Tracking Cookies for Targeted Marketing: Policy Brief

Hassan Alshehri

Rochester Institute of Technology

PUBL363.02: Cybersecurity Policy and Law

Prof. Ben Woelk

10/21/2023

Executive Summary

Over the past few years, the advertising sector has transformed significantly, moving away from conventional advertising mediums such as newspapers and television to new mediums that rely on digital technologies. These new mediums provide numerous benefits that have enhanced their attractiveness to businesses and led to widespread adoption. However, cybercriminals have also not been left behind and have been inventing ways of exploiting the platforms to carry out malicious acts such as online fraud (Sadeghpour & Vlajic, 2021). It is worth noting that one of the features that online advertisers rely on is cookies