iapp

“Say it, do it, prove it” for consent:

Best practices for building a closed-loop consent & preference audit program at scale

Thursday, 19 March
10:00–11:00 PDT
13:00–14:00 EDT
18:00–19:00 CET

feroot

IAPP WEBINAR · CONSENT & PREFERENCE AUDIT

“Say It, Do It, Prove It”

Best Practices for Building a Closed-Loop Consent & Preference Audit Program at Scale

Ian Wardell & Ivan Tsarynny
Reddit & Feroot Security

March 19, 2026

March 2026

WEBINAR AGENDA

1 **Speaker Introductions**

Ian Wardell, Reddit · Ivan Tsarynny, Feroot Security

2 **Best Practices for Consent Compliance**

Common program failures, closed-loop audit design, and KPIs, and operationalizing continuous testing

3 **Auditing Consent Compliance at Scale**

Scenario matrices, sampling blind spots, and scaling across properties, geos, and regulations

4 **Performing Consent Audit at Scale**

Ivan Tsarynny, Feroot Security — how automated consent auditing closes the loop

5 **Moderated Discussion**

10 practitioner questions on consent program challenges

Meet the Speakers

Ian Wardell, J.D.

Privacy & Risk · Reddit - Security

Ian Wardell is a privacy and security professional with expertise spanning legal and technical privacy. His work focuses on ‘finding yes’ with real-world technical solutions, ensuring compliance and safeguarding data privacy across highly regulated sectors.

Before Reddit, Ian was the Privacy Engineering Lead at FinTech Gusto and Privacy & AI Researcher at Intel, where he published conference papers and contributed to ISO Standards. Prior experience includes IP and data protection at Mertzel Law PLLC, and systems administration at Rutgers University.

J.D., Seton Hall University School of Law · Masters, Rutgers · Bachelors Computer Science & Political Science, Rutgers

Ivan Tsarynny

CEO & Co-Founder · Feroot Security

Ivan leads Feroot Security, a recognized leader in helping enterprises deliver compliant and secure digital experiences by safeguarding sensitive user data across websites and mobile applications.

In February 2025, he led the discovery of hidden code in DeepSeek designed to covertly transmit data to China Mobile, and testified before a U.S. Congressional committee on national security risks of data collection by China’s big tech sector.

Featured on CNBC, ABC Good Morning America, CNN Anderson Cooper 360. Cited by The Wall Street Journal, Bloomberg, and AP.

Disclaimer

The information presented in this session is for educational purposes only and does not constitute legal advice. The case examples, penalties, and regulatory references discussed are provided for informational context and should not be relied upon as a legal opinion or compliance determination. Every organization's situation is unique. Please consult qualified legal counsel before making decisions about your consent management practices, privacy compliance program, or legal obligations.

feroot

Best Practices for Consent Compliance

Ian Wardell · Privacy & Risk, Reddit

1 Why CMP Configuration ≠ Compliant Outcomes

MOST CONSENT PROGRAMS FAIL IN THE GAPS — NOT THE CONFIG

Gap 1: Policy → Implementation

Consent rules are defined but never validated at runtime. Banner logic, geo-targeting, and opt-out flows are assumed to work — not verified.

Gap 2: Banner Choice → Runtime Outcome

A user declines. But what actually fires afterward? Without runtime testing across all consent states, you don't know what vendors load post-decision.

Gap 3: Point-in-Time → Continuous

Website releases, script and tag manager updates, and new vendor tags can silently break consent controls overnight. A yearly or quarterly audit captures just one day in a time window.

KEY INSIGHT

Deploying a Consent Management Platform (CMP) configures rules. It does not verify they work at runtime, across every page, in every consent state, after every release. Bridging that gap is the core challenge of a mature Compliance & Privacy program.

2 Designing a Closed-Loop Consent & Preference Audit

VERIFY THE FULL CHAIN — NOT JUST THAT THE BANNER APPEARED

01

Policy

Define Script/Tag categories, consent rules per regulation and geo. Set expectations for Accept, Decline, and No Action states across all properties.

