Journal of Recent Trends in Computer Science and Engineering (JRTCSE)
Vol. 13, No. 1, January - February, 2025, PP. 31-34.
ISSN: 2322-0872
https://jrtcse.com
DOI: https://doi.org/10.70589/JRTCSE.2025.13.1.5

The Demise of Third-Party Cookies and Beacons

Sunil Kishor Pathak,
https://www.linkedin.com/in/sunilkpathak/

Abstract

Third-party cookies and web beacons have long been central to personalized marketing and user behavior analytics. However, escalating privacy concerns and stringent regulations, such as GDPR and CCPA, have shifted the digital landscape, prompting browsers to phase out support for these tracking mechanisms. This article explores the business need for third-party cookies and beacons, the privacy challenges they pose, the influence of regulations, and the implications of their decline. Finally, it delves into the future of marketing in a privacy-first era.

Keywords: Third-party cookies, web beacons, personalized marketing, user behavior analytics, privacy concerns

Pathak, S.K. (2025). The demise of third-party cookies and beacons. *Journal of Recent Trends in Computer Science and Engineering (JRTCSE)*, *13*(1), 31–34.

DOI: https://doi.org/10.70589/JRTCSE.2025.13.1.5

1. Introduction

Effective marketing hinges on understanding the target audience. For industries such as automotive, precision is critical in reaching the right customers. For example:

- A car manufacturer launching a new electric vehicle (EV) may aim to target individuals who research EVs, visit car showrooms, or browse automotive content online.
- Simultaneously, businesses seek insights into customer behavior, such as who interacts with their ads, what drives purchases, and how their campaigns perform.

To address these needs, businesses rely on third-party cookies and web beacons, tools that enable detailed tracking and analytics. These mechanisms allow businesses to:

1. Track user behavior across multiple websites.
2. Deliver personalized advertisements and recommendations.
3. Measure ad performance and engagement.

Despite their advantages, third-party cookies and beacons have raised significant privacy concerns, leading to regulatory actions and changes in browser policies.

2. The Need for Third-Party Cookies and Beacons

2.1 Third-Party Cookies

Third-party cookies are created by domains other than the one a user is visiting. They enable:

- **Cross-Site Tracking**: Tracking user activity across multiple websites.
- **Behavioral Targeting**: Building profiles to serve personalized ads.
- **Performance Analytics**: Measuring the success of marketing campaigns.

Example Workflow:

1. A user visits abc.com, which embeds a script from xyz.com.
2. The script sets a cookie (xyz_id=12345), enabling xyz.com to track the user across other sites.

2.2 Web Beacons

Web beacons, also called tracking pixels, are small invisible elements embedded in web pages or emails. They work by triggering a request to a server, collecting user metadata such as IP address, browser details, and referrer.

Use Cases:

- **Web Pages**: A beacon embedded in a product page can track views and user interactions.
- **Emails**: A beacon can track whether a recipient opened the email or clicked a link.

3. Privacy Concerns

The extensive tracking capabilities of third-party cookies and beacons raise several privacy issues:

3.1 Data Collection Without Consent

- Many users are unaware of the data being collected or how it is used.
- Consent mechanisms are often vague or inadequate.

3.2 Overreach in Data Collection

- Detailed user profiles, including sensitive data, are created without explicit permission.
- Tracking extends beyond user expectations, such as monitoring browsing history across unrelated sites.

3.3 Transparency and Control

- Users have limited visibility into the data collected and shared.
- Deleting or managing this data is often challenging for users.

3.4 Security Risks

- Third-party scripts and beacons can introduce vulnerabilities, including Cross-Site Scripting (XSS) and data leakage.
- as the cookie's domain.

4. Regulatory Influence

Regulations like GDPR and CCPA aim to protect user privacy by formalizing how third-party data collection should occur. Key provisions include:

- **User Consent**: Data collection requires explicit user consent.
- **Purpose Limitation**: Data can only be used for the purposes stated at the time of consent.
- **Transparency**: Organizations must disclose how user data is collected, stored, and shared.

Despite these regulations, non-compliance has been widespread, further exacerbating privacy concerns.

5. Browser Actions and the Decline of Third-Party Tracking

Recognizing the risks posed by third-party technologies, browsers have taken steps to protect user privacy:

- **Google Chrome**: Plans to phase out third-party cookies by 2024, introducing privacy-friendly alternatives like the Privacy Sandbox.
- **Apple Safari**: Blocks third-party cookies using Intelligent Tracking Prevention (ITP).
- **Mozilla Firefox**: Enforces Enhanced Tracking Protection (ETP) to prevent cross-site tracking.

By deprecating third-party cookies and restricting beacon capabilities, browsers aim to:

1. Reduce exposure of user data to third parties.
2. Align with privacy regulations and user expectations.
3. Foster a trust-based digital ecosystem.

6. Implications for Businesses

Challenges

- The loss of cross-site tracking limits businesses' ability to deliver highly targeted ads.
- Companies reliant on third-party data must overhaul their strategies.

7. Conclusion

The decline of third-party cookies and beacons signifies a paradigm shift in digital marketing. Businesses must adapt to privacy-first approaches, prioritizing transparency and user consent while exploring innovative alternatives for personalization and analytics. In this evolving

landscape, balancing user privacy with marketing effectiveness will be key to sustainable success.

References

Pathak, S.K. (2024a). "User Identification Through First-Party Cookies." Journal of Recent Trends in Computer Science and Engineering (JRTCSE). DOI: https://doi.org/10.70589/JRTCSE.2024.5.6.

Pathak, S.K. (2024b). "Exploring User Identification with Third-Party Cookies." Journal of Recent Trends in Computer Science and Engineering (JRTCSE). DOI: https://doi.org/10.70589/JRTCSE.2024.5.8.

Pathak, S.K. (2025c). "Web Beacons and Online User Identification." Journal of Recent Trends in Computer Science and Engineering (JRTCSE). DOI: https://doi.org/10.70589/JRTCSE.2025.13.1.3.

Mozilla Developer Network (MDN). "HTTP Cookies." Retrieved from https://developer.mozilla.org/.

GDPR Overview. Retrieved from https://gdpr-info.eu/.

CCPA Overview. Retrieved from https://oag.ca.gov/privacy/ccpa.

Google Privacy Sandbox. Retrieved from https://privacysandbox.com/.

Apple Intelligent Tracking Prevention (ITP). Retrieved from https://developer.apple.com/documentation/webkit/intelligent_tracking_prevention