IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Innovating Beyond Cookies: Brand Communication and Media Personalization in a Privacy-First Era

Sharanya Goel
Student
Strawberry Fields, Chandigarh

Research Question: To what extent does the decline of third-party cookies impact brand communication and media personalization, and how can advertisers innovate to succeed in a privacy-first era?

Abstract

The decline of third-party cookies marks a watershed moment in digital advertising, disrupting long-established practices of audience tracking and targeted personalization. Once central to brand communication strategies, third-party cookies have been increasingly restricted due to concerns from consumers, regulatory pressures, and browser limitations. This paper examines the extent to which the loss of cookies impacts brand communication and media personalization, while evaluating the innovative pathways advertisers are adopting in response. Through the analysis of strategies such as first-party data ecosystems, contextual advertising, Google's Topics API, data clean rooms, and server-side tracking, the study highlights how privacy-respecting approaches can sustain relevance without undermining trust. Case studies, including Burger King's *Whopper Detour* campaign, demonstrate the potential of creative, non-intrusive models to achieve both scale and engagement. Ultimately, the paper argues that the shift to a privacy-first era is not a limitation but an opportunity for brands to cultivate more transparent, responsible, and impactful communication.

Keywords: third-party cookies, first-party cookies, privacy-first marketing, brand communication, contextual advertising

Introduction

Imagine casually glancing at a pair of leather boots online. You don't click "buy," nor do you add it to the cart. Yet, in the days that follow, those boots seem to shadow your every click: they appear on news sites, in your social media feeds, even on blogs entirely unrelated to fashion. This digital specter is not a coincidence but the result of a background mechanism that quietly orchestrates much of our online experience: *the HTTP cookie.*

Devised initially to keep users logged in and websites functioning smoothly, cookies have become the backbone of contemporary digital marketing. They fall into two categories. *First-party cookies* originate from the site you're directly visiting; they store session information, such as your language preference and the items in your cart, ensuring a seamless browsing experience (Riley, 2022). In contrast, *third-party cookies* are set by external domains embedded within a site – ad networks, social widgets, tracking pixels – to follow your activity across multiple websites. In doing so, they build detailed behavioral profiles that enable highly targeted advertising (Drake, 2021).

For years, this invisible web of third-party cookies underpinned advertisers' ability to deliver personalized content and measure campaign impact with precision. However, that era is drawing to a close. The General Data Protection Regulation (GDPR) and similar privacy laws have forced companies to rethink data collection practices; browsers have begun restricting or blocking third-party cookies altogether (ADMA, 2022). The result is a fundamental disruption: brands can no longer rely on surreptitious cross-site tracking to understand or influence consumer behavior. In light of these changes, a critical question emerges: **To what extent does the decline of third-party cookies impact brand communication and media personalization, and how can advertisers innovate to succeed in a privacy-first era?**

This paper argues that although the end of third-party cookies disrupts traditional methods of behavioral targeting, it also opens the door to more ethical and creative strategies. By turning attention to contextual advertising and building strong first-party data systems based on transparency and user consent, brands can still offer personalized experiences more responsibly. Rather than being a setback, this evolution can deepen consumer trust, transforming privacy constraints into a foundation for genuine connection rather than intrusive surveillance.

Understanding Cookies: First-Party vs. Third-Party Cookies

When you load a website and it greets you by name or remembers your last search, you're experiencing the subtle work of cookies. But not all cookies are the same. First-party cookies belong to the site you've intentionally opened. They track only what happens on that domain, whether you've clicked "remember me," chosen dark mode, or filled part of a form, and then they disappear, usually when you close your browser or after a short interval (LaFleur, 2022). Third-party cookies, however, come from external services integrated into a page's code, such as ad

networks, social widgets, and analytics scripts. These trackers follow you across multiple sites, gathering your clicks and time spent into a comprehensive profile that advertisers use to tailor their messages.

The lifespan of these cookies reflects their missions. A first-party cookie might vanish within hours or days, perfectly aligned with its purpose of preserving the continuity of a single session (Nilakshi, 2021). Third-party cookies are designed to persist, sometimes for months, so that an item you once glanced at can reappear in ads long after your initial visit, as if it were waiting for you.

In marketing circles, this distinction holds significant importance. First-party cookies quietly enhance site functionality without raising red flags; they're the friendly guide that remembers your preferences. Third-party cookies, by contrast, are the cartographers of your online behavior, mapping every turn and pause to deliver precise, cross-site targeting. However, as privacy regulations tighten and browsers clamp down on these persistent trackers, brands must rethink personalization, shifting toward consent-driven data and contextual relevance instead of tracking users across the web (Dodt, 2020).

