iapp + feroot

Findings from the field: Consent audits reveal top five CMP policy gaps and root causes

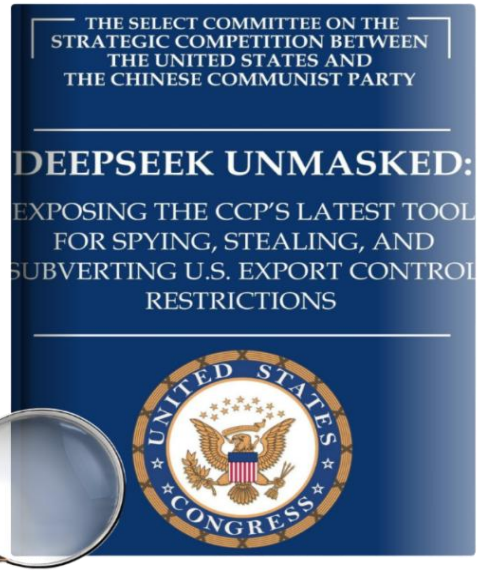
Tuesday, 8 September
08:00-09:00 PDT
11:00-12:00 EDT
17:00-18:00 CEST

Agenda

1. Introduction & Speaker Background
2. Consent Management Landscape Confidence & Failures: Learnings From Our June IAPP Webinar
3. Findings From Our Real-World Assessments
4. Competencies Organizations Need to Avoid Litigation
5. Next Steps/Audience Q&A

Today's Speaker: Ivan Tsarynny, CEO Feroot

- TikTok collects large amounts of U.S. personal data – even from people who don't use the app.
- DeepSeek's web login page connects directly to China Mobile.
- Healthcare websites leak sensitive patient data to big tech like Google, Facebook, TikTok and more.



Feroot cited in a U.S. Congress report exposing DeepSeek's link to the Chinese Communist Party, raising concerns about potential foreign access to Americans' private information.

Moreover, cybersecurity researchers at Feroot Security uncovered hardcoded links in DeepSeek's web login page that directly connect it to China Mobile,[17] a state-owned telecommunications company also designated as a Chinese military company by the U.S. Department of Defense, as mentioned.[18] China Mobile is explicitly tasked by the CCP with supporting China's broader information control and intelligence objectives.[19] While the extent of data transmission remains unconfirmed, DeepSeek's integration with China Mobile infrastructure raises serious concerns about potential foreign access to Americans' private information.

Recent publications:

- Feroot on New York Times
- Feroot on Forbes
- Feroot on Fortune
- Feroot on ABC Good Morning America
- Feroot U.S. Congressional Testimony
- Feroot on Wall Street Journal
- Feroot on Associated Press
- Feroot on CNBC
- Feroot on ABC News
- Feroot on Bloomberg

Consent Management Platform (CMP) Landscape: Confidence & Failures

What happens after users make a consent choice?

A Consent Management Platform (CMP) is more than just a technology solution; it is a combination of technology, governance, legal requirements, business processes, and user experience controls designed to collect, manage, enforce, and demonstrate user consent preferences across digital channels.

About the Research

Censuswide conducted this study independently on behalf of Feroot Security in May 2026, surveying 800 privacy, legal, marketing, and IT professionals across four countries and five industries.

800+
Respondents
Privacy, Legal, Marketing & IT

4
Countries
US · UK · Canada · Australia

5
Industries
Financial Services, Healthcare, Retail, Technology, Media

Mid–Large
Enterprise Focus
Mid-size to large organizations

WHAT WE'LL COVER

1 Third-Party Script Landscape

2 CMP Confidence & Failures

3 Vendor Governance & Accountability

4 Regulatory Enforcement Reality

5 Resources, Maturity & Investment Outlook

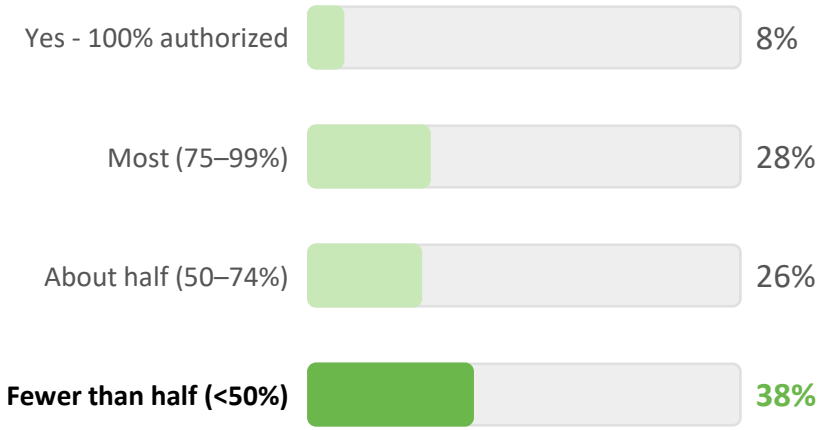
How Many Vendor Scripts Are Running on Your Websites?

The websites of nearly every organization surveyed - 99.4% - run at least one third-party script.
The median operating environment is 11 to 50 scripts running simultaneously.

