

• RESEARCH

The Execution Gap

Why privacy programs need to monitor every tag on their site, especially the ones they don't know about.

Contents

01	Summary	3
02	What is the execution gap?	3
03	One site, many rulebooks	5
04	Five failure patterns	7
05	The second front: private lawsuits	11
06	What orders and settlements now require	12
07	A quarterly checklist for privacy teams	13
08	How DataTrue helps	13
09	Sources and method	14

EXHIBITS

Exhibit A: The execution gap	4
Exhibit B: One site, many rulebooks	6
Exhibit C: Five failure patterns and what to test	7
Exhibit D: The opt-out signal is not honored	8
Exhibit E: Sensitive data travels in the tags	10

Summary

Recent privacy enforcement keeps finding the same problem. Companies offered visitors a choice about tracking, and the tags on their websites did not follow it.

Most of the companies in the cases below had a privacy notice, a consent banner or an opt-out form in place. The trouble was what happened behind it. Tags kept sending data after an opt-out, ignored a browser privacy signal, or carried details that should never have left the site.

THE FIGURES:

More than \$9.3 million

in penalties and fines across the eight California actions on opt-outs and tracking listed in Sources, from 2022 to 2026 (DataTrue's tally of the published amounts). The largest of the eight, \$2.75 million, came in Disney's February 2026 settlement with the California Attorney General.

13 high-traffic websites

in a July 2024 New York Attorney General review, which found marketing tags that stayed active after visitors used the sites' privacy controls.

\$12.5 million

that AARP agreed to pay to settle a class action over the Meta Pixel on its video pages.

A tag monitoring system

that TaxAct must now run under an August 2026 settlement with the Connecticut Attorney General, one that regularly scans its website.

This paper sets out five failure patterns behind these cases, the rules in the US, Canada and beyond that make them costly, and a short checklist a privacy team can use this quarter. Each pattern can be tested on a live website before a regulator or a plaintiff tests it.

This paper is general information about public enforcement records. It is not legal advice. Teams should confirm with their own counsel how these rules apply to them.

What is the execution gap?

The execution gap is the distance between what a website promises visitors about their privacy and what the tags on that website actually send.

A privacy notice, a consent banner and an opt-out form are promises. The tags decide whether those promises are kept.

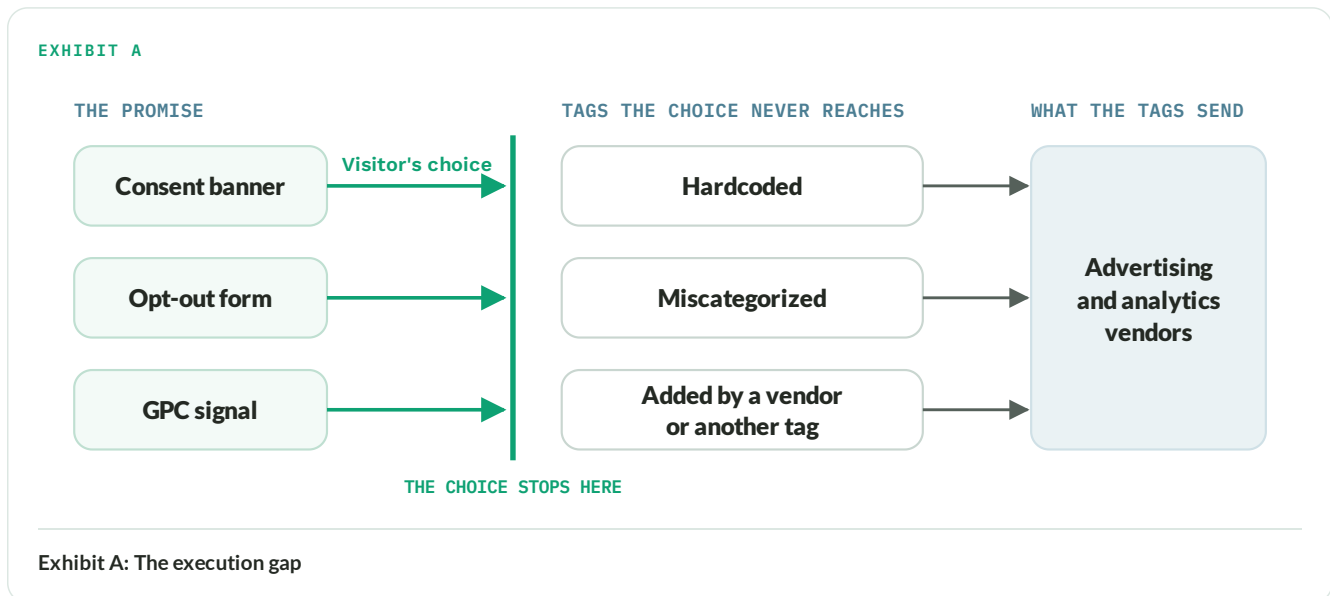
A few terms come up throughout this paper:

