A Live Litigation Tool

California's Shine the Light law (Cal. Civ. Code § 1798.83) requires businesses to disclose third-party marketing data sharing upon request.

Plaintiffs' firms are now sending mass Shine the Light requests

Public Settlements: Consumer Request Failures

Todd Snyder (CA AG, 2024)
$345K — failed to provide consumers with a functional mechanism to opt out of the sale or sharing and did not honor opt-out requests that were submitted.

DoorDash (CA AG, 2024)
$375K — shared customer data without required disclosures; deficient consumer rights processes

Tilting Point (CA AG, 2024)
$500K — collected children's data; failed to honor deletion requests in children's privacy context

FOOT FAULT #6: PRIVACY POLICY & LINK PLACEMENT — The Fine Print of Where and How

State privacy laws are highly prescriptive about where links must appear and how notices must be displayed. These aren't suggestions — they are statutory requirements regulators are actively testing.

"Do Not Sell or Share" Link Placement

- Must appear in your website footer
- Must be "clear and conspicuous" — not buried in a list of 20+ links in tiny font
- Mobile apps: must appear in the app's privacy settings or settings menu
- CCPA also permits a single link titled "Your Privacy Choices" with the opt-out icon

Opt-Out Link: Specific Naming Requirements

- CCPA: required link text is "Do Not Sell or Share My Personal Information"
- Some states permit a universal "Privacy Choices" link that must conspicuously lead to opt-out options
- Link cannot be the same color/size as surrounding legal links — must stand out visually

Privacy Policy: Placement & Accessibility

- Must be accessible from a "conspicuous link" on your homepage and at every point where personal information is collected
- At checkout, account creation, and data-collection form
- California-specific: must include a designated section for CA residents with all CCPA-required disclosures
- Must be written in plain language and be as readable as the rest of the site

"Limit the Use of My Sensitive Personal Information"

- CCPA (as amended by CPRA) requires a separate link for sensitive data if you use it beyond permitted purposes
- Can be combined with the DNSS link but must be clearly labeled
- Failure to include this link when required is its own separate violation

FOOT FAULT #7: ADDITIONAL PITFALLS REGULATORS & PLAINTIFFS ARE TARGETING

Third-Party Scripts Without Oversight

Many companies load third-party tags via tag managers without legal review. A vendor's script update can silently introduce new tracking.

Children's Data & Mixed Audiences

If your site could be visited by children under 13, COPPA applies. Several states (CA, TX, FL) have additional laws for minors under 17.

Email & SMS Marketing Consent Drift

Consent obtained years ago may not satisfy current requirements. Purchased lists, event sign-up forms, and legacy opt-ins are common liability sources.

Pixel Firing Before Consent ("Pre-consent Leakage")

Analytics and advertising pixels that load on page render — before the user interacts with a consent banner — are a direct enforcement target. Regulators and Plaintiffs have used screenshots and HAR files to document this. Consent must precede data collection, not follow it.

Stale or Inconsistent Privacy Policies

A policy last updated in 2021 that doesn't reflect current data practices, new vendors, or new state laws is both a legal exposure and a regulatory red flag.

No Process for Sensitive Data or De-identification Claims

Companies claiming data is 'de-identified' must meet technical and contractual standards. Many do not.

PART 04

Your Practical Playbook

What legal teams should prioritize — teams, vendors, DPAs & risk assessments

PRACTICAL PLAYBOOK: What Legal Teams Should Prioritize

1. Know Your Teams & Their Tools

Marketing, product, analytics, and IT often deploy tools independently. Questionnaires and internal audits are critical — surface what's actually in use, not what legal thinks is in use.

2. Know Your Terms & Your Vendors

Many cookies collect more than teams expect, and many vendors share data onward. If disclosures say one thing but vendor contracts allow another, regulators will ask for those contracts.

3. Data Processing Agreements (DPAs) Matter

DPAs aren't just paperwork. They're often the difference between a 'service provider' and a 'sale or sharing' finding. Use service provider DPAs wherever possible.

4. Document Your Risk Assessments

Regulators increasingly expect documented risk assessments — CCPA's updated regulations specifically address this.

KEY TAKEAWAYS

The Bottom Line

1. Regulators are looking for bad design, not just bad actors
2. Cookie compliance is an enforcement priority — not a technical afterthought
3. If you know a user for advertising, you may need to know them for consent
4. GPC signals are legally binding opt-outs, not preferences
5. Design choices are legal choices — dark patterns invalidate consent
6. Audit early, audit often — and document everything

Each company is different. Each use case is different. Risk tolerance is different.

Questions?

Speakers: Session Title

Paul Sarkis
Associate General Counsel
Associated Press

Mallory Acheson
Partner
Nelson Mullins

Daniel Lumm
Partner
Nelson Mullins

Privacy+ Security Forum