



How to Build a Reliable Privacy Consent Verification Process

Monday, October 19, 2026

IAPP Web Conference

Ivan Tsarynny, CEO and Co-Founder, Feroot Security



What we'll cover in the next hour

1 Why a consent banner isn't bulletproof

2 What you're required to do

3 The consent audit, step by step

4 What it takes to keep doing it

5 Next steps and Q&A

7

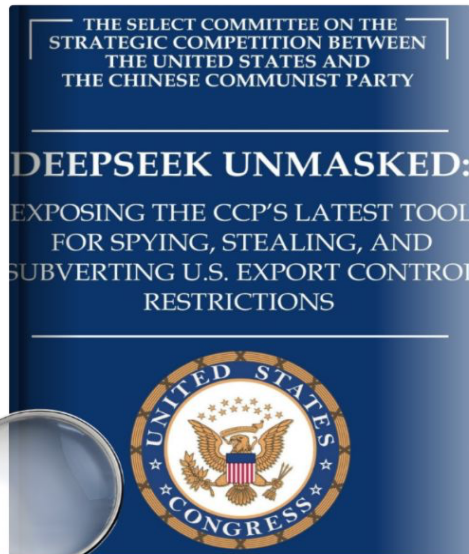
steps you can start with using a browser and a spreadsheet

3

anonymous polls along the way

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.



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 WALL STREET JOURNAL
EXCLUSIVE NATIONAL SECURITY
U.S. State-Government Websites Use TikTok Trackers, Review Finds
Security firm's report shows states might be inadvertently helping Chinese-owned app collect data
By [Byron Tau](#) and [Dustin Volz](#)
Updated March 21, 2023 11:45 am ET



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.



Private Health Data Still Being Exposed to Big Tech, Report Says

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](#)

Survey responders trust their CMP (eg., cookie banners), but scripts create exposure.

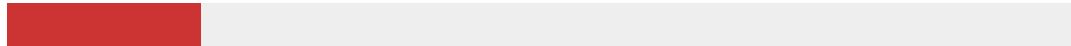
82%

of 800 surveyed have a consent management platform deployed



18%

of 640 CMP users of CMP users are very confident it blocks every script before consent



8%

of 800 surveyed say every script on their website is authorized



92%

can't fully account for what's collecting data on their own pages

Source: Censuswide survey for Feroot Security, 800 privacy, legal, marketing and IT professionals in the US, UK, Canada and Australia, May 2026.

Majority Websites keep tracking after visitors click “Reject”

WHAT SURVEY FOUND

81%

of CMP users have confirmed or suspected scripts firing before consent

of 640 CMP users, Censuswide, May 2026

WHAT ASSESSMENT FOUND

69%

of websites kept loading ad and tracking vendors after the visitor clicked Reject All

of 74 websites measured

WHAT ASSESSMENT FOUND

93%

of websites ignored the Global Privacy Control signal

of 83 websites measured

Ferroot consent audits of 92 companies that requested an audit, 168 scans, July 15 to September 1, 2026.

AUDIENCE POLL 1 OF 3

How would you rate your ability to verify that your website honors consent choices today?

A Strong: we test regularly and keep evidence of what loads in each consent state

B Partial: we spot-check some pages or rely on periodic manual reviews

C Limited: we rely mainly on our CMP's own reports

D We don't currently verify it

Submit your answer in the poll panel. Responses are anonymous.

Why it happens: scripts override the choice



A consent platform captures and records the choice.

Scripts decide what actually happens next.



Where scripts slip past the choice



Tags fire on page load, before anyone touches the banner



A new tag goes into the tag manager without updating consent rules



Embedded forms, chat and video run in frames the banner can't control



A tracker is filed under a category the banner never blocks



Data is sent server to server, where no browser setting reaches it

69%

of 90 audited companies miscategorize ad or analytics cookie under a category the banner allows to load

What you're required to do:



Say it

A visible banner with real choices, in the right places and languages, and privacy disclosures people can find



Do it

Honor accept, reject, withdrawal and opt-out signals such as Global Privacy Control, on every page



Prove it

Keep evidence of what loaded in each consent state, over time

Proof is usually about the past. A letter that arrives in November may be about a tracker that ran in March.