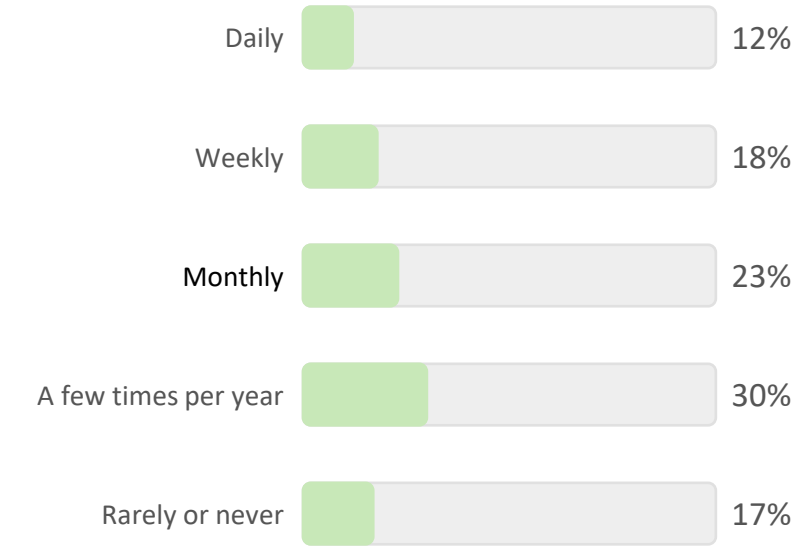
Source: Censuswide / Feroot Security - Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

Script Authorization & Unauthorized Discovery

Are all scripts on your website fully authorized?



How often are unauthorized scripts discovered?

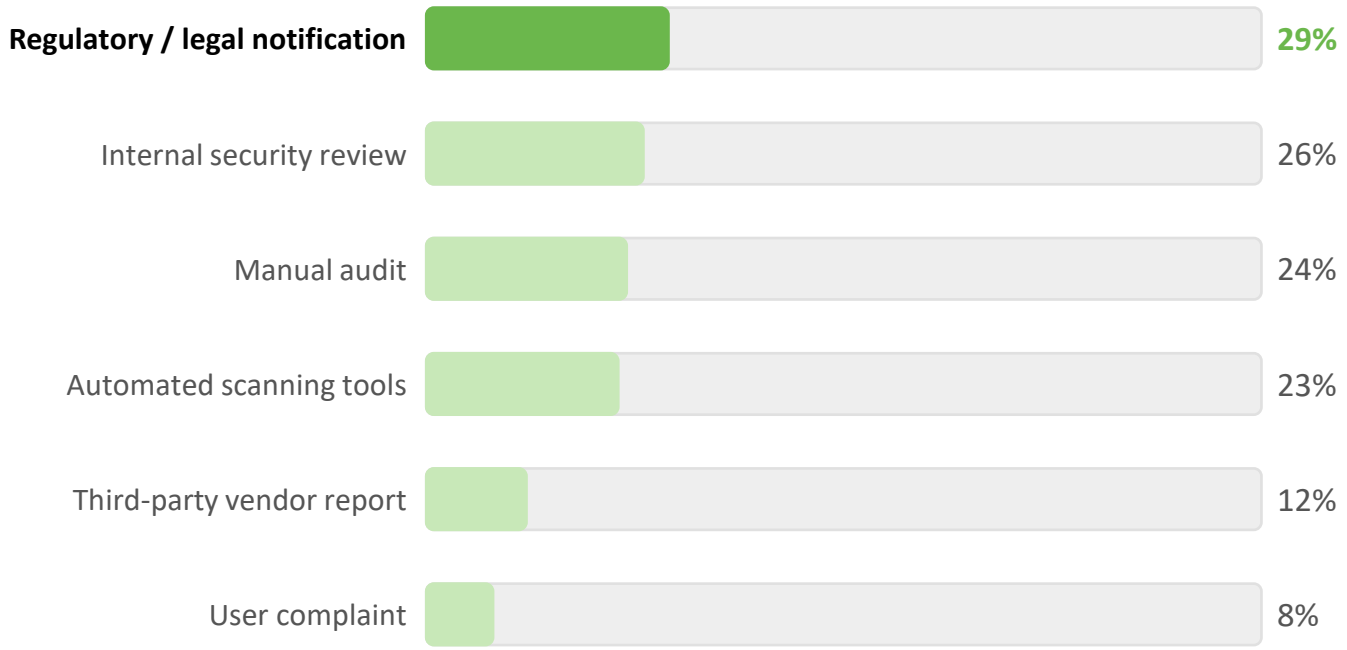


Only 8% believe all their scripts are fully authorized - 92% cannot account for all data collection activity on their properties. More than half (53%) discover unauthorized scripts monthly or more.

Source: Censuswide / Feroot Security - Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

How Are Unauthorized Scripts Typically Discovered?

The most common discovery method is regulatory or legal notification - meaning organizations learn of compliance failures through enforcement, not internal monitoring.



Fewer than 1 in 4

organizations use automated scanning for proactive detection

Source: Censuswide / Feroot Security - Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

AUDIENCE POLL

If legal action - civil or regulatory - were filed today over a consent failure, how ready are you to respond and produce evidence?

A Fully prepared - we have historical, auditable evidence on demand

B Mostly prepared - we could produce it, but it would take time

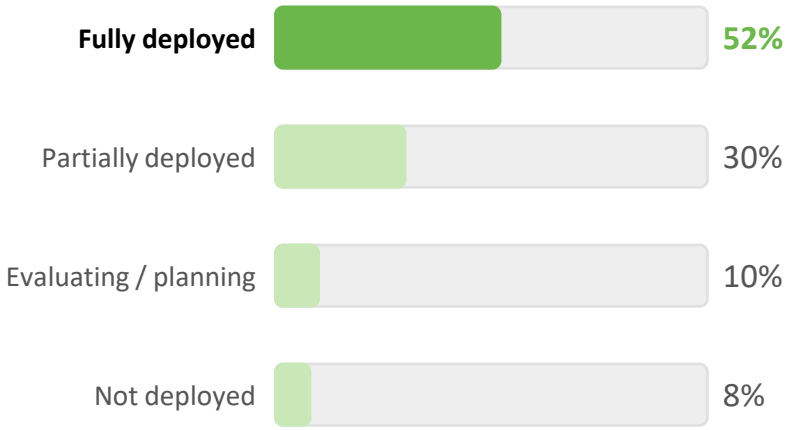
C Uncertain - we're not sure what evidence exists or where

