The browser blind spot:

Why data privacy often comes too late

Monday, March 23, 2026

08:00–09:00 PST
11:00–12:00 EST
16:00–17:00 CET

Welcomes and Introductions

Gareth Bowker

Head of Security Research

jscrambler

The browser blind spot:

Why data privacy often comes too late

Where governed data actually begins

Gareth Bowker

Head of Security Research

jscrambler

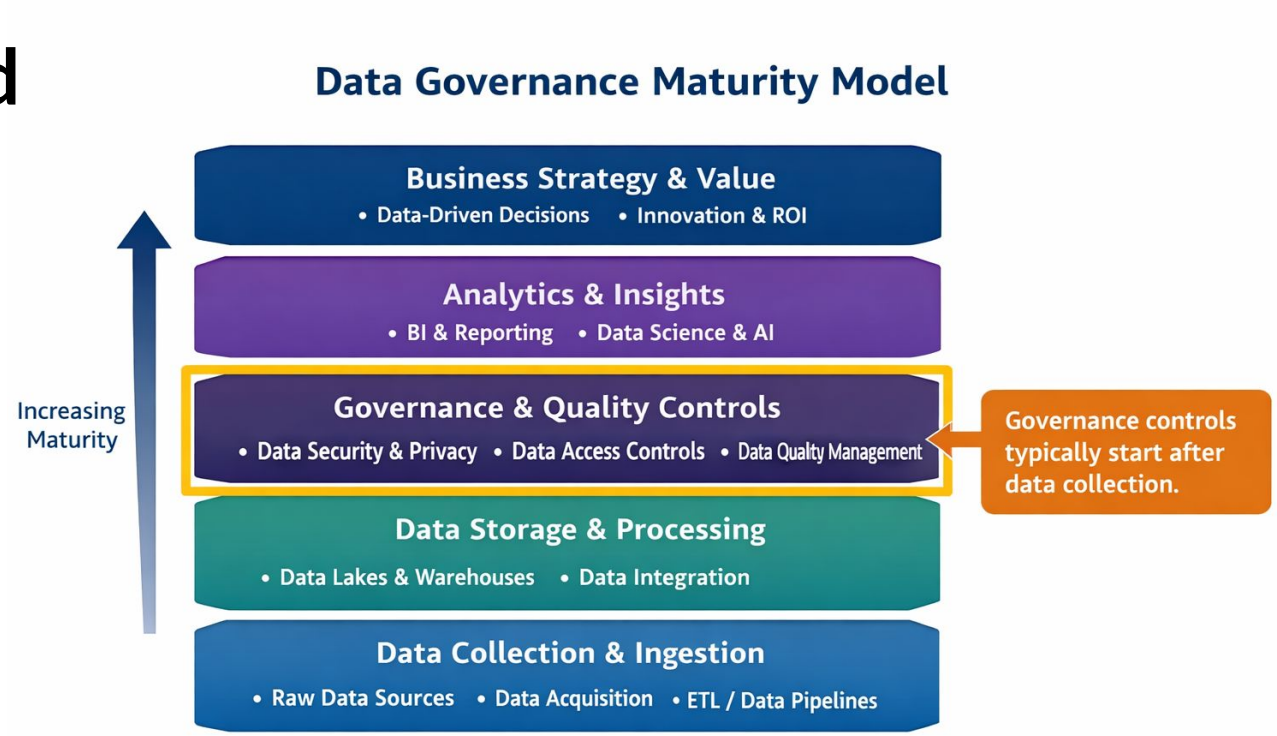
Privacy programs have matured significantly

Organizations have invested heavily in:

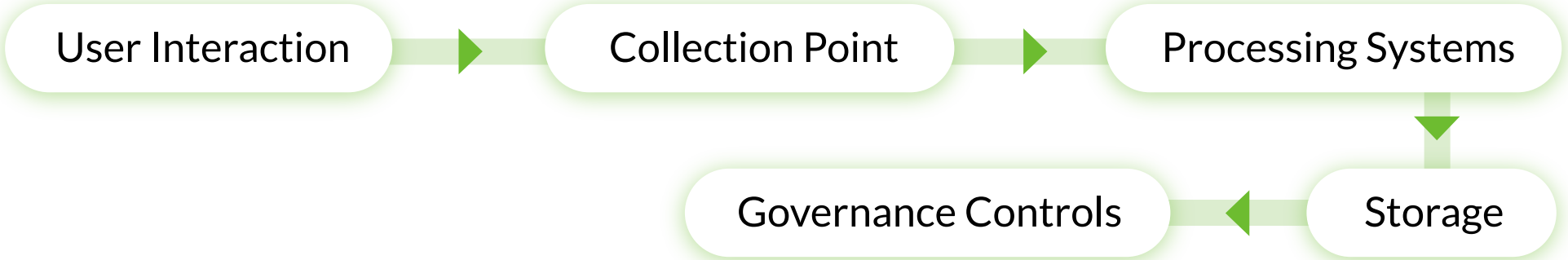
- ✔ Data mapping
- ✔ Privacy notices
- ✔ Consent management
- ✔ Vendor risk management
- ✔ Governance frameworks

But an important question is emerging:

Where does governed data actually begin?



How privacy governance is typically structured:



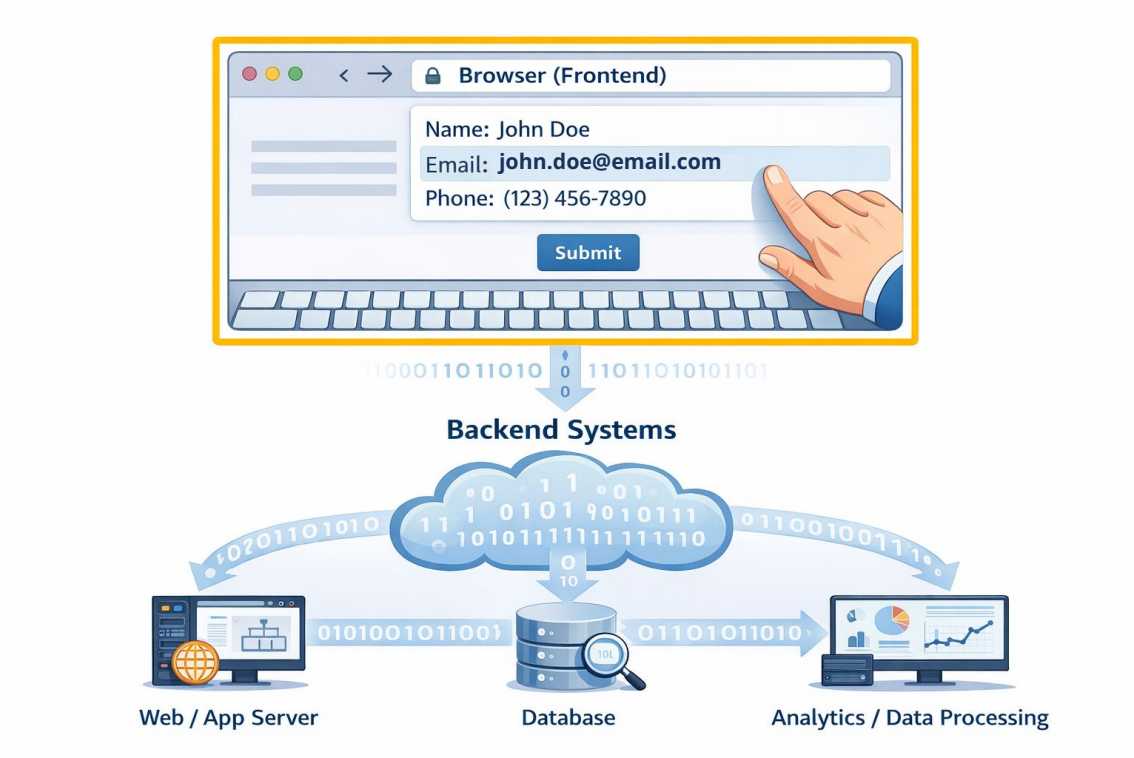
This works well for **systems of record.**

In modern digital services:

Data is created during interaction.

- ✔ typing into forms
- ✔ search queries
- ✔ clicks
- ✔ navigation behavior

This activity happens **inside the browser** before enterprise systems receive it.