MARCH



Tracker runs

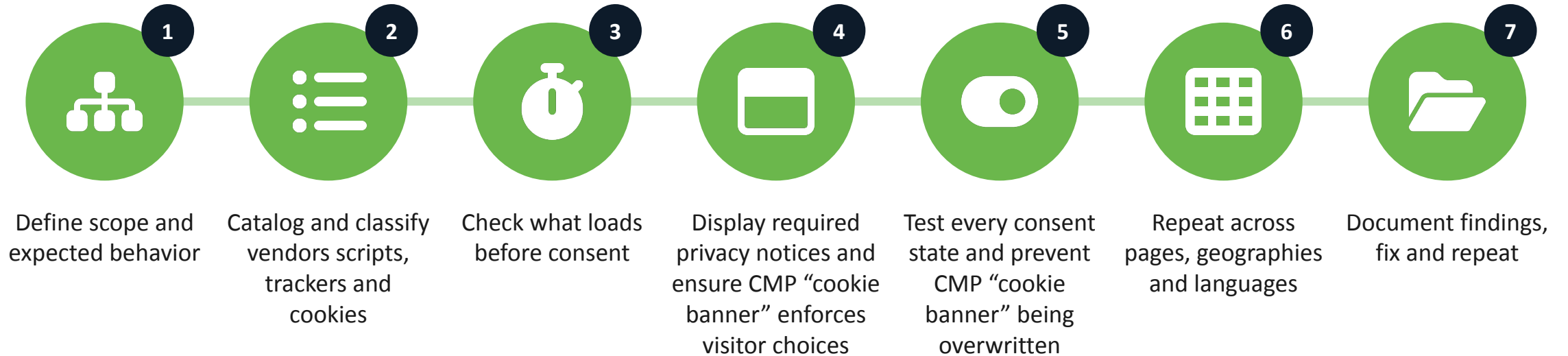
NOVEMBER



Letter arrives

Requirements vary by jurisdiction. This is not legal advice; confirm your obligations with your counsel.

The consent audit in seven steps



You can start every step with a browser and a spreadsheet.

Step 1: Define scope and expected behavior

STEP 1 OF 7

1

Write down what should happen before you test anything



List every property: main site, subdomains, shops, portals and apps



Pick the page types that matter: home, product, forms, checkout, login, search



Map geographies, languages and the laws that apply to each



Write down what each consent state should allow, by category and jurisdiction

EXAMPLE EXPECTED-BEHAVIOR MATRIX (ONE GEOGRAPHY, OPT-IN RULES)

Script category	Accept all	Reject all	No action
Strictly necessary	✓	✓	✓
Analytics	✓	✗	✗
Advertising	✓	✗	✗

Step 2: Catalog and classify

STEP 2 OF 7

2

**Know what's actually there,
and why**



Inventory every script, vendor and cookie you find, page by page



Give each one a category, an owner and a business reason



Challenge anything filed as "Strictly Necessary" or "Functional"



Flag anything nobody recognizes

8%

say every script on their website is authorized (survey of 800)

69%

of 90 audited companies loaded a known tracker

Step 3: Check what loads before consent

STEP 3 OF 7

3

**Everything that fires before
a choice fired without
consent**



- 1 Start clean: new browser profile, no cookies, no stored consent
- 2 Open developer tools and record network traffic before touching the banner
- 3 Note every request and cookie set before a choice is made
- 4 Compare against your expected behavior for that geography

FROM A HEALTHCARE AUDIT



Step 4: Check the banner, controls and disclosure notices

STEP 4 OF 7

4

The "say it" job



The banner appears in the right geographies and languages



Choices are real and clearly presented, including reject where required



The privacy notice is easy to reach and matches the vendors you found



Visitors can change their preferences later, from any page

Check disclosures against what you found in step 2. Informed consent can't occur if visitors are not told who receives the data.

Step 5: Test every consent state

STEP 5 OF 7

5

Test each state separately,
against your expected
behavior



Accept all

only vendors your policy allows load



Reject all

no non-essential scripts load, on this page or the next



Withdraw

after accepting, then withdrawing, tracking stops and is not reset on the next page



GPC on

the opt-out is honored before any script runs



No action

pre-consent behavior stays controlled as the visitor browses

AUDITED COMPANIES THAT HONORED ONE SIGNAL, NOT BOTH

Honored Reject All, ignored GPC



Honored GPC, ignored Reject All



Step 6: Repeat across pages, geographies and languages

STEP 6 OF 7

6

One test is one page, one geography, one language, one consent state, on one day



Run the matrix, not a sample

Sampling is where blind spots live



Rerun after releases and tag changes

That's when consent breaks

1 day

of proof out of 365 days.

That is what an annual audit gives you.

Step 7: Document findings, fix and retest

STEP 7 OF 7

7

**Write it down so someone
can act on it**



For every finding, record:



What fired, where, and in which consent state, geography and language



Evidence: network capture, screenshot and timestamp



Owner, priority and the fix



Retest date and result

Keep the history. Questions often arrive months later.

If you only have today's results, you can't answer questions about March. Lawyers tend to pick targets where the evidence is easy to get, so a good archive makes you a harder target.

Track whether the program is improving

INSTEAD OF REPORTING

"The banner is on every page"



"Our CMP is configured"



"We did an audit last quarter"



"We haven't had complaints"



TRACK

Drift rate

pages where consent behavior changed since the last test

Violations per 10 to 20 webpages / per consent state

Time to fix

from finding to verified successful retest

Evidence coverage

properties with a complete record for each required period of time

These are the numbers your legal team, your DPO and your board can use.

AUDIENCE POLL 2 OF 3

Could your team run this full audit by hand today, across every page type, geography, language and consent state?

A Yes, and we already do it on a regular schedule

B Yes, but only once or twice a year

C Only for a sample of pages or regions

D No, we don't have the time or people

Submit your answer in the poll panel. Responses are anonymous.

