





Online Trackers and Privacy: Managing Technology, Transparency, and Control

Why businesses use online trackers

- 
Enhance User Experience
 Improve website functionality and customization.
- 
Improve Security
 Detect and prevent fraudulent activities.
- 
Targeted Advertising
 Personalize advertising based on user interests.
- 
Data Collection Purposes
 Personalized content, marketing strategies, fraud prevention.

What are trackers?

Online trackers are technologies used by websites and apps to collect data about user interactions. These trackers record details such as browsing habits, time spent on a webpage, clicked links, and more.

Common organizational or business purposes for using online trackers:

- 
Website analytics: Understanding how users interact with websites helps businesses improve their user experience and marketing strategies.
- 
Targeted advertising: Tracking technologies allow advertisers to show personalized ads based on user interests and browsing behavior.
- 
Fraud detection and security: Tracking can be used to identify and prevent suspicious activity, such as credit card fraud or online hacking.
- 
Market research: Companies use tracking data to learn about consumer behavior and preferences.
- 
Personalization: Some websites, advertising, and social media platforms use tracking to personalize the user's experience by remembering their preferences and settings.






Types of data collected


First-party data
 Collected directly from user interactions with the site.

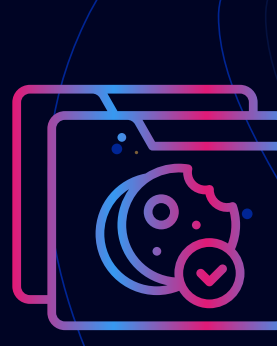

Third-party data
 Collected by external entities.

Common online trackers





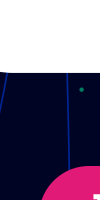
Trackers come in several forms, each serving distinct purposes and collecting different types of data. Here are some common types:

- 
Cookies: These are small files stored on a device that track the user's website activities.
- 
Pixels: Also known as web beacons, these are tiny, invisible images embedded in web pages or emails. They are used to track user interaction and are popularly used for advertising as well.
- 
Browser fingerprinting: A more advanced method that gathers data about the user's device (like screen resolution, installed fonts, or browser type) to create a unique profile for tracking, even without cookies.
- 
Embedded scripts: Code snippets that track user behavior within a website.
- 
Web beacons: Embedded images that track when a page is loaded.





Types of cookies

- 
Session cookies: Temporary, deleted after a browser is closed.
- Persistent cookies:** Remain on the device for a set time.
- First-party cookies:** Created by the visited website.
- Third-party cookies:** Created by external entities like advertisers.

Privacy regulations impacting ad tech vendors

- 
EU's ePrivacy Directive
 - Requires **clear, informed consent** before using non-essential cookies (e.g., for ads or analytics).
 - Consent must be **opt-in** and cannot rely on pre-ticked boxes.
- 
UK GDPR & PECR
 - Similar to the EU, mandates **explicit consent** for non-essential cookies.
 - Enforced by the **ICO**, emphasizing transparency and user control.
- 
US State Privacy Laws
 - Require businesses to provide clear **opt-out options** for targeted ads and data collection.
 - Focus on **user rights** and easy-to-access privacy controls.
- 
Quebec's PPIPS
 - Demands **opt-in consent** for cookies and profiling technologies.
 - French-first cookie banners** are required to ensure language compliance.
- 
Saudi Arabia's PDPL
 - Obligates businesses to get **explicit consent** for data processing through cookies.
 - Users must **be informed** about data purposes and any third-party sharing.

Practical tips for Ad Tech management

- 
Be Transparent: Clearly explain what your trackers do and why.
- 
Get Valid Consent: Use opt-in methods where required—no pre-ticked boxes!
- 
Respect Regional Rules: Adapt your tracker practices for each market.
- 
Monitor Regularly: Conduct audits to stay compliant with evolving laws.


Simplify your online tracker technologies with TrustArc's all-in-one solution!

Our suite of tools is designed to make managing online tracker technologies seamless and scalable.


Cookie Consent Manager
 Effortlessly manage geo-dynamic cookie disclosures, end-to-end tracker monitoring, and compliance reporting.


Website Monitoring Manager
 Automate regular vendor tracker scans to ensure your site complies with **GDPR, CCPA, and FTC** guidelines.


Consent & Preference Manager
 Centralize and sync all customer consents across your systems and ensure precise control over first-party data collection and tracker management.


DAA AMI Validation
 Validate your addressable media identifiers and demonstrate compliance with industry standards, safeguarding consumer privacy and bolstering trust with partners and customers.

Take control of your trackers and protect user privacy.

[REQUEST A DEMO](#)