02

User Experience

Validate banner renders correctly, geo-appropriate variants display, and all consent states are testable across pages and flows.

03

Consent Signal

Verify the signal is captured, passed to downstream systems, not overridden by default behavior, and persisted correctly.

04

Evidence & Remediation

Document scripts and tags fired vs. blocked per consent decision. Flag violations, action remediation, re-test to confirm resolution.

Most programs fail between steps — not within them. Point-in-time checks and incomplete coverage are where compliance gaps hide.

3 Scaling Consent Testing: The Scenario Matrix Approach

MANUAL PAGE-BY-PAGE SCRIPTING CANNOT COVER THIS MATRIX

Pages × Properties × Geographies × Languages × Consent States × Vendor Behaviors

DIMENSION 1

Coverage Axes

- Every page type across every property
- Every geo with its own consent rules
- Every language variant of a banner
- Define scenarios once — run everywhere

DIMENSION 2

Consent State Testing

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

DIMENSION 3

Sampling vs. Continuous

- Sampling creates blind spots between checks
- Releases & tag changes break consent daily
- Point-in-time = 1 day of proof out of 365
- Continuous testing is the only defensible approach

4 Measuring C&P Program Performance with Operational KPIs

REPLACE BINARY STATUS CHECKS WITH OPERATIONAL METRICS

⚠ BINARY STATUS — What most programs report	✓ OPERATIONAL KPI — What you should track
"Banner is present on all pages"	Drift Rate — % of pages where consent behavior changed since last test
"Our CMP is configured correctly"	Violation Density — # of vendor fires in wrong consent state per 100 pages tested
"Audit was completed last quarter"	Time-to-Remediate — avg hours from violation detected to verified fix
"We haven't received any complaints"	Evidence Coverage — % of properties with full audit chain for current period
"We believe our controls are working"	Program Trend — KPI trendlines over time showing improvement or regression

5 Operationalizing Continuous C&P Auditing

FROM ONE-TIME EXERCISE TO ALWAYS-ON PROGRAM

1 DEFINE SCOPE

Inventory all web properties, apps, tracking technologies ie tags/scripts, geographies, and applicable regulations. Define your consent policy matrix per jurisdiction.

2 BUILD SCENARIO LIBRARY

Create test scenarios for each consent state and geo. Map expected vs. actual vendor behavior for each rule set — no manual scripting.

3 AUTOMATE TESTING

Run scenario matrix continuously — triggered by releases, scheduled daily runs, or on-demand. Determine scope or cover all pages, all properties, all geos.

4 CAPTURE EVIDENCE

Document the full audit chain: consent choice → scripts fired → scripts blocked → timestamped proof. Store for regulatory defensibility.

5 REMEDIATE & RE-TEST

Route violations to responsible teams. Track time-to-remediate. Re-run affected scenarios to confirm resolution before closing.

6 REPORT & IMPROVE

Share KPI trends with legal, DPO, and GRC. Use program data to justify CMP investments and demonstrate measurable risk reduction.

Consent Audit of Digital User Experiences.

How to Verify at Scale That Consent Choices Are Respected and Enforced.

Ivan Tsarynny · CEO, Feroot Security

Clarifying the limitation of CMP / cookie banners

What CMP is designed to DO

- ✓ Displays consent notice to users
- ✓ Records user consent choices
- ✓ Manages cookie preference categories
- ✓ Provides opt-out mechanism

What CMP is NOT designed to DO

- ✗ Control all tracking pixels are actually firing
- ✗ Prove whether pixels fire BEFORE consent is given
- ✗ Data sent by third-party scripts to external servers
- ✗ Pixels embedded deep inside iFrames or tag managers

Coming from The Experience of Finding National Security Risks in Digital User Experiences.