The Role and Decline of Third-Party Cookies in Advertising and Personalisation

Third-party cookies have been the foundation of targeted online marketing for over a decade. Tiny data files, installed by third-party domains such as ad networks, enable cross-site tracking. In contrast to first-party cookies, which save information on the website a user visits, third-party cookies track users' activity across sites.

This network enables advertising systems such as Google Ads and Facebook Ads Manager to serve highly targeted campaigns. For example, a person looking for running shoes might subsequently find ads for the same product on news sites, video sites, and social networks (Wagner, 2018). Called retargeting, this tactic improves consumer response by reiterating user interest. Behavioral information gathered from third-party cookie data also enables advertisers to segment audiences, such as frequent flyers or students, and tailor content to suit their needs. These techniques significantly reduce the cost of acquiring customers and improve the efficiency of advertising at scale.

However, the same systems of monitoring that enable personalization also raise significant privacy concerns. The majority of users have long been unaware of how much of their activity is being tracked or how they are being used. Public alarm particularly grew in response to political developments, such as the 2016 U.S. presidential election and the UK's Brexit referendum, in which targeted digital campaigns had been deployed to influence public opinion. The Cambridge Analytica affair, although centered on first-party Facebook data, revealed how users' personal data might be used to gain influence without users' express consent (Singer, 2018).

As Shoshana Zuboff (2019) aptly puts it, *"You are not the product. You are the discarded carcass. The actual product is your behavior—forecasted, altered, and marketed.*"

The mass backlash resulted in broad regulatory reform. The European Union enacted the General Data Protection Regulation (GDPR) in 2018, with stringent regulations regarding data consent and use. GDPR requires websites to obtain informed user consent before collecting personal information, including data from cookies (Bond, 2012). Users were also afforded the right to access, correct, or have their data erased. Non-compliance can result in annual global revenue penalties of up to 4%. Furthermore, in 2020, California enacted the California Consumer Privacy Act (CCPA) into law. Less inclusive than the GDPR, the CCPA provided consumers with the right to access what information was being gathered and the right to opt out of its sale. The law brought about the now ubiquitous "Do Not Sell My Personal Information" functionality on sites based in California (Finkelstein, 2020).

Technology firms also made internal adjustments to react to increasing pressure. Apple's App Tracking Transparency (ATT), introduced with iOS 14.5 in 2021, requires apps to obtain consent before tracking individuals across websites and apps. Most users opted out. Meta (the parent firm of Facebook) accounted for a $10 billion loss in 2022 due to less effective ads and diminished access to tracking data. Browsers started following similar policies. Safari and Firefox brought default third-party cookie blocking. Google, after some delays, has now pledged to remove third-party cookies entirely from Chrome by the end of 2025. With Chrome's market share leadership, this is a turning point away from third-party tracking on the open web.

Third-party cookie phase-out is a sign of a larger shift in the way digital advertising works. A decade and more of dark data collection practices have created increasing pressure for user opt-in, transparency in ethics, and platform responsibility. Brands that do not change are not only risking regulatory blowback but also reputational loss and a loss of trust from their customers (Poddębniak, 2024). This shift also presents an opportunity to rebuild the ecosystem on more sustainable terms. It requires the industry to confront long-standing questions: How much data is necessary? Can personalization coexist with privacy? Is it possible to deliver relevant digital experiences without constant surveillance?

Navigating the Privacy-First Era: Innovative Solutions and Strategies

Escalating demands for consumer privacy have catalyzed the development and adoption of innovative, more privacy-centric data strategies among advertisers and marketers. One of the primary shifts is towards *first-party data collection*, which refers to the data that brands can gather directly from users through logins, subscriptions, purchases, services, or on-site engagement (Bajaj, 2024). This approach not only ensures consent but also enhances data accuracy and compliance with privacy laws such as GDPR and CCPA. For instance, agencies and brands that

implement robust first-party strategies can both reduce reliance on third-party cookies and deepen customer trust by offering value in exchange for data.

That being said, first-party data collection does have some challenges. It requires a high level of consumer trust and must deliver clear value (LiveRamp, 2025), as users are increasingly cautious about sharing personal information. These constraints drive marketers to blend first-party data with *contextual targeting*, a method that matches ads to the semantic content of a page rather than user-specific profiles (Johnson, 2025). Contextual ads align with privacy principles because they entail no collection of personal data or cross-site tracking. In a striking example, research by Seedtag and Lumen has found that contextual odds are 87% more likely to be viewed than standard ads (Auchterlonie, 2025). Another technique is the use of *data clean rooms*, which are secure, collaborative environments where aggregated and privacy-protected audience data can be matched and analysed without exposing any raw customer data to external parties. These enable joint marketing initiatives without compromising individual privacy. Additionally, *server-side tracking* is gaining traction. Unlike traditional browser-based tracking, server-side tracking processes data on the brand's own servers, offering enhanced control and compliance. When it is correctly implemented, it can reduce data leakage and enhance privacy, though it does still require rigorous regulatory oversight and transparent consent mechanisms.