D Not prepared - we have no audit trail to produce

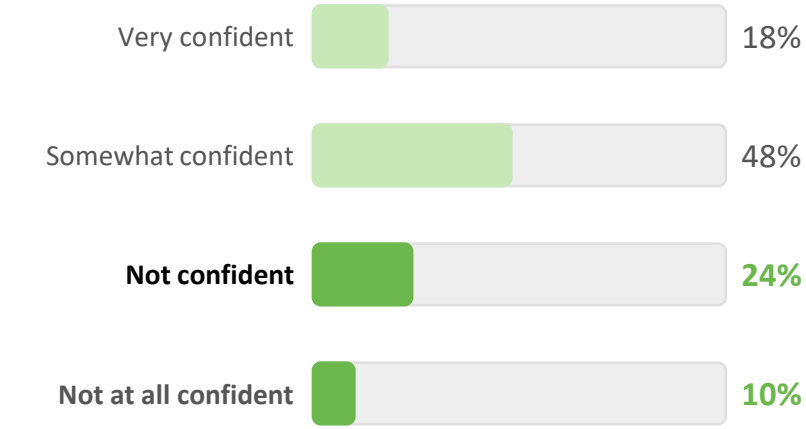
Submit your answer using the poll panel in the webinar platform.

CMP Deployment vs. Confidence in Blocking

CMP deployment status



Confidence that CMP blocks all pre-consent scripts (among CMP users)



82% of organizations have a CMP deployed. Yet among those users, only 18% are very confident it is blocking all non-consented scripts. One in three CMP users actively lacks confidence their consent infrastructure is functioning correctly.

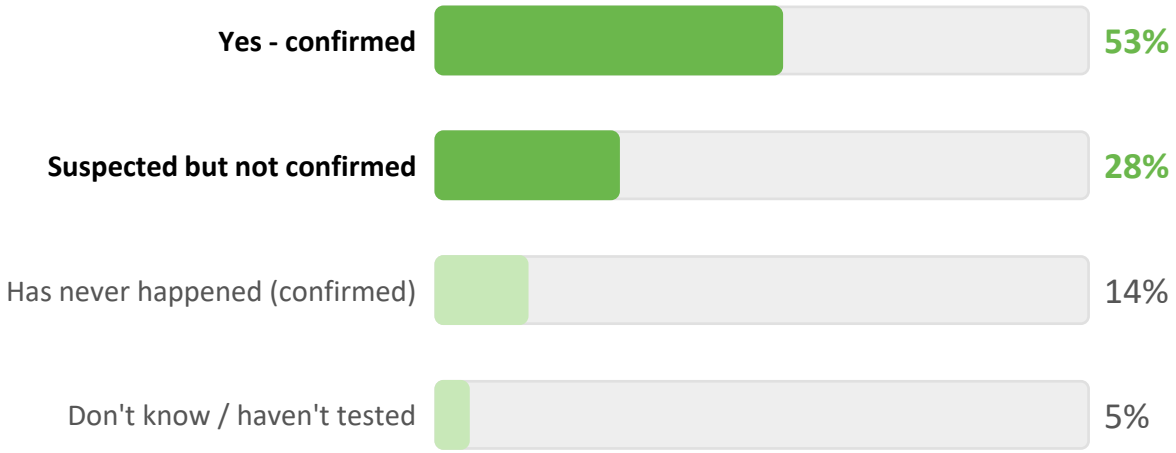
Source: Censuswide / Feroot Security - Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

Pre-Consent Script Firing - The Defining Statistic

81%

of CMP-deployed organizations have confirmed or suspected scripts firing before user consent was given

Among organizations with a CMP deployed:



These organizations did the right thing - they deployed a CMP. And their consent infrastructure still failed them. Only 14% can confirm pre-consent firing has never occurred. Deploying a CMP configures consent rules. It does not verify they work at runtime.

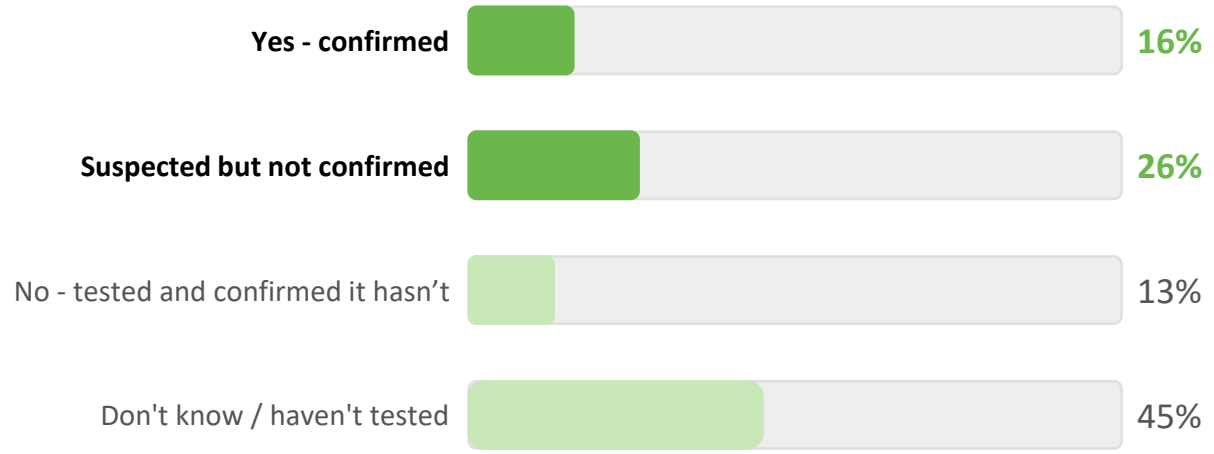
Source: Censuswide / Feroot Security - Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