What 'client-side' actually means

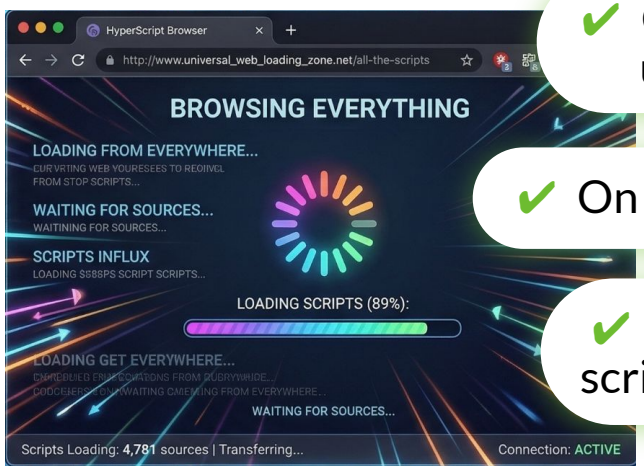
Your Servers

Server-side

- ✔ Code runs on infrastructure you control
- ✔ You see the logs
- ✔ You set the rules

User's Web Browser

Client-side

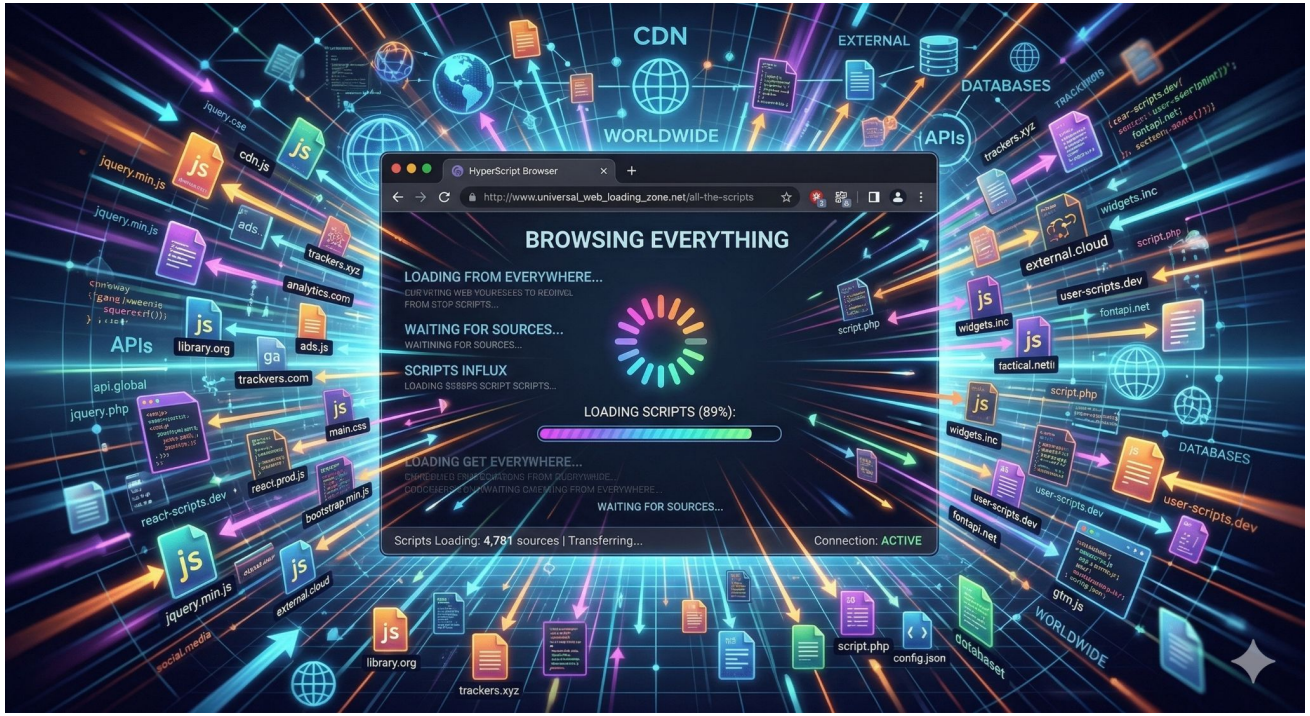


- ✔ Code runs in the user's browser
- ✔ On their device
- ✔ Alongside every other script on the page

When we say 'client-side technology,' we mean code that executes in this environment, not on your servers

