Addressing the Privacy and Security Concerns Associated with Tracking Cookies for Targeted Marketing: Policy Brief

Hassan Alshehri

Prof. Ben Woelk

Executive Summary

Over recent years, cookies have become a critical feature of online marketing, with businesses relying on them to promote their products. Mellet and Beauvisage (2020) define cookies as codes incorporated into web browsers to collect relevant information for personalizing web experiences. They are divided into two: first-party and third-party cookies. According to Deloitte (2020), first-party cookies are placed by website owners to analyze users' preferences and personalize their experiences, while third-party cookies are designed and set by outside parties other than the website owner. Their primary objective is to track, profile, personalize, and target website users for advertising (Deloitte, 2020). However, research indicates that third-party cookies pose the highest cybersecurity risks, considering that users are unaware of their owners, raising privacy and security concerns (Cinar & Ateş, 2022). This finding highlights the need for a public policy to protect users from privacy violations and security breaches. It suggests that a comprehensive analysis of this problem is needed to shed light on what policymakers can do to address it. For this reason, this policy brief critically analyzes challenges associated with third-party cookies to help policymakers develop an effective policy solution. Its audience includes lawmakers and the management of tech companies such as Google and other browser developers.

Context or Scope of Problem

Online marketing presents numerous benefits to advertisers, including an innovative way to personalize ads and make them appealing to the target audience. According to Sadeghpour and Vlajic (2021), these benefits have made this form of marketing the most prominent and cost-effective method of reaching a global customer base. However, the method's increased reliance on third-party cookies has raised significant security and privacy concerns among Internet users. It is worth noting that though cookies alone do not pose substantial security risks, they collect and keep information that unauthorized entities can access illegally. Sadeghpour and Vlajic (2021) argue that tracking cookies for targeted marketing has become so advanced that they can track internet users for a significant period and collect all the information regarding their website preferences. This trend has raised significant concerns among users due to fears of data breaches and unauthorized use of personal information by third parties (Cinar & Ateş, 2022).

Their primary concern regarding third-party cookies is that they are produced and used by different websites from those visited by the user, suggesting that there is a high possibility of users' personal data being used by other entities without their consent or knowledge. Despite the General Data Protection Regulation (GDPR) requiring users to give their consent, the manner in which these tracking cookies are processed and used implies that users have limited control over how the data collected from them is used and who uses it (Mellet & Beauvisage, 2020). To this end, they are usually exposed to constant ads, mostly from unknown and untrustworthy sources. Some of the details collected from users include internet usage behaviors, user location, shopping history, and device specifications. These details can pose significant privacy and security risks, considering that users have no control over their usage after consenting.

Policy Alternatives

The privacy and security concerns raised by users regarding the tracking of third-party cookies have prompted the development of numerous data protection laws across the globe. They include provisions allowing users to consent to cookies seeking to collect information from them. Tech companies like Google have also taken steps to address these concerns, including gradually phasing out third-party cookies (Deloitte, 2020). If this policy succeeds, it can significantly reduce fears associated with these cookies and improve users' control over what can be collected through their online activities. Against this background, this policy brief calls for lawmakers to develop a policy framework to facilitate the banning and phasing out third-party tracking cookies. Such a framework could help to mitigate the privacy and security concerns highlighted above. Although Google has promised to phase out these cookies by 2024, such an initiative should not be left to the discretion of tech companies. Enacting legislation through legally mandated institutions such as Congress would give it legal backing and obligate other companies to follow the lead. These laws should also require these companies to fully disclose how the information collected about them will be used. There is also a need for awareness campaigns to be conducted through online platforms to ensure that internet users understand the meaning of cookies technology and the implications of their consent.

Policy Recommendations

As indicated in the first section, online marketing through tracking cookies has become a prominent advertisement method, with businesses seeking to exploit their numerous benefits. However, significant privacy and security concerns have been raised by users, who fear that the lack of control over other entities that process and use their details can expose them to data breaches. Bian et al. (2023) noted that the information collected through cookies can be used in malicious activities such as online fraud. The proposal by Google to phase third-party cookies out of their browsers by 2024 is a noble initiative that could help mitigate these concerns. However, it needs to be made a law for all other companies and web developers to follow. By enacting regulations that ban third-party tracking cookies and control how cookies are used, the initiative would become law rather than being left to companies' discretion. These benefits will, however, come with costs because new policies have upsides and downsides.

One of the downsides of policies that ban third-party tracking cookies is limiting personalization of the content available on the websites they have visited. This limitation can expose consumers to unnecessary ads or suggestions. However, Deloitte (2020) noted that consumers can still get personalized content from their favorite brand or their affiliates. The policy will also prompt advertisers to be innovative in their marketing campaigns rather than relying solely on third-party cookies. It is also crucial for such a policy to be complemented with awareness campaigns to enlighten users about the meaning, usage, and implications of cookies. This recommendation is based on the rationale that many internet users are unaware of this technology's implications for their privacy and security, meaning they can consent to cookies that threaten their privacy (Asgher et al., 2022). The new policies should, therefore, include a clause that obligates websites to educate their users about the implications of cookies and fully disclose their uses. These measures will ensure that users are making consent decisions from an informed perspective. However, their success will depend heavily on global cooperation and universal application.

References

Asgher, S., Latif, F., & Tahir, N. (2022). Online Behavioral Advertising: Do Awareness and Privacy Concerns Protect the Users. *Journal of Development and Social Sciences*, *3*(4), 165-174.

Bian, B., Pagel, M., & Tang, H. (2023). *Consumer surveillance and financial fraud* (No. w31692). National Bureau of Economic Research.

Cinar, N., & Ateş, S. (2022). Data Privacy in Digital Advertising: Towards a Post Third-Party Cookie Era. *Privacy: Algorithms and Society, Routledge*.

Deloitte. (2020). How the cookie crumbled: Marketing in a cookie-less world. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consultancy/deloitte-uk-cookie-less-marketing.pdf

Mellet, K., & Beauvisage, T. (2020). Cookie monsters. Anatomy of digital market infrastructure. *Consumption Markets & Culture*, *23*(2), 110-129.

Sadeghpour, S., & Vlajic, N. (2021). Ads and Fraud: A Comprehensive Survey of Fraud in Online Advertising. *Journal of Cybersecurity and Privacy*, *1*(4), 804-832.