Pre-Consent Script Firing: What You Told Us in Our Last IAPP Webinar

87%

of respondents could not confirm their own scripts never fire before consent

Among the 86 of 113 respondents who answered:



Only 13% of respondents could confidently say their organization has tested and confirmed scripts never fire before consent. This is the clearest signal from that session: most organizations cannot currently answer a basic compliance question about their own website.

Source: Feroot Security - Live poll, IAPP Webinar, June 30, 2026 (86 of 113 respondents answered)

SECTION 4

Findings From the Field

What 92 consent audits actually show

A consent banner is a doorbell, not a lock. Almost every site has one. Almost none of them stop the trackers.

What We Audited

Between July 15 and September 1, 2026, Feroot ran automated consent audits across 92 companies - 168 scans total, collapsed to each company's most complete audit so nobody is counted twice. All companies specifically requested the audit.

92	168	6,261	6,454
Companies Audited	**Total Scans**	**Vendor Observations**	**Cookies Observed**
Audited once each	July 15 – September 1, 2026	Across all 92 companies	464 regulation assessments

SECTOR MIX

- 22 Healthcare
- 12 Financial Services
- 8 Higher Education
- 50 Distributed Evenly Across Industries
- Mostly large North American brands

Gap 1: The "Do Not Sell" Signal Is Ignored Almost Everywhere

93%

of companies ignored the Global Privacy Control (GPC) signal entirely

Of 83 companies measured for GPC:

GPC is a browser setting that tells every site "do not sell or share my data." California treats it as legally binding - so do Colorado, Connecticut, and Texas. This is the most dangerous gap because it is trivially provable: a regulator flips one browser setting, loads the page, records what fires. No subpoena, no expert witness. The California Privacy Protection Agency has already used exactly this method. Median 8 vendors kept loading; the worst case carried 31.

Gap 2: Clicking "Reject" Doesn’t Stop Them Either

93%

kept loading ad and tracking vendors after a visitor clicked "Reject All"

Of 74 companies measured on both signals:

The asymmetry is the diagnosis: 20 companies honored the Reject button but ignored the GPC signal. Only 3 did the reverse. Teams wired up the thing they can see - the click. They never wired up the signal that arrives silently in a request header before the page renders. Median 7 vendors kept loading after rejection.

Gap 3: Miscategorized Trackers

69%

file a known ad or analytics cookie under a category the consent banner never blocks

Of 90 companies measured for cookie categorization:

This is the gap nobody knows they have. A consent platform blocks cookies by category - "Strictly Necessary" is never blocked, by design. So if an advertising cookie is labeled "Strictly Necessary," the platform works perfectly and the tracker fires anyway. TikTok is unanimous: 83 TikTok cookies across 18 companies, every single one filed under "Functionality." Not 18 independent mistakes - a default that ships wrong and never gets reviewed. 236 mislabeled cookies in total.

Gap 4: Data Leaves the Country of Origin, and CMP Can’t do anything about it

82%

have a third party that both reads a form field and sends data off the page

Of 91 companies measured for cross-border flows:

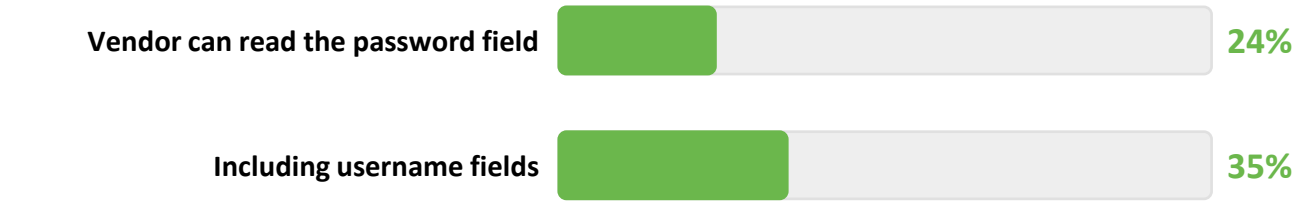
A tracker firing before the banner is answered has already sent the visitor’s IP address abroad - a completed international transfer with no lawful basis under GDPR. You cannot un-send it. Consent is not a valid basis for a permanent ad-tech pipeline, and almost no privacy notice names the vendors receiving the data. Fields most often read: email, last name, first name, zip, phone, address, and password.

Gap 5: Insufficient Safeguards - Third-Party Scripts Can Read the Password Field.

24%

had an outside vendor's script with **read access** to the password field, and that vendor sends data off the page

Of 91 companies measured for form-field access:



This is the clearest possible proof that nobody is checking what third-party scripts can reach. On one exchange operator's site, Reddit Ads, X/Twitter Ads and TikTok all had read access to the password field. On a major retail bank, an advertising platform did too. If an ad tag can see the password box, the claim that anyone has verified what it does with consent data is not credible. Google Tag Manager was the vendor most often in a position to read it.

How Well Are CMP's Actually Performing?