What happens when a user visits your website

- **92%** of websites use third-party JavaScript
- Over **50%** of e-commerce website JS comes from third parties
- Each of these scripts can observe user interactions on the page - they share the same execution environment

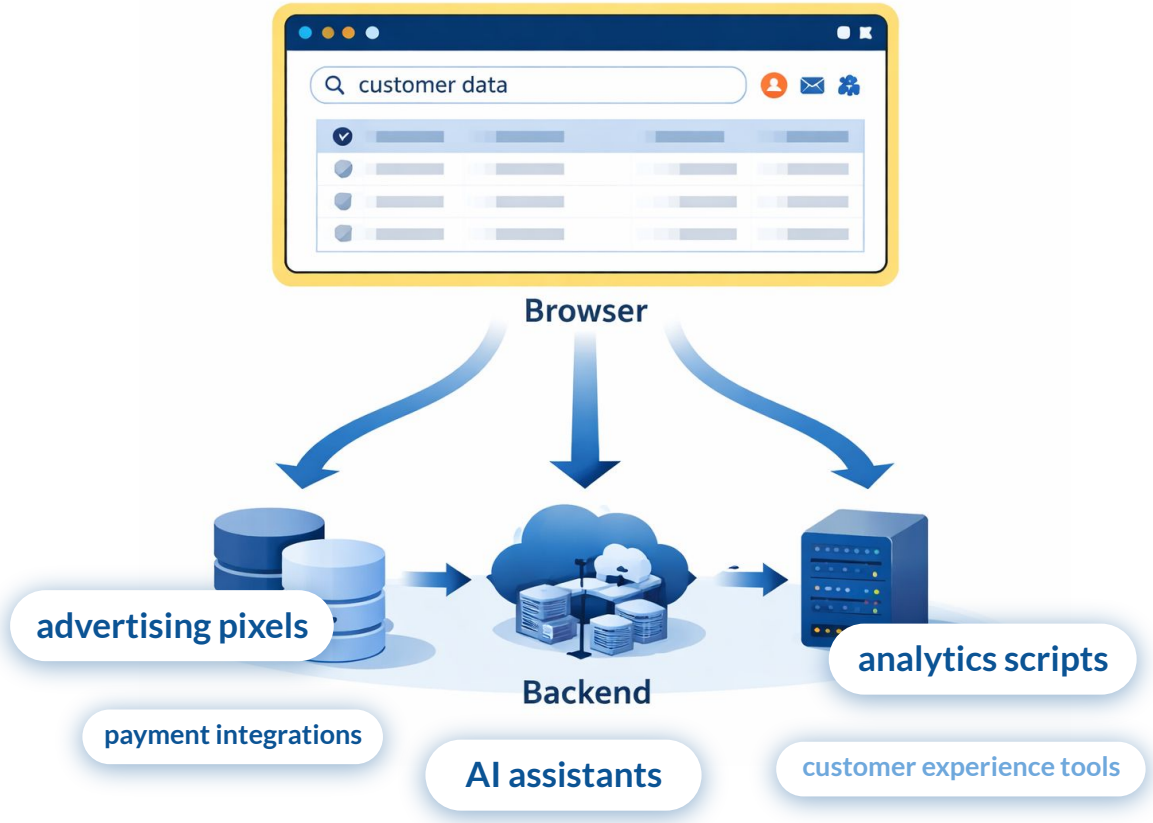


The browser has unique access to user interaction.

It can observe:

- ✔ form entries
- ✔ clicks and navigation
- ✔ behavioral signals
- ✔ sensitive and competitive data

And it executes multiple client-side technologies simultaneously.



What Privacy Programs Often Expect.

Data collected after submission

- Name
- Email address
- Payment information
- Physical address
- Account identifiers

Captured in enterprise systems.