Tag:	a small piece of code, usually supplied by an advertising or analytics vendor, that runs when a page loads and sends information about the visit to that vendor. A pixel is one common kind of tag.
Tag manager:	a tool many teams use to add, organize and control their tags in one place.
Consent management platform (CMP):	the tool behind a cookie or consent banner. It records each visitor's choice and passes it to the tags it controls.
Opt-out preference signal:	a setting in a visitor's browser that asks every site they visit not to sell or share their data. Global Privacy Control (GPC) is one such signal. The browser sends it with every page request.

What regulators found when they looked

In July 2024 the New York Attorney General said a review of 13 high-traffic websites, mostly well-known e-commerce sites, found marketing tags that stayed active after visitors used the sites' privacy controls, often because tags were miscategorized or hardcoded. All of the companies fixed the issues.

Those two causes are worth understanding. A **miscategorized** tag is filed under the wrong category in the CMP, for example as "essential", so it keeps running when a visitor opts out. A **hardcoded** tag is written straight into the page code, outside the tag manager, so the CMP never gets a say over it.



The tag doesn't have to be yours

Many of the tags on an enterprise website were never added by the privacy team. Marketing teams, agencies and vendors add them. Some tags load other tags, so a site can end up running tags nobody on the privacy team has reviewed.

A one-time check goes stale

Enterprise sites change often. Each release, campaign or new vendor can add a tag or change what an existing one sends. A consent setup that passed review in the spring can be out of step by the summer. The only way to know what the tags do today is to keep checking, on the live site, in every consent state visitors can choose.

Code on a site can also change without its owner knowing. British Airways is a security case, and it shows how far that can go. In 2020 the UK Information Commissioner's Office (ICO) fined British Airways GBP 20 million after attackers changed JavaScript on its own website in 2018 and skimmed payment card details from about 429,000 people. The ICO found BA's security measures inadequate.

One site, many rulebooks

A global enterprise answers to different privacy and consent rules in each US state, each Canadian province and each country it serves, and one website usually serves all of them. A tag setup that is acceptable in one place can be a problem in the next.

United States

More than a dozen states have comprehensive consumer privacy laws, and more take effect each year.

In California and most US states with privacy laws, advertising use of personal data is opt-out. People have the right to stop it, and a GPC signal counts as that request in the states that recognize it. California has required businesses that sell or share personal information to treat an opt-out preference signal such as GPC as a valid opt-out since March 2023.

Nine states now require businesses to honor browser opt-out signals directly: California, Colorado, Connecticut, Delaware, Minnesota, Montana, New Hampshire, New Jersey and Oregon. Texas, Maryland and Nebraska recognize them, with conditions, through an authorized agent. And since January 2026, California requires businesses to give people a way to confirm that their opt-out request was processed, including requests sent through GPC.

Canada

Quebec's Law 25 has a rule aimed at tracking technology. Section 8.1 of Quebec's Law 25 requires telling people up front when technology can identify, locate or profile them, and how to turn those functions on. Quebec's regulator, the Commission d'accès à l'information (CAI), reads this as meaning those functions must be off by default until the person activates them.

The stakes in Quebec are real. Administrative penalties reach CAD 10 million or 2% of worldwide turnover, penal fines reach CAD 25 million or 4%, doubled for repeat offences, and individuals can sue, with punitive damages of at least CAD 1,000 for intentional or gross fault.

Federally, under PIPEDA, Canada's privacy regulator says express consent is needed when information is sensitive, when a use is outside what people would reasonably expect, or when there's a meaningful risk of significant harm. Otherwise implied consent may be enough. Its findings show how that plays out:

Home Depot (2023).

Canada's Privacy Commissioner found Home Depot sent hashed customer emails and in-store purchase details to Meta, through Meta's Offline Conversions tool, without valid consent. Home Depot stopped and agreed to get opt-in consent in future. There was no fine.