A real-world case study that showcases how innovation and privacy can merge effectively is seen in Burger King's *'Whopper Detour'* campaign (2018) (Clark, 2024). The company utilized a geo-fencing approach by setting up virtual fences around McDonald's restaurants. When Burger King app users entered these areas, they were offered a one-cent Whopper, available for redemption only via the app. This campaign did not depend on browsing history or third-party data. Instead, it leveraged real-time contextual cues – something like a location in this instance – to provide timely and relevant offers (Black, 2019). The campaign was able to achieve more than 1.5 million downloads in just nine days (Koltun, 2019), topped both the Apple App Store and Google Play charts for days (Oputa, 2024), generated between 3.3 to 3.5 billion media impressions, tripled app base sales and delivered one of the highest foot traffic increases in recent years (Startup Stoic, 2024), and achieved a staggering ROI of 37:1 (Oputa, 2024). These outcomes illustrate that creative context strategies can very well rival and sometimes even outperform traditional behaviour-based campaigns while preserving privacy.

Together with contextual advertising, *cohort-based targeting* has been investigated as a compromise between relevance and privacy. Google's initial proposal, Federated Learning of Cohorts (FLoC), grouped users into categories based on their interests, as determined by recent browsing history, but did not directly identify them (R., 2021). The system was criticized for its lack of transparency and indirect ability to identify users. Its replacement, the Topics API, provides a simplified and privacy-conscious approach. It assigns the users a small number of general interest topics (e.g., "travel" or "technology") based on their browsing history, which participating

advertisers can subsequently use. Notably, the data are stored on the user's device, and the users are provided with the capability to view and control their topic preferences – a significant departure toward more user control.

Whereas context- and cohort-based strategies provide competing targeting paradigms, firms possessing strong first-party systems, such as Amazon and Netflix, have succeeded to a high degree in personalization without relying on third-party cookies. These sites gather rich behavior data directly from users acting within their own respective worlds, such as video history, search patterns, and buying profiles. Since this information is collected openly and stays under the control of the platform, it is safer and more compliant with privacy laws. All the while, it supports accurate recommendations and segmented content delivery that keep pace with consumers' expectations of relevance.

Overall, while the demise of third-party cookies poses operational hurdles, it has also driven innovation around privacy-aware advertising. For advertisers, this is both a limitation and an opportunity to redefine the world of advertising.

Conclusion

The loss of third-party cookies marks a significant shift in how online advertising operates. Brands have been relying on these cookies for years in order to track users across websites. As people became more aware of the volume of information that was being collected on them without their permission, and as major scandals like the Cambridge Analytica event were exposed, this model fell out of favor among regulators and consumers. With regulations like the GDPR and CCPA in place now, and browsers limiting third-party tracking, advertisers are being forced to adapt. Engaging customers is now more effort and capital-intensive. Still, these challenges have opened the door for new, privacy-first strategies that can help rebuild the relationship between consumers and brands.

This report charted a few such alternatives. Contextual advertising enables brands to target ads with content that users are already consuming, thereby implying a limited use of individual tracking. The Google Topics API enables targeting based on broad interests without requiring individual identification. Companies like Netflix and Amazon continue to flourish by collecting first-party data directly from users, with their consent, and utilizing it for personalizing experiences. There are other solutions, such as server-side tracking and clean rooms, that demonstrate how measurement can still be conducted in a manner that respects user privacy. Campaigns such as Burger King's Whopper Detour further illustrate how creative, non-intrusive strategies can achieve massive engagement without reliance on intrusive surveillance.

The task for advertisers now is to strike a balance between relevance and responsibility. Transparency and trust are becoming as critical as reach and efficiency. While data remains central to modern marketing, the ways it is collected, governed, and applied must evolve in line with shifting consumer expectations for privacy and control. Ultimately, the decline of third-party cookies is not a loss but a redirection. It represents an opportunity for brands to pursue more respectful, intentional, and impactful forms of communication. Rather than following users unwittingly, advertisers are now challenged to create environments where engagement is freely chosen and mutually beneficial. Those who embrace this privacy-first mindset will not only comply with regulation but also unlock new pathways to sustainable consumer trust and competitive advantage.