What May Be Accessible During Interaction

Data actually collected before and after submission:

- email as it typed
- phone numbers
- physical address fields
- search queries
- product selections
- authentication events
- form entries before submission

Why this matters

Implications for:

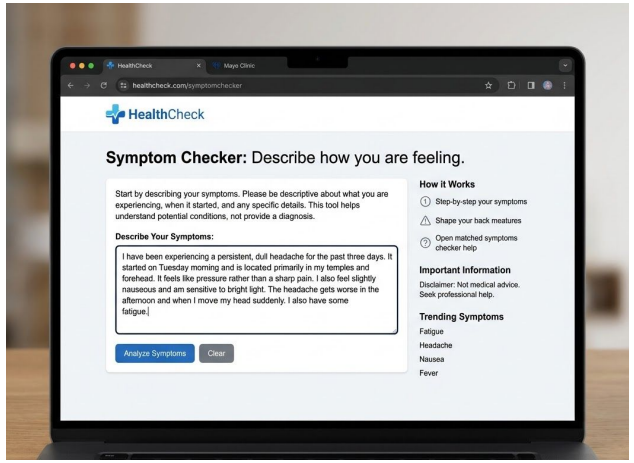
- ✔ Privacy compliance
- ✔ Competitive intelligence exposure

The consent timing gap

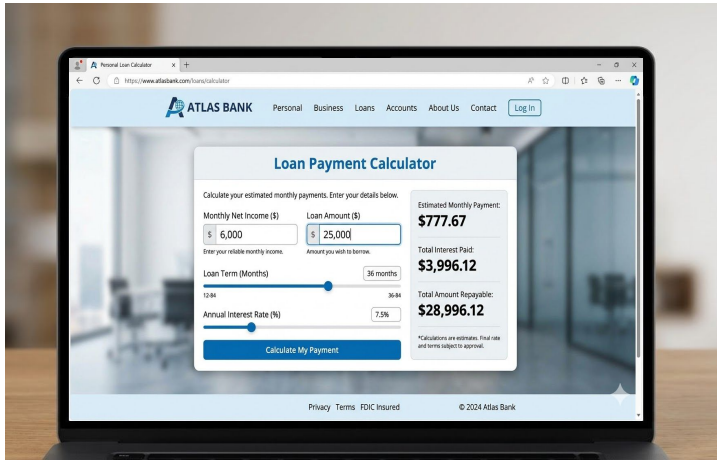
User lands on page	scripts begin executing
Consent banner appears	user is already being observed
User interacts with banner	interaction itself may be observed
User consents (or doesn't)	governance "starts" here
User submits form	this is what most privacy programmes consider "collection"

The governance assumption is that collection begins at step 5. The technical reality is that observation begins at step 1.

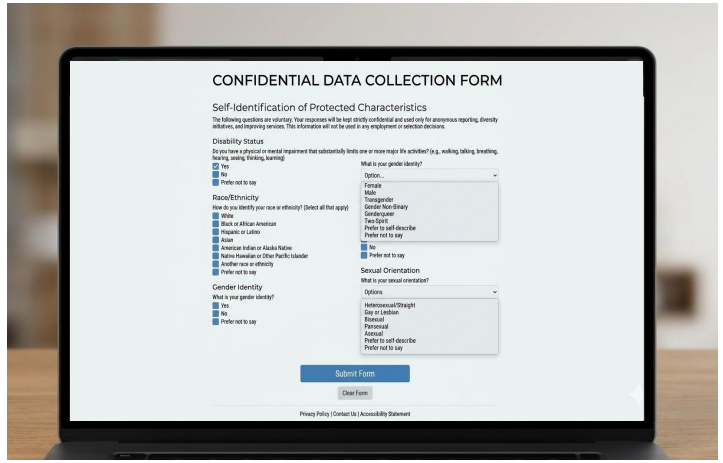
What's accessible during interaction



Healthcare Portal



Financial Services



Employment Application

Research into client-side technologies shows:

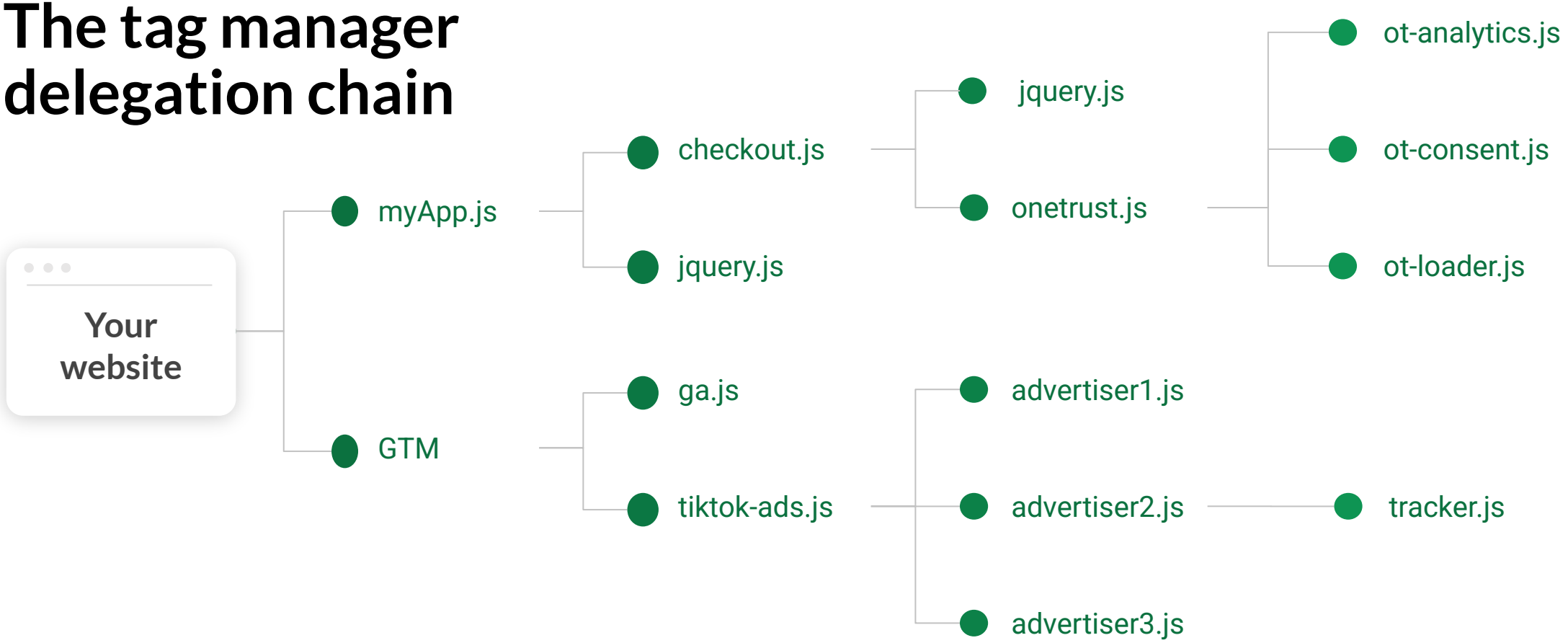
Many websites deploy **dozens of scripts and pixels.**

These technologies may observe:

- ✔ page activity
- ✔ user interactions
- ✔ form field behavior
- ✔ navigation events

Often before server-side processing.

The tag manager delegation chain



Where vendor oversight gaps emerge

- **Contractual coverage:** DPAs may not exist for all scripts executing on your site, particularly piggyback scripts loaded by other vendors
- **Purpose limitation:** A script deployed for analytics may also collect data for ad targeting, exceeding the purpose you disclosed to users
- **Data transfer:** Client-side scripts may transmit interaction data to servers in jurisdictions not covered by your transfer impact assessment
- **Vendor inventory accuracy:** Your Article 30 records list server-side processors. Do they include *every script* running in the browser?

Beyond personal data: competitive exposure

The data observable in browsers isn't just PII, it includes:

- Search queries revealing product interest and intent
- Pricing page interactions showing price sensitivity
- Feature comparison behaviour
- Cart composition and abandonment patterns
- B2B: company identifiers, deal sizes, procurement signals

Third-party scripts with access to this data may serve multiple clients, including your competitors. This is a competitive intelligence exposure, not just a privacy risk

AI agents in the browser: a new governance surface

AI-powered tools increasingly run client-side:

- chatbots
- assistants
- copilots
- recommendation engines

These tools may:

- Observe page content and user interactions as input
- Process data locally in the browser or transmit to external APIs
- Operate under their vendor's privacy policy, not yours

KEY POINT

"If an AI tool on your site ingests user interaction data as input, is that reflected in your AI governance documentation?"

Emerging frameworks emphasize data traceability.

Focus on traceability and accountability. Jscrambler can help with visibility into which AI agents run on on their website.

Focus on governance of AI system inputs. Align execution with compliance.

Both highlight the need to understand:

Where data originates.