What it takes by hand: the matrix multiplies

EACH AUDIT COVERS



AUDITS PER YEAR



7,800 audits × 40 scenarios

Consent states: pre-consent, reject, accept and re-opt-in

312,000

scenario reviews a year, at about 8.25 minutes each

Illustrative model. Your numbers will differ; the shape won't.



What manual audits can cost

\$2.68M

Total cost of manual audits by humans per year.

CONSENT AUDITS / YEAR

7,800

10 pages/screens each

MANUAL HOURS REQUIRED / YEAR

42,900

5.5 hours per audit

FULL-TIME EMPLOYEES NEEDED

22+

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

Illustrative model. Your numbers will differ.

Tools you can use today

Manual, one page at a time

Automated, many pages



Browser developer tools and a GPC-enabled browser

Free, manual, one page at a time



Tag manager preview and debug modes

See what fires and why



Your CMP's scans and reports

Useful, but it's grading its own work



Website crawlers and scanners

Find scripts and cookies across many pages



Scripted tests and AI agents

Repeat consent-state tests and capture evidence

Each of these does one part of the job.

AUDIENCE POLL 3 OF 3

Have you built any of your own tooling for consent testing?

A Yes: automated tests, scripts or agents that run on a schedule

B Partly: scripts or spreadsheets we run by hand

C No, we use our CMP's or other vendors' tools

D No, nothing yet

Submit your answer in the poll panel. Responses are anonymous.

WHAT'S DIFFERENT IN 2026 AND 2027

From a tool to a harness

A tool can run a point-in-time scan, but a harness keeps the whole process running.

A harness manages tools in a consolidated process. It's the brain that knows what matters to you, has control of the right tools, and runs them without someone having to stitch them together by hand.

The three parts of a consent verification harness



Context

Your scope, your expected-behavior matrix, the laws that apply to you, your inventory and your past findings, organized so they can be found

Steps 1 and 2



Data and Tools

Scanners, your CMP, browser tests and verification agents, each doing one job well

Steps 3 to 6



Automation

Tests that run on releases and schedules, findings routed to owners, retests and evidence kept

Keeps step 7 going

HOW THE PARTS MAP TO THE SEVEN STEPS

1 Scope

2 Catalog

3 Pre-consent

4 Banner

5 Consent states

6 Matrix

7 Evidence

Build it yourself or use a supported setup



Build

Connect scanners, scripts and agents yourself, and maintain the integration as your site, your vendors and the rules change.

You're in the systems integration business: a custom agent for each job, kept working together while everything underneath changes.

or



Supported

Use a supported setup that runs the process end to end and keeps the evidence and reporting for you.

Judge it against the same checklist you would use for anything you build, ours included.

Either way:

Context

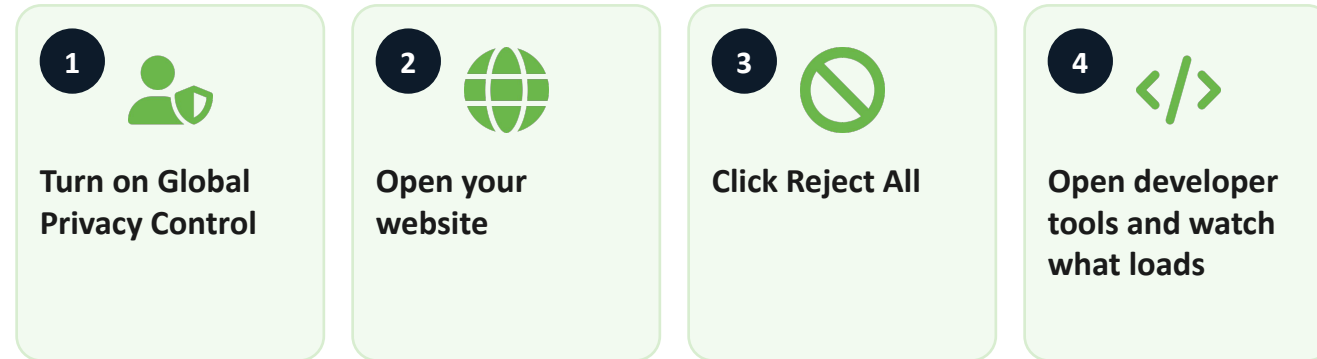
Tools

Automation



Audit Your CMP Today

Complimentary Website Privacy Consent Assessment



Want to see the full picture on your own site? Get your complimentary privacy consent assessment.



A banner records the choice. Make sure your site obeys it.



feroot.com/privacy-assessment

Questions and answers

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

DISCUSSION TOPICS

- Where to start if you can only do one step this month
- Testing withdrawal and Global Privacy Control
- What evidence a regulator or plaintiff's attorney asks for
- How often to retest
- Building your own tests versus using a vendor



Thank you for joining!

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

livewebconteam@iapp.org

For more information: www.iapp.org

This webinar was brought to you by Feroot Security · feroot.com/iapp