60% vs 81%

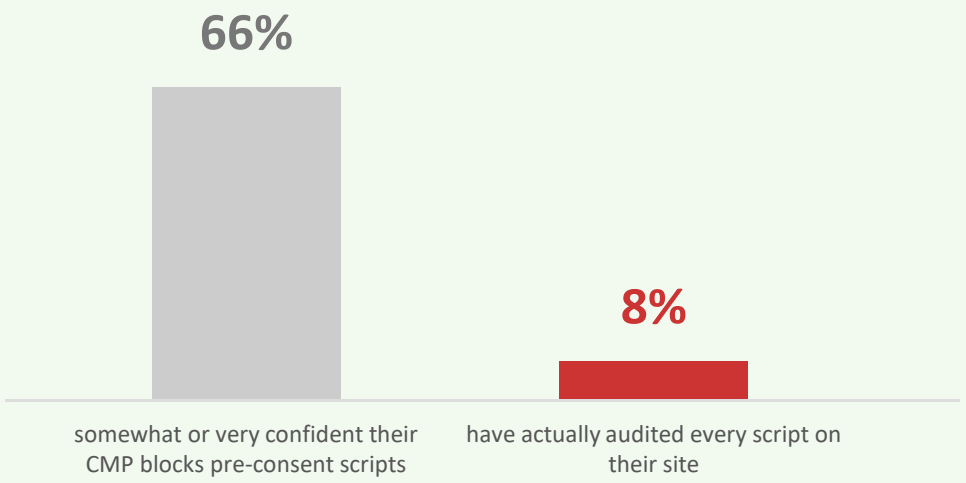
of vendors still fire scripts before or after the consent click (CMP signal) - with a CMP platform vs. without one.

Source: Feroot Security - Consent Audits, 92 Companies, July–September 2026

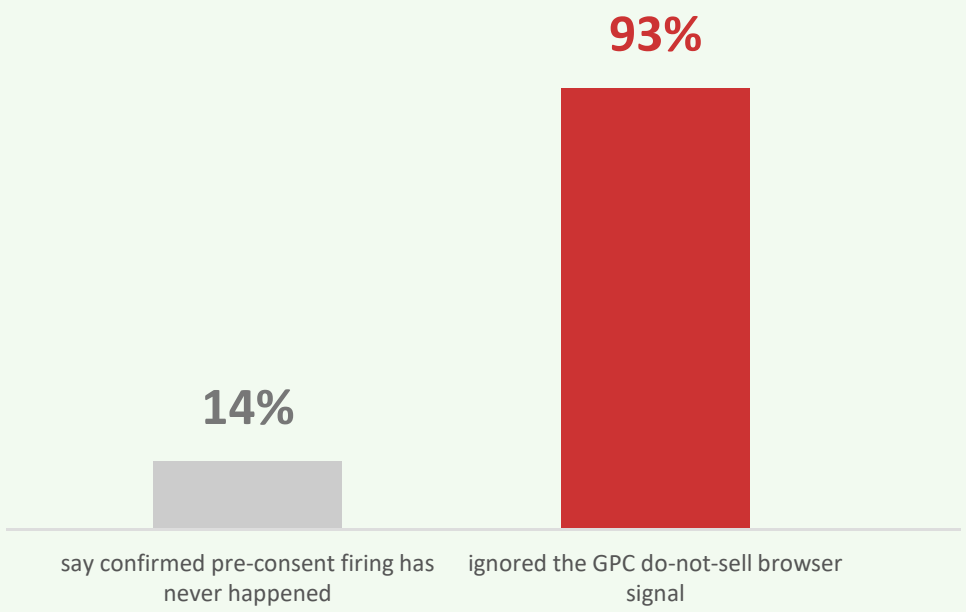
The raw comparison is misleading: platform customers carry twice the tracking load (median 16 vendors vs. 9), so they simply have more to get wrong. Normalized, a consent platform cuts the leak from about 8 trackers in 10 to about 6 in 10 - it does not close it. Buying the platform is roughly a third of the job. The other two-thirds is configuration and verification, and almost nobody is doing it. We identified a named platform on 52 of 92 companies (57%) - OneTrust, Tealium, CookieYes, TrustArc and others.

PERCEPTION VS. REALITY: Confidence Runs Ahead of Control

The confidence gap



Belief vs. audited behavior



Sources: Censuswide / Feroot Security survey, 800 professionals, May 2026 · Feroot Security consent audits, 92 companies, July–September 2026