Privacy leaders may increasingly ask:

- ✔ **When is data first accessible?**
- ✔ **Which technologies operate in the browser?**
- ✔ **When does consent occur relative to exposure?**
- ✔ **What vendors have interaction-level access?**

Where should data enforcement start?

These questions strengthen **audit defensibility.**

Questions for your next vendor assessment

1. "Do we have a complete inventory of all scripts executing on our web properties — not just server-side processors?"
2. "Which of these scripts can observe form field input before submission?"
3. "Do our DPAs cover the data these scripts can technically access, or only what we intend them to collect?"
4. "Has our consent implementation been tested to confirm it loads and captures choice before other scripts begin observation?”
5. "Are browser-deployed AI tools included in our AI governance register?"

Scoping a client-side audit

1. Inventory
2. Map data access
3. Consent timing
4. Contractual review
5. Documentation alignment

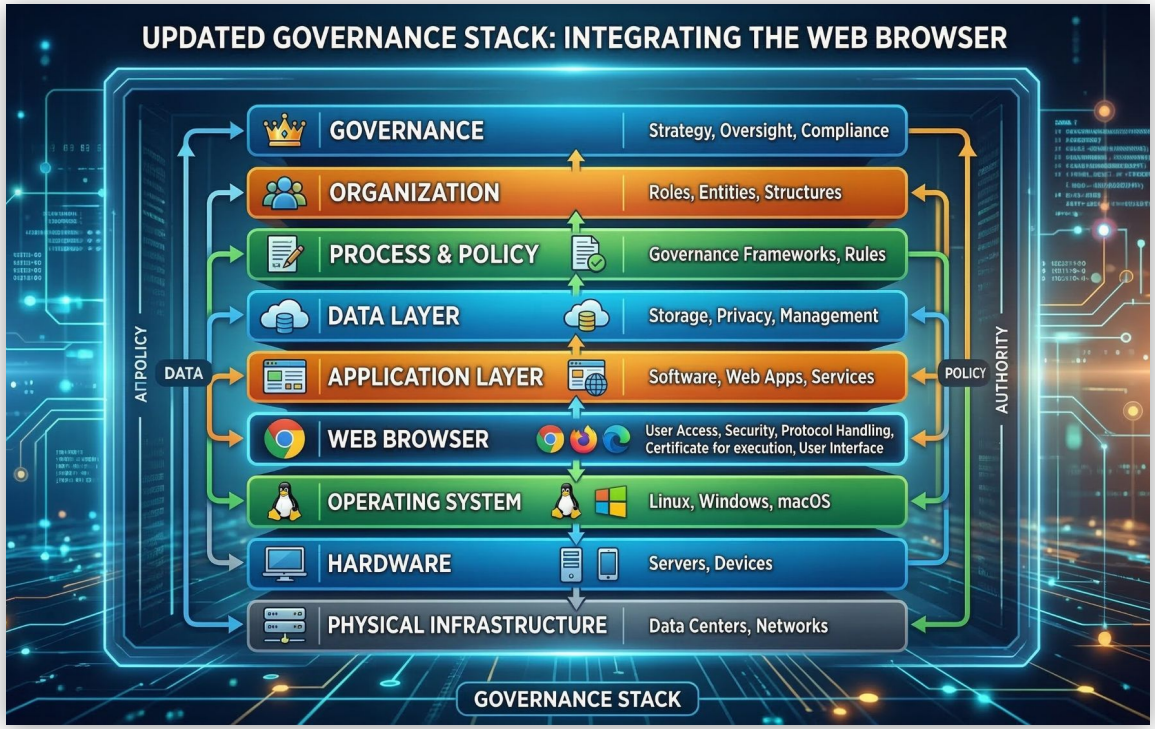
KEY POINT

"This isn't a one-time exercise. Script inventories change as marketing and product teams deploy new tools."