Bibliography

ADMA (2022). *What Third Party Cookies do and why they matter to data marketing*. [online] ADMA. Available at: https://www.adma.com.au/resources/what-third-party-cookies-do-and-why-they-matter-to-data-marketing

Auchterlonie, A. (2025). *Driving Privacy, Precision, and Performance with a First-Party Data Strategy*. [online] Seedtag.com. Available at: https://blog.seedtag.com/driving-privacy-precision-and-performance-with-a-first-party-data-strategy

Bajaj, S. (2024). *How Third-party Cookies Impact Brands: Adapt with New Strategies - Shiprocket*. [online] Shiprocket. Available at: https://www.shiprocket.in/blog/how-third-party-cookies-impact-brands/

Black, N. (2019). *Campaign of the Year: Burger King's 'Whopper Detour'*. [online] Available at: https://www.marketingdive.com/news/burger-king-whopper-detour-mobile-marketer-awards/566224/.

Bond, R. (2012). The EU e-privacy directive and consent to cookies. *The Business Lawyer*, [online] 68, pp.215–223. Available at: http://www.jstor.org/stable/23527086

Clark, P. (2024). *Inside the Burger King 'Whopper Detour' Marketing Campaign*. [online] Mediashower.com. Available at: https://mediashower.com/blog/burger-king-marketing-campaign/.

Dodt, C. (2020). *Cookies: an Overview of Associated Privacy and Security Risks*. [online] Infosec, Inc. Available at: https://resources.infosecinstitute.com/topic/cookies-an-overview-of-associated-privacy-and-security-risks/.

Drake, M. (2021). *What are HTTP Cookies?* [online] DigitalOcean. Available at: https://www.digitalocean.com/community/tutorials/what-are-http-cookies.

Finkelstein, J. (2020). *CCPA: What It Is and What It Means for Brands*. [online] AdRoll. Available at: https://www.adroll.com/blog/ccpa-what-it-is-and-what-it-means-for-brands.

Johnson, J. (2025). *Contextual Targeting: Reach New Users in the Era of Privacy*. [online] Edge226. Available at: https://edge226.com/contextual-targeting-tips-for-how-to-reach-new-users/

Koltun, N.B. (2019). *Campaign of the Year: Burger King's 'Whopper Detour'*. [online] Marketing Dive. Available at: https://www.marketingdive.com/news/burger-king-whopper-detour-mobile-marketer-awards/566224/

LaFleur, G. (2022). *First-party vs. third-party cookies: What's the difference?* [online] SearchCustomerExperience. Available at: https://www.techtarget.com/searchcustomerexperience/tip/First-party-vs-third-party-cookies-Whats-the-difference.

LiveRamp (2025). *8 Steps to Create a First-Party Data Strategy*. [online] LiveRamp. Available at: https://liveramp.com/blog/first-party-data-strategy/

Nilakshi, N. (2021). *What Exactly Are HTTP Cookies?* [online] CodeX. Available at: https://medium.com/codex/what-exactly-are-http-cookies-3d58b5386ebb.

Oputa, E. (2024). *Case Study: Burger King's Whopper Detour Campaign*. [online] Begine Fusion. Available at: https://www.beginefusion.com/post/case-study-burger-king-s-whopper-detour-campaign

Poddębniak, M. (2024). *'Cookieless Future' Is Just a Buzzword – Here Is all you need to know about the end of third-party cookies*. [online] Piwik PRO. Available at: https://piwik.pro/blog/the-end-of-third-party-cookies/.

R., K. (2021). *Google FLoC: a Third-Party Cookie Alternative - CookieYes*. [online] CookieYes. Available at: https://www.cookieyes.com/blog/what-is-google-floc/.

Riley, A. (2022). *What are First Party Cookies vs Third Party Cookies - Examples*. [online] Claravine. Available at: https://www.claravine.com/what-are-first-party-cookies/.

Seedtag (2024). *What the future of contextual advertising looks like in a privacy-first world*. [online] Digiday. Available at: https://digiday.com/sponsored/what-the-future-of-contextual-advertising-looks-like-in-a-privacy-first-world/.

Singer, N. (2018). What You Don't Know about How Facebook Uses Your Data. *The New York Times*. [online] 11 Apr. Available at: https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html.

Startup Stoic (2024). *How a 1-cent Whopper offer could turn into a marketing phenomenon?* [online] Startup Stoic. Available at: https://www.startupstoic.com/p/simple-1cent-whopper-offer-turn-marketing-phenomenon

Wagner, K. (2018). *Facebook ads: This is how the company uses your data for targeting*. [online] Vox. Available at: https://www.vox.com/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.