Competencies Needed to Avoid Litigation

What separates exposure from defensibility

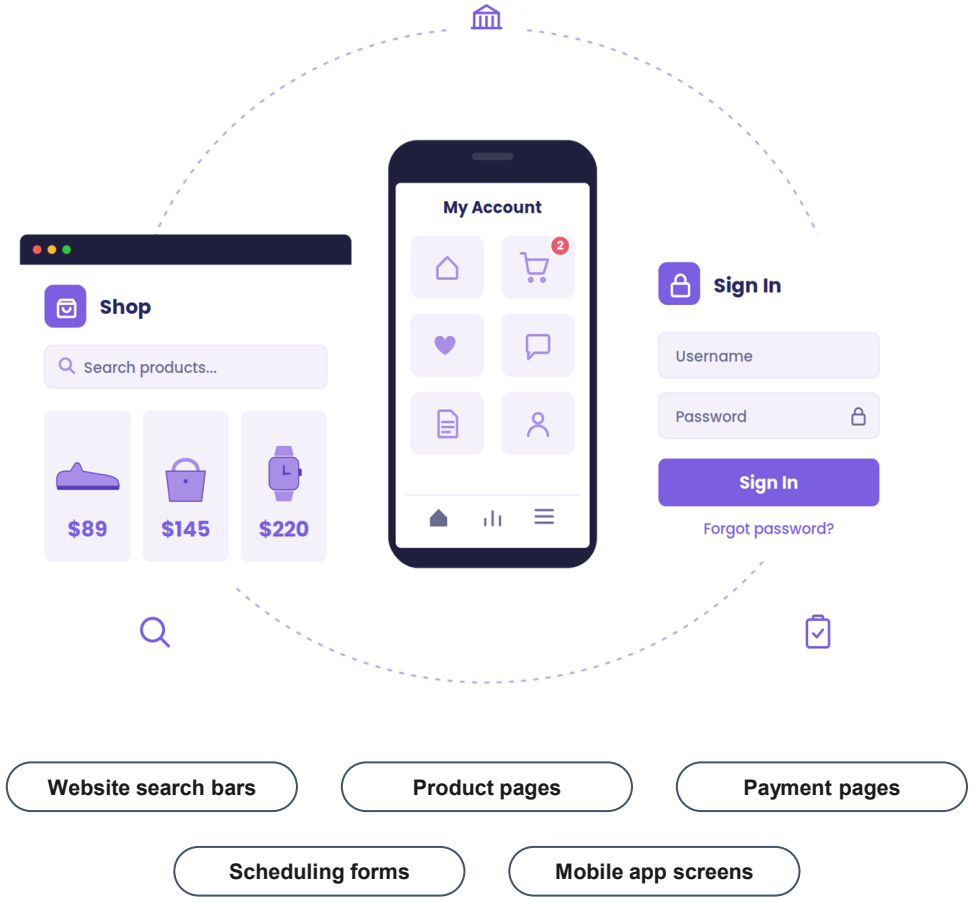
Every gap in this deck is fixable with a control point, not a rewrite.
Here is what regulators will look for and what closes the gap.

The Risk Perimeter

Websites, portals, and mobile apps are now part of every major compliance regulation.

Every customer-facing touchpoint, from public search bars to authenticated portals and mobile app screens, needs visibility, governance, and evidence.

The user experience is no longer just a digital front door. It is now part of the regulated privacy environment.



Why This Is a Legal Problem, Not Just a Technical One

$5,000

Per-Visit Exposure: Each unauthorized website visit or data transmission via tracking pixels or chat widgets can be counted as a separate $5,000 violation.

The regulations that carry material risk today:

CIPA carried 100% failure on both consent and GPC across the 48 companies we could assess it against. A tracker firing before consent on a site with a million monthly visitors is an arithmetic problem, not a legal one. California is also the only regulator that has enforced specifically on GPC, and the finding is provable in a browser in thirty seconds. GDPR compounds it: every company in this set sends data to the US, so there is both an unlawful transfer and no valid basis for it.

Trap #1: The Fractional Compliance Trap

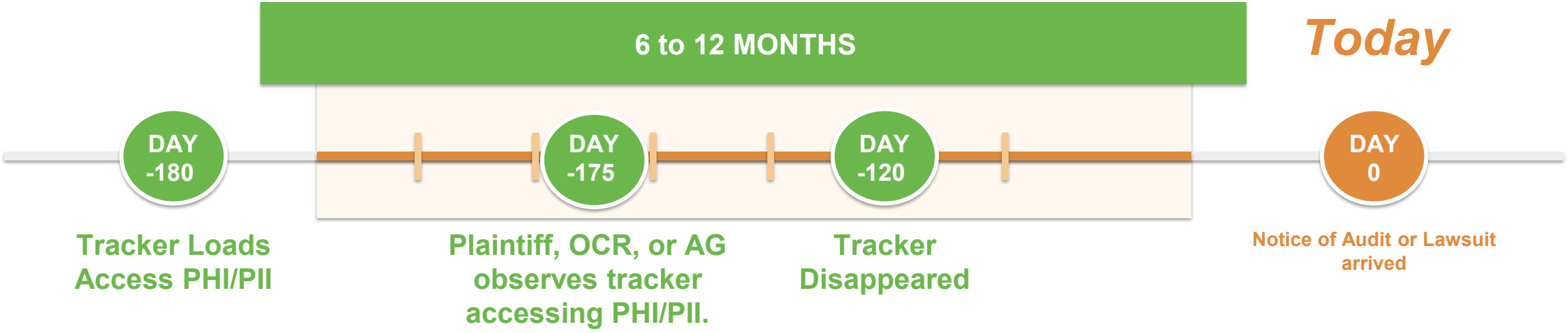
✗ FRACTIONAL Point-in-time Privacy and Risk Assessments	✓ END-TO-END, ALWAYS ON
BAA with 1 of 10 trackers → fractional coverage	Every script, and every banner on every page - discovered and governed continuously
Annual script tracker audit → snapshot of 1 day in 365	Real-time monitoring, 365 days - with historical audit trail and proof of evidence
Cookie banner on homepage only → 3 of 47 pages covered	Consent audit validates runtime behavior across all pages & apps
Privacy program covers backend, not the browser layer	Website + portal + mobile app - the full DUX perimeter
Manual tracker inventory → outdated within days	Always-on tracker inventory - alerts when anything changes

Recent Compliance Actions

Organization	Settlement	Sector	Digital Experience Layer Compliance Gap
LinkedIn	**$310M**	Tech/B2B	GDPR fine: behavioral ad targeting via third-party data without valid consent basis for tracking
Disney / ESPN	**$90M Class Action**	Media/Entertainment	VPPA & CCPA: ESPN app shared video viewing data with Facebook pixel without user consent
Sephora	**$1.2M**	Retail	CA AG settlement: sold consumer data without opt-out; OTT tracking on website without disclosure
TikTok	**€345M**	Social Media	GDPR: children's data collected via default settings; consent banners failed to honor preferences
Aspen Dental	**$18.7M**	Healthcare	Meta Pixel + Google Analytics on patient-facing pages collecting PHI without consent
Henry Ford Health	**$12.2M**	Healthcare	Meta Pixel tracked MyChart portal users 2020–2023 without HIPAA-compliant consent
BJC HealthCare	**Up to $9.25M**	Healthcare	Meta Pixel sharing patient PHI during website interactions
Blue Shield of California	**Class Action**	Insurance	Member data shared with Google advertising product via website tracking

Trap #2: The Time-Lag Trap

Lawsuits and audits target what happened on web pages months ago, not today.