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.

https://selectcommitteeontheccp.**house.gov**/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/DeepSeek%20Final.pdf

- Feroot at US Congress
- Feroot on Wall Street Journal
- Feroot on Associated Press
- Feroot on CNBC
- Feroot on ABC News
- Feroot on Bloomberg
- Feroot on New York Times
- Washington Post
- Feroot on Forbes
- Feroot on Fortune
- Feroot on ABC Good Morning America

CSPAN @cspan · 1h

.@ivan_tsarynny, CEO of Feroot cybersecurity, testifies @USCC_GOV on the cyber risks of TikTok. He says ByteDance, the parent company of TikTok, uses technology that collects large amounts of U.S. users' data--even from people who have never used TikTok.

The Top 3 Ways Web Tracking Pixels Can Bypass CMP “cookie banner” (technically explained).

1. Pre-Consent Fire

Pixel fires on page load before user interacts with banner. This is the most common violation pattern — happens even with GTM-based CMP integrations.

2. Tag Manager Drift

A marketer adds a new pixel to GTM without updating CMP category rules. CMP has no knowledge of the new tag. Pixel fires unchecked.

3. iFrame Blind Spot

Third-party forms, chat widgets, or embedded content run in iFrames. CMPs cannot inspect or block JavaScript inside iFrames they don’t own.

Performing Consent Audit at Scale

EVERY DAY IS AUDIT DAY — BECAUSE EVERY CHANGE CAN BREAK CONSENT

THE CLASSIC WAY

Most organizations treat consent as a one-time configuration

Point-in-time audits miss regressions after new releases

Manual testing cannot scale across hundreds of pages & properties

No visibility into what actually fires after a consent decision

CMP platforms are necessary — but not sufficient

THE AT SCALE APPROACH

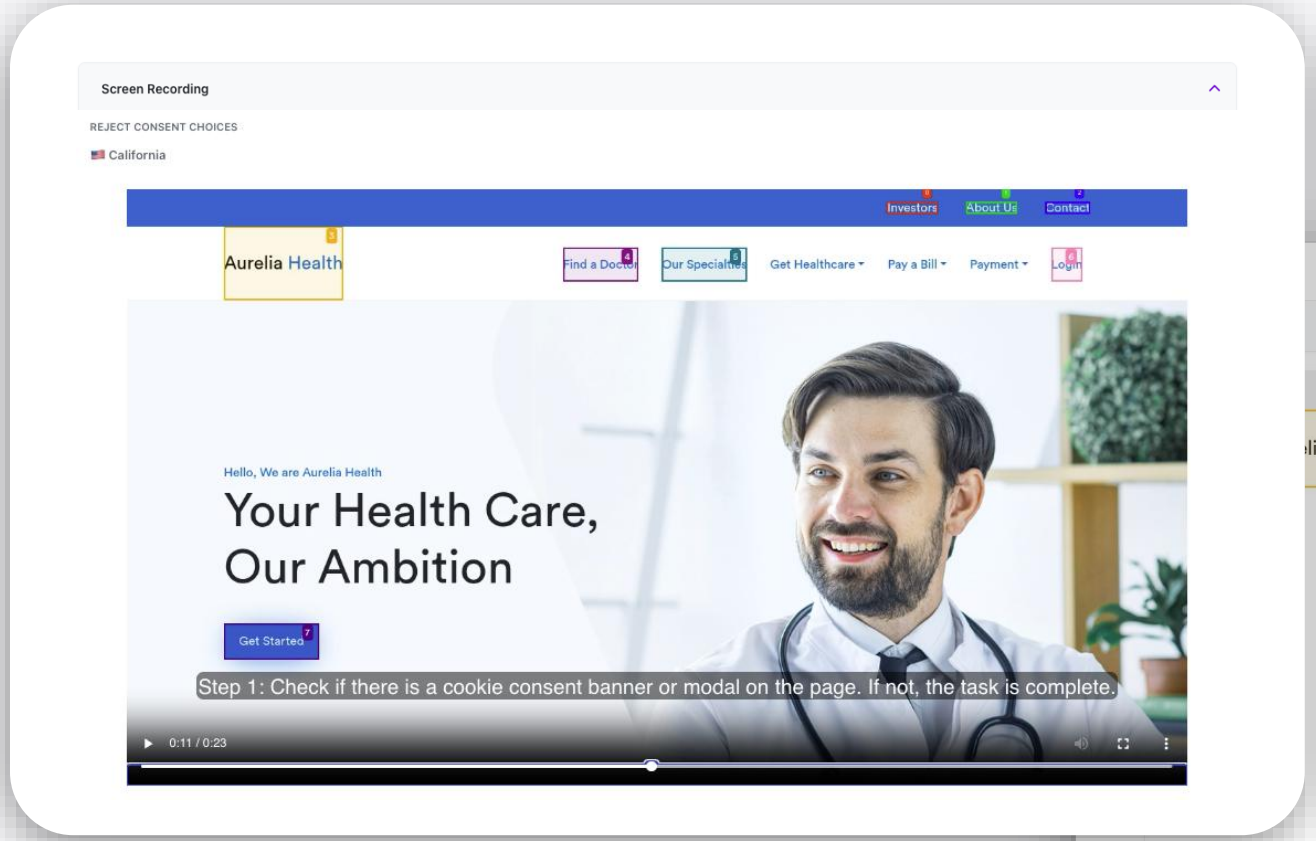
Every Regulation and Jurisdiction.