Google (2014).

The Commissioner found Google's remarketing used a user's health-related browsing to target ads without the express consent sensitive health information requires. Google agreed to fix its practices.

Tim Hortons (2022) and TikTok (2025).

Joint findings by the federal commissioner and Quebec's CAI, with British Columbia and Alberta, found an app tracking users' location through a third-party SDK even when the app was closed (Tim Hortons), and tracking and profiling for targeted ads without meaningful consent (TikTok). Both companies agreed to changes.

None of these findings carried a fine. The federal commissioner cannot fine under PIPEDA. Quebec's Law 25 penalties, described above, give the CAI powers the federal commissioner does not have.

A site that serves both

A website that follows the US opt-out model for visitors in Texas may fall short of the off-by-default expectation for visitors in Quebec. Monitoring has to test every consent state the site offers, in every region it serves.

EXHIBIT B

OPT-OUT

Most US states with privacy laws

OFF BY DEFAULT

Quebec

As the CAI reads Law 25

CONSENT FIRST

EU

CONSENT FIRST, WITH A STATISTICS EXCEPTION

UK

For some analytics cookies, since February 2026

Exhibit B: One site, many rulebooks

Beyond North America

172 countries have data privacy laws, according to an academic count published in April 2025. Many also have specific rules on cookies and tracking, and regulators enforce them:

France.

In September 2025 the CNIL fined Shein's operator EUR 150 million, finding that advertising cookies were placed as soon as visitors arrived on shein.com and that cookies were still placed or read after visitors clicked "Refuse all".

United Kingdom.

The ICO reprimanded Sky Betting and Gaming's operator in September 2024, finding that for about eight weeks in early 2023 roughly 40 third-party marketing cookies, set through a MediaMath pixel, were placed before visitors made a cookie choice.

Australia.

In June 2026 Australia's Privacy Commissioner found that fertility clinic Monash IVF and telehealth provider Medmate breached the Privacy Act by collecting visitors' health information through Meta, TikTok and other tracking pixels without consent and using it to retarget ads.

Five failure patterns

The cases fall into five patterns, and each one can be tested on a live website. For each, we set out what it looks like, the cases behind it, and what to check.

EXHIBIT C

Pattern	Cases	What to test
1. The opt-out signal is not honored	Sephora, Tractor Supply, PlayOn	Load key pages with GPC on and record what each tag sends
2. The banner or form doesn't stop the tags	Healthline, Tractor Supply, New York AG review	Opt out, then walk the site and record every tag that still fires
3. The opt-out covers too little	Disney	Opt out once, then check other devices, logged-in sessions and properties
4. The opt-out path adds friction or delay	Honda, Todd Snyder, Ford	Count the steps and time the opt-out against the accept path
5. Sensitive data travels in the tags	Healthline, BetterHelp, Cerebral, Monument, TaxAct	Inspect tag payloads for health terms, financial values and personal details
Exhibit C: Five failure patterns and what to test		

1. Is the opt-out signal being honored?

A visitor turns on GPC in their browser. The site's advertising tags keep firing and keep sending data to third parties anyway. Nothing on the page looks wrong, so the problem can run for months.

EXHIBIT D

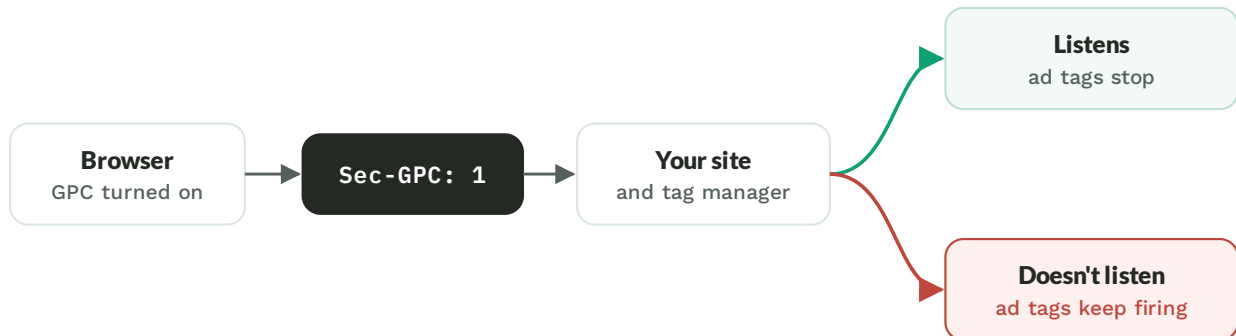


Exhibit D: The opt-out signal is not honored

Sephora.