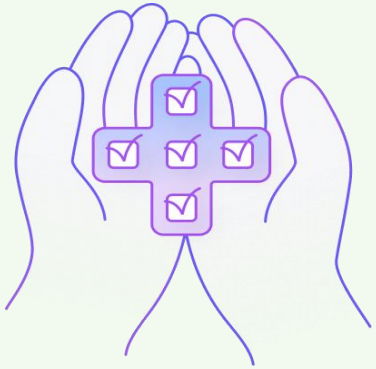
The State Patchwork: Active, Aggressive, and Accelerating

State	Law	Status	DUX Compliance Requirement at the Digital Experience Layer
California	CPRA	ACTIVE	Opt-out of sale/sharing via GPC signal; consent banner must match actual vendor firing behavior; sensitive data requires opt-in; right-to-delete flows to third-party scripts
Virginia	VCDPA	ACTIVE	Opt-in required for sensitive data processing; controller must maintain auditable consent records; third-party vendor firing must reflect captured consent state
Colorado	CPA	ACTIVE	Universal opt-out via GPC must be honored; sensitive data requires opt-in consent; cookie banners must match actual runtime script and tracker behavior
Connecticut	CTDPA	ACTIVE	Universal opt-out mechanism required; consent must be validated per-vendor and per-jurisdiction; dark patterns in consent UI are prohibited
Texas	TDPSA	ACTIVE	Applies to any site accessible to TX residents; controller must maintain verifiable per-activity consent documentation; no revenue threshold for many provisions
Oregon	OCPA	ACTIVE	Consent must be granular per data category and purpose; third-party OTT inventory required; continuous monitoring needed for downstream vendor compliance
Montana	MCDPA	ACTIVE	Opt-in for sensitive data; consent records must be auditable; cookie banners must accurately reflect which vendors fire under each consent state
New Jersey	NJDPA	ACTIVE	Opt-out of sale and targeted advertising; controller must document processing activities; consent banner behavior must be validated against actual script execution
New Hampshire	NHPA	ACTIVE	Opt-out rights for sale and profiling; sensitive data requires opt-in; compliance program must cover all consumer-facing digital properties

Six Steps From Exposed to Protected.

1 IDENTIFY

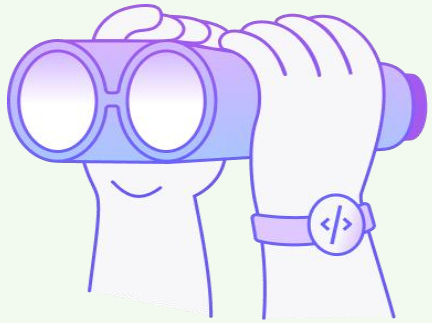
2 DISCOVER



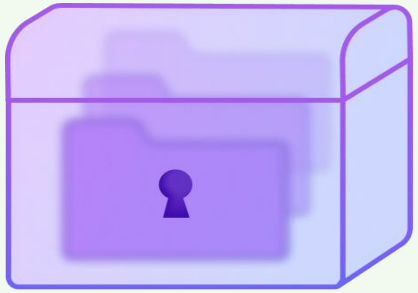
3 GOVERN

4 PREVENT

5 MONITOR



6 ARCHIVE



Estimating Costs of Consent Compliance Audits of DUX in 2026

- × 5 Digital Properties
- × 10 Geographies
- × 3 Languages
- × 4 Consent States
- × 52 weeks

= **31,200**

weekly audits/year

The 3 Dimensions of Privacy Compliance and Consent Effectiveness Audits

DIMENSION 1

Coverage Axes

- Number of pages across every property
- Every geo with its own consent rules
- Every language variant of a banner
- Presence of required privacy notices

DIMENSION 2

Consent State Testing

- Accept: only permitted vendors should fire
- Decline: no non-essential scripts should load
- No Action: pre-consent behavior controlled
- Each state tested independently per rule set

DIMENSION 3

Sampling Rate vs. Continuous

- Point-in-time = 1 day of proof out of 365
- Acceptable coverage gap: none, 10%, 30%, etc.
- Acceptable evidence gap: None, 1 day, 1 week, 1 month, 1 year.

Costs of Labor

$10.7M

Total cost of manual audits by humans per year.

CONSENT SCENARIOS / YEAR

31,200

10 pages/screens each

MANUAL HOURS REQUIRED / YEAR

171,600

5.5 hours per audit

FULL-TIME EMPLOYEES NEEDED

90

Based on 160 hrs/month and $120,000 avg salary

AUDIENCE POLL

Do you have the resources to properly audit your CMP today?

A Yes - we audit continuously with dedicated tooling

B Yes - but only periodically (manual, quarterly, etc.)

C No - we rely on the CMP vendor's own reporting

D No - we don't currently audit CMP behavior at runtime

Submit your answer using the poll panel in the webinar platform.