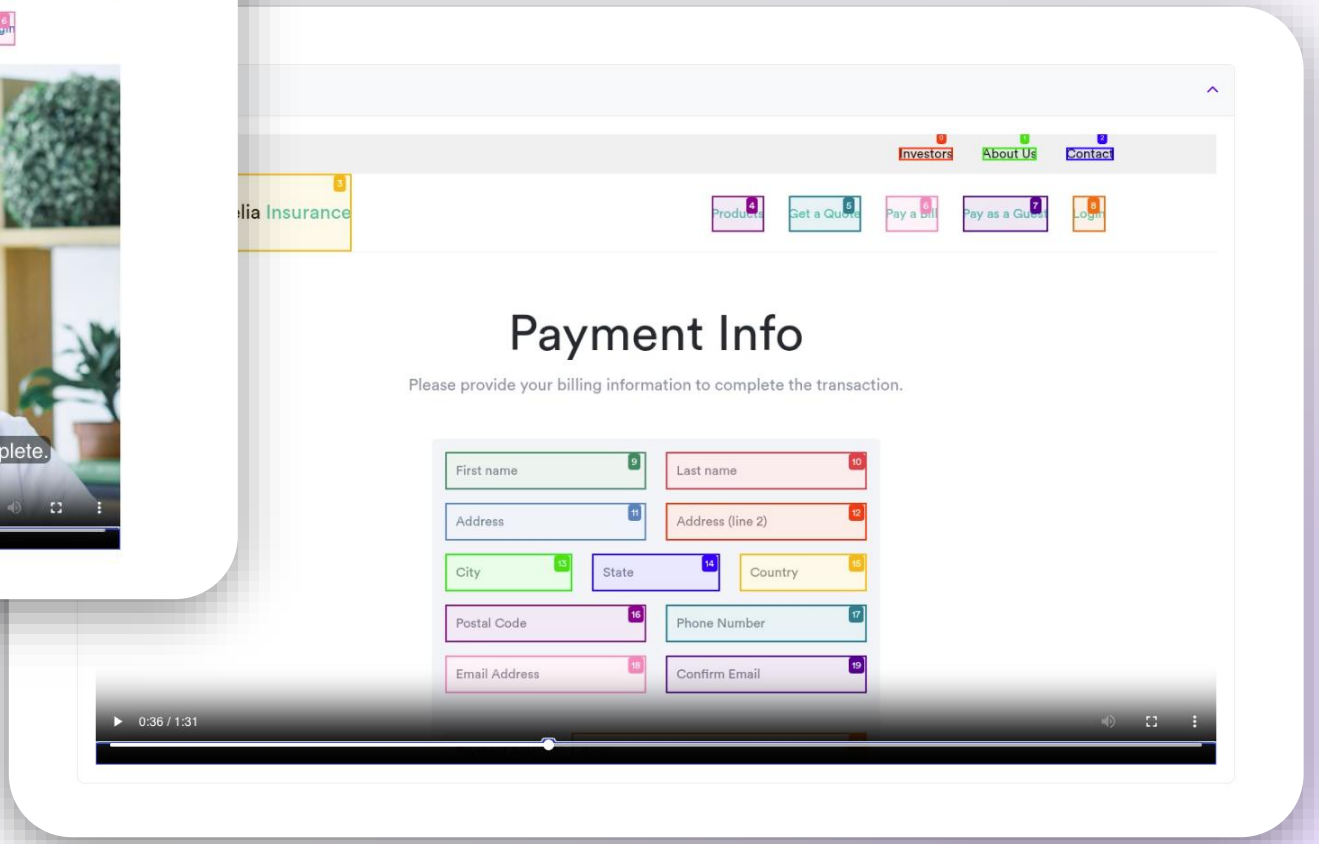
Every Digital User Experience.

Everything automated. Zero human hours.

01	02	03	04
Define Policy →	**Audit Everywhere** →	**Inspect Evidence** →	**Measure Outcomes**

Have You Seen AI Agents Do the Repetitive and Tedious Tasks?





feroot

Moderated Discussion

Ian Wardell & Ivan Tsarynny

feroot

Discussion
Q1

Many organizations deploy a CMP and assume consent is working.
Where do you most commonly see the gap between CMP configuration and actual runtime outcomes?

feroot

Discussion
Q2

Auditing consent at scale sounds straightforward. In practice, it isn't.
What are the biggest operational challenges when trying to test across hundreds of pages, multiple geographies, and different consent states simultaneously and what breaks down first?

feroot

Discussion
Q3

Sampling-based audits are the default for most programs.
Ian, what blind spots does sampling create and how do you explain to leadership why “we checked last quarter” isn’t good enough?

feroot

Discussion
Q4

The closed-loop model you described is clear in theory.
Walk us through what a real-world violation looks like from the moment a tracker fires when it shouldn’t, to investigation, to evidence, to remediation and re-test?

feroot

Discussion
Q5

Privacy and GRC teams are being asked to prove program effectiveness, not just report on activity.

What is the best way to develop KPIs unique to an organization?

feroot

Discussion
Q6

Most organizations already have a CMP. They've made that investment.
How does automated consent auditing amplify a CMP investment rather than compete with it and what does the ROI story look like?

feroot

Discussion
Q7

Vendor creep is one of the most common sources of consent regression.
Ivan, what does that look like in practice?
How does a new marketing tag silently break a consent program that was working fine the week before?

feroot

Discussion
Q8

Organizations operating in multiple jurisdictions face different consent rules for the same digital property.
Ivan, how do you architect a consent audit program that handles GDPR, CCPA, and 22+ state laws simultaneously without recreating everything for each regulation?

Discussion
Q9

We've talked about technical audit mechanics. But privacy programs also have to answer to regulators.
Ivan, what does "defensible evidence" look like in practice. What format, what level of detail, and how long does it need to be retained?

feroot

Discussion
Q10

Let’s bring it back to the audience.
Ian and Ivan: if a practitioner leaves today and wants to take one concrete step toward a closed-loop consent audit program, what’s the highest-leverage action they can take right now?

Audience Q&A

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iappwf.questionpro.com/t/AbBPvZ8IeN

Thank you in advance!

For more information: www.iapp.org

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