In 2022 Sephora agreed to pay \$1.2 million in penalties to settle California Attorney General allegations that third-party tracking on its website and app amounted to a sale of shopper data, which it did not disclose and did not stop when shoppers opted out through GPC.

Tractor Supply.

The California Privacy Protection Agency (CPPA) ordered Tractor Supply to pay a \$1.35 million fine. The order says its opt-out webform did not stop the third-party tracking technologies used for advertising, and that the site did not honor opt-out preference signals such as GPC until July 2024.

PlayOn Sports.

CalPrivacy, the CPPA's current name, ordered PlayOn Sports to pay a \$1.1 million fine. The order says ticket holders had to click "Agree" to tracking before they could use their tickets, were pointed to industry opt-out tools instead of PlayOn's own, and had their opt-out preference signals ignored.

WHAT TO TEST:

load key pages with GPC turned on. Advertising and data-sharing tags should stay off, and the site should give visitors a way to confirm the opt-out request was processed.

2. Does the banner or opt-out form actually stop the tags?

The banner records the visitor's choice. The form accepts the request. Behind them, the tags carry on as before, because they were never connected to the choice.

Healthline.

Healthline agreed to \$1.55 million in civil penalties in a July 2025 settlement with the California Attorney General, which said its consent banner did not disable tracking cookies, sharing continued after opt-out, and article titles suggesting a diagnosis were shared with advertisers.

Tractor Supply.

As above, the CPPA's order says the company's opt-out webform did not stop the third-party tracking technologies used for advertising.

The New York review.

The New York Attorney General's review of 13 high-traffic websites found marketing tags that stayed active after visitors used the sites' privacy controls, often because tags were miscategorized or hardcoded.

WHAT TO TEST:

reject or opt out, then move through the site the way a visitor would. Record every tag that still fires and every request that still goes to a third party.

3. Does the opt-out cover everything it should?

The opt-out works, but only in one place. It applies to one device, one app or one brand, while the same person is still tracked everywhere else.

Disney.

Disney agreed to \$2.75 million in civil penalties in a February 2026 settlement with the California Attorney General, which said opt-outs, including GPC, applied only to a single Disney streaming service or device instead of the whole account.

WHAT TO TEST:

opt out once, then check the same account on other devices, in logged-in sessions, and across the brand's other sites and apps.

4. Is the opt-out path harder than the accept path?

Accepting takes one click. Opting out takes several, or asks for details the business doesn't need, or takes weeks to process. Regulators treat that friction as a failure in its own right.

Honda.

The CPPA ordered Honda to pay a \$632,500 fine. The order describes a cookie tool where accepting all took one click and opting out took at least two, and ad-tech sharing without the contract terms the CCPA requires.

Todd Snyder.

The CPPA ordered Todd Snyder to pay a \$345,178 fine after its privacy portal failed to process opt-out requests for 40 days and it required people to verify their identity before opting out.

Ford.

CalPrivacy ordered Ford to pay a \$375,703 fine after it required people to verify their email address before it would process requests to opt out of the sale or sharing of their data.

WHAT TO TEST:

count the clicks to opt out against the clicks to accept, check what information the opt-out asks for, and time how long it takes for tags to actually stop.

5. Is sensitive data traveling in the tags?

Some tags send more than a page view. Page titles, form fields and URLs can carry health conditions, financial details or email addresses straight to an advertising platform. Personal data of this kind is often called personally identifiable information (PII).

EXHIBIT E EXAMPLE, FICTIONAL

1. ON THE PAGE

clinic.example/cardiology/book

Cardiology appointment

Specialty

Cardiology

Date

Book

2. WHAT THE ADVERTISING PIXEL SENDS

```
GET adplatform.example/collect
?event=form_submit
&page_url=/cardiology/book
&page_title=Cardiology appointment
&specialty=Cardiology
```

3. WHERE IT GOES

Advertising platform

Exhibit E: Sensitive data travels in the tags

Healthline.

As above, article titles suggesting a diagnosis were shared with advertisers, according to the California Attorney General.

BetterHelp.

Under a 2023 Federal Trade Commission (FTC) order, BetterHelp paid \$7.8 million for partial consumer refunds and is banned from sharing health data for advertising. The FTC alleged it shared email addresses, IP addresses and intake questionnaire answers with Facebook, Snapchat and others.

Cerebral.

Under a 2024 FTC order, Cerebral agreed to pay nearly \$5.1 million in refunds over its cancellation practices and a \$10 million civil penalty, suspended after \$2 million was paid. The FTC said it gave nearly 3.2 million consumers' sensitive information to platforms such as LinkedIn, Snapchat and TikTok through tracking tools.

Monument.

In 2024 Monument settled FTC and Department of Justice allegations that it sent health information on as many as 84,000 users to advertising platforms through pixels and Meta's Conversions API. The order includes a \$2.5 million civil penalty, suspended because the company could not pay.

TaxAct.

Connecticut Attorney General William Tong announced a \$275,000 settlement with TaxAct in August 2026. The Attorney General said TaxAct disclosed rounded income, refund and other tax data to Meta and Google through tracking technologies from 2018 to 2022.

WHAT TO TEST:

fill in forms with made-up test details and inspect what each tag sends, in plain text and hashed. Check page titles and URLs on sensitive pages for terms that should never reach a third party.

The second front: private lawsuits

Regulators are one source of exposure. Class actions over website tracking are another. AARP's \$12.5 million settlement, below, is larger than any of the eight California actions in this paper. Many rely on older laws written for phone calls and video rentals, now applied to tags.

The laws plaintiffs use

California Invasion of Privacy Act (CIPA).

A California wiretap law, enforced through private lawsuits and as a crime. A person injured by a violation can sue for the greater of \$5,000 per violation or three times their actual damages, and the statute says they don't have to show actual damages. The \$5,000 figure is a statutory amount per violation. Courts decide what, if anything, is owed.

Video Privacy Protection Act (VPPA).

A federal law on sharing people's video viewing history, now applied to pixels on pages with video.

What a closed case looks like

AARP agreed to pay \$12.5 million to settle a class action alleging that the Meta Pixel on AARP.org video pages sent members' identities and viewing activity to Meta in violation of the VPPA. The court granted final approval in February 2026.

This paper names companies only in matters that are closed. Other website tracking class actions are still open, and we leave them out until they are final.

Not every suit succeeds

Some of these cases fail or are dropped. A federal court dismissed a CIPA complaint against Laird Superfood with leave to amend in June 2026. The plaintiff refiled, Laird moved to dismiss again, and in September 2026 he voluntarily dismissed the case.

Even a suit that fails costs time and legal fees to defend. The better position is knowing what the tags do before a demand letter arrives.

What orders and settlements now require

Orders and settlement terms show what regulators and courts expect a working privacy program to include, and one settlement now requires ongoing monitoring of tags.

TaxAct and Connecticut (August 2026).

TaxAct must run a tag monitoring system that regularly scans its website and obtain two independent audits.

BetterHelp (2023).

Under its FTC order, BetterHelp is banned from sharing health data for advertising.

Monash IVF and Medmate (Australia, 2026).

Both must stop using the pixels until they have consent and notice in place, and destroy the pixel data where the law allows.

Across these terms the expectation is the same. A company should know what its tags are doing and be able to show it. TaxAct's settlement goes further and requires regular scans. A privacy team that already monitors its tags can answer that question before anyone asks.

A quarterly checklist for privacy teams

These ten questions turn the five patterns into checks a team can run on its own live site. Each one should have an answer backed by a test result.

The Execution Gap: quarterly checklist

- ☐ 01 With GPC turned on, which tags still send data to advertising or data-sharing platforms?
- ☐ 02 Does the site give visitors a way to confirm their opt-out request was processed, as California now requires?
- ☐ 03 After a visitor clicks "Reject all" or submits the opt-out form, which tags still fire?
- ☐ 04 Which tags run outside the tag manager, and who added them?
- ☐ 05 Is every tag in the consent tool filed under the right category?
- ☐ 06 Does an opt-out carry across devices, logged-in sessions, apps and sister sites?
- ☐ 07 How many clicks does opting out take compared with accepting, and how long until tags actually stop?
- ☐ 08 What do tags send from forms, search boxes and sensitive pages? Check for health terms, financial values and email addresses, plain or hashed.
- ☐ 09 Do session replay or live chat tools load before a visitor makes a choice?
- ☐ 10 Do the answers change by region? Test as a visitor from each US state, province and country the site serves.

DATATRUE.COM

Run the checks after every major release as well as each quarter. Keep the results. A dated record of what the tags did is the evidence a privacy team needs when a regulator or plaintiff asks.

How DataTrue helps

DataTrue gives privacy, marketing and analytics teams the tools to test what their tags actually do on the live site, and to keep testing on a schedule.

-  **Coverage scans** crawl the whole site and report what tags are present and how they behave on each page, including tags running outside the tag manager.

- ✓ **Journey simulation** walks a defined path, such as a signup or a checkout, in each consent state: no choice, accepted, rejected and GPC on. It checks what each tag sent at each step.
- ✓ **Payload inspection** reads what each tag actually sends, so the team can see when personal data or sensitive terms are going to a third party.
- ✓ **Alerts** come from scheduled tests. The team is alerted when a test result changes, for example when a tag fires after an opt-out.
- ✓ **Pre-publish testing** is also available, checking draft tag manager containers before they go live.

DataTrue doesn't make a site compliant. Compliance depends on each organization's data, agreements and legal judgments. DataTrue gives teams the tools to test what their tags actually do, so they can become compliant and stay compliant. Teams should confirm with their own counsel how these rules apply to them.

Sources and method

Every case in this paper comes from DataTrue's enforcement registry, checked against the primary order, press release or court record. Case descriptions follow the wording of those records. Only closed matters are named. Where a company denied wrongdoing, we say so. Figures are current as of September 2026.

THE CALIFORNIA TALLY

The "more than \$9.3 million" figure is DataTrue's sum of the published amounts in these eight actions.

Company	Enforcer	Date	Amount (USD)
Disney	California Attorney General	February 2026	2,750,000
Ford	CalPrivacy	March 2026	375,703
PlayOn Sports	CalPrivacy	March 2026	1,100,000
Tractor Supply	CPPA	September 2025	1,350,000
Healthline	California Attorney General	July 2025	1,550,000
Todd Snyder	CPPA	May 2025	345,178
Honda	CPPA	March 2025	632,500
Sephora	California Attorney General	August 2022	1,200,000
Total			9,303,381

OTHER CASES

- US regulators: [New York Attorney General website privacy review](#), [BetterHelp](#), [Cerebral](#), [Monument](#), [TaxAct](#) and [Connecticut](#)
- Private lawsuits: [AARP](#), [Laird Superfood](#) (C.D. Cal. 2:25-cv-12407)
- Canada: [Home Depot](#), [Google](#), [Tim Hortons](#), [TikTok](#)
- Outside North America: [Shein \(CNIL\)](#), [Sky Betting and Gaming \(ICO\)](#), [British Airways \(ICO\)](#), [Monash IVF and Medmate \(OAIC\)](#)

LAWS AND COUNTS

- [11 CCR 7025](#), California's rule on opt-out preference signals
- [CalPrivacy, Things to know before 2026](#), on confirming opt-outs
- California Penal Code sections 631, 637.2 and 638.51 (CIPA)
- Quebec's Act respecting the protection of personal information in the private sector (Law 25), sections 8.1, 90.12 and 93.1, and PIPEDA guidance from the Office of the Privacy Commissioner of Canada
- [Graham Greenleaf, "Global Data Privacy Laws 2025: 172 Countries"](#), Privacy Laws & Business International Report, April 2025

See what your tags do today, free

We set up tests for your domain, run them against key pages (your home page, a content page, a form, a sensitive or high-value page, and your privacy policy) from the regions you serve, and send you a plain-English report within two business days, scored against eight checks:

1 Is Global Privacy Control honored?

With GPC turned on, advertising and data-sharing tags should stay off.

2 What fires before a visitor makes a choice?

Where consent comes first, only essential tools should load before a choice.

3 Do tags stop after an opt-out?

After a visitor rejects or opts out, advertising and data-sharing tags should drop to zero.

4 Are any tags running outside your tag manager?

Hardcoded tags are often the ones nobody on the team knows about.

5 Is personal data leaking through forms?

We type made-up test details into a form and check whether any of it reaches a third party.

6 Does session replay or live chat load before consent?

7 What tags are on your site?

A full inventory of every tag we find on your domain, by vendor.

8 Is anything firing twice?

Duplicate analytics page views and placeholder IDs distort your data.

[Request your free scan →](#)

[Book a meeting with our team](#)

ABOUT DATATRUE

DataTrue gives privacy, marketing and analytics teams the tools to test what their tags actually do on the live site, and to keep testing on a schedule.