The Evolution Of AI-Assisted Privacy Compliance

A full self-driving analogy for how privacy professionals increasingly use AI systems

THE AUTOCOMPLETE (Level 1)

AI serves as a reference tool or enhanced search. Humans use AI for specific answers, citations and research.

THE INTERN (Level 2)

AI writes boilerplate or low-risk reports. The privacy person prompts for specific functions, then immediately reviews and integrates output.

JUNIOR PROFESSIONAL (Level 3)

Interactive pair-assessments. Human and AI trade off control while results and conclusions are reviewed as they are generated in real time.

THE PRO (Level 4)

AI generates most of the compliance assessments. The privacy person reviews everything AI does and becomes the verification bottleneck.

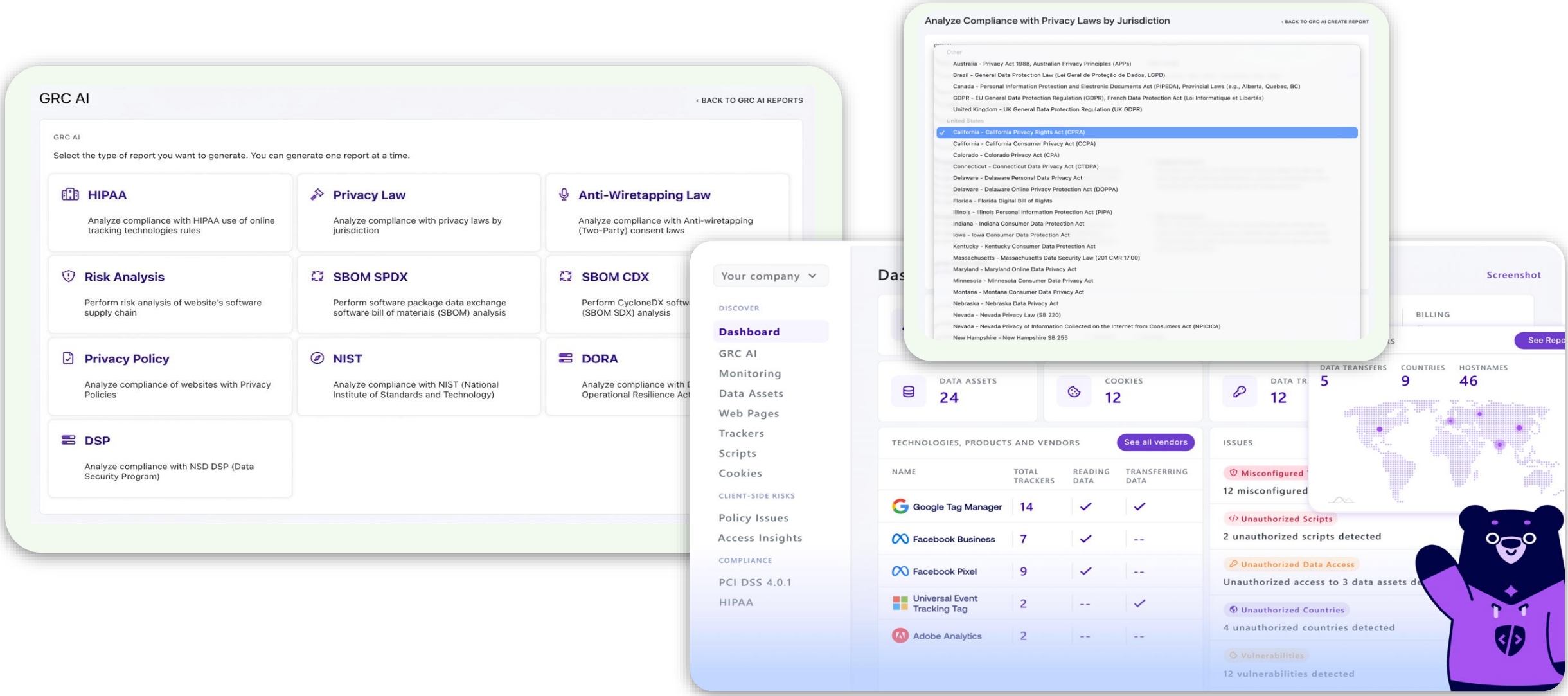
SENIOR PROFESSIONAL (Level 5)

AI runs unattended for longer periods, handles complex tasks, and relies on self-checks. Humans verify final results later.

"FSD" COMPLIANCE FACTORY (Level 6)

Privacy people manage goals and constraints, not software. AI defines implementation, performs discovery, runs tests, writes reports, fixes gaps, enforces policies, and ships.

Autonomous AI-Agents: Always-On, Precise, and Working 24/7



AUDIENCE POLL

How often are you using AI to validate compliance?

A Daily or continuously - AI runs largely unattended

B Weekly or monthly - AI assists specific reviews

C Rarely - we've experimented but don't rely on it

D Never - compliance validation is fully manual

Submit your answer using the poll panel in the webinar platform.

Where To Go From Here

We covered a lot today: third-party scripts, CMP failures, vendor blind spots, and more. If you'd like more information, scan the QR code to:

- ✓ Get the full report for the data behind today's discussion
- ✓ Start a free privacy consent assessment of your own website

feroot

feroot.com/iapp

Questions & Answers

Submit your questions using the Q&A panel in the webinar platform.

DISCUSSION TOPICS

- Which of the five gaps is most common in your own environment
- How to prioritize remediation when you can’t fix everything at once
- What audit-ready evidence looks like for a regulator or plaintiff’s attorney
- Evaluating automation tools versus manual review - where each fits
- How the free assessment works, and what you get back

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings please contact:

livewebconteam@iapp.org