Leading organizations are beginning to focus on:

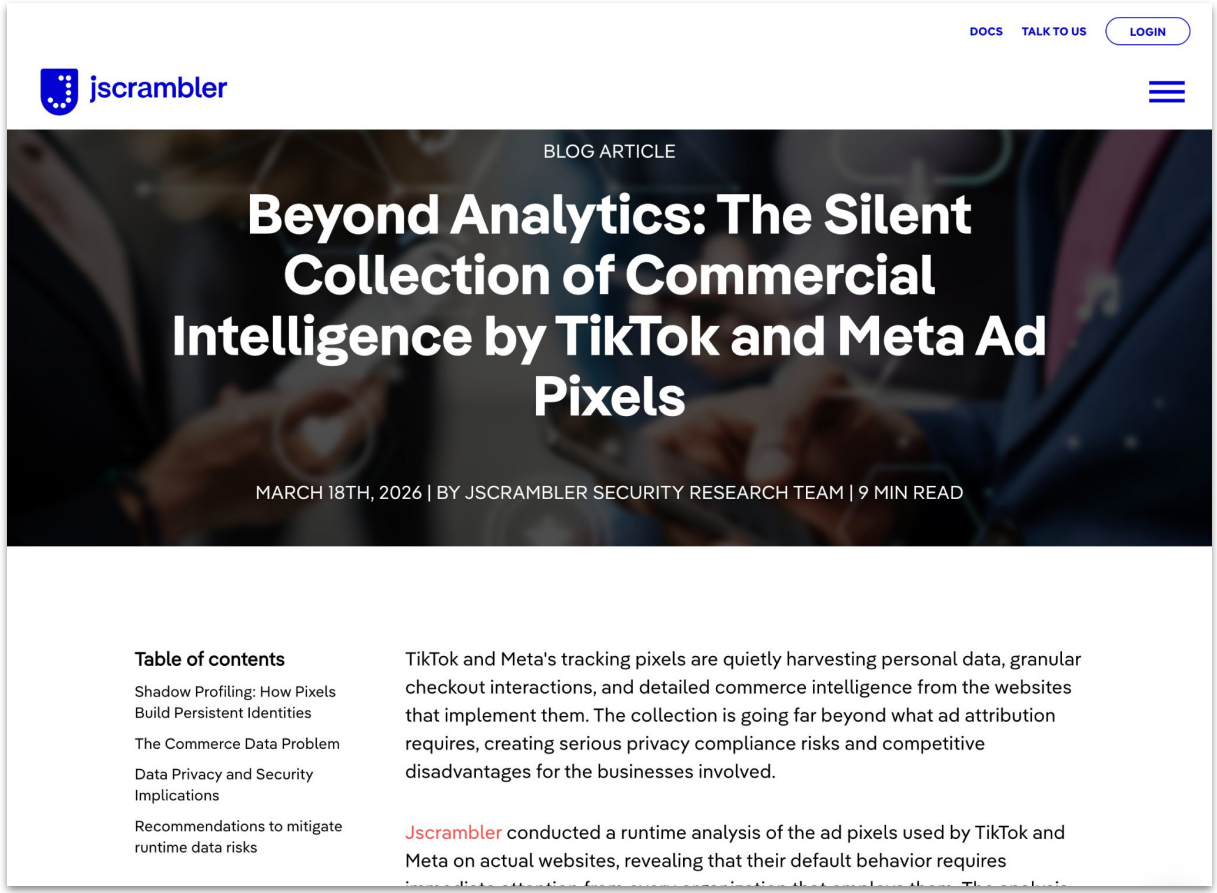
- ✔ **client-side visibility**
- ✔ **vendor inventory at the browser layer**
- ✔ **interaction-level data awareness**
- ✔ **real-time control of third-party scripts**

Aligning **technical reality with privacy commitments.**



1. The browser is a **privileged but low-visibility environment**
2. Third-party client-side technologies complicate **vendor oversight**
3. Sensitive data may be accessible **during interaction at the point of creation**
4. Interaction data includes **personal data and strategic competitive signals**
5. Privacy governance increasingly begins **in the browser**

Latest Research



Latest research into how Meta and TikTok collect data

https://jscrambler.com/blog

How Jscrambler can help

Observability: Gain visibility into which scripts are running on your website, what they're accessing, and where data is going

Governance: Control what feeds external models by restricting data access for AI-powered scripts. Convert policies into technical enforcement for GDPR, CCPA, and PCI DSS v4

Enforcement: Enforce least-privilege access to DOM elements and form fields during live sessions. Block unauthorized third-party data access and exfiltration in real time.

Questions and Answers

Gareth Bowker

Head of Security Research

jscrambler

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/AbBPvZ8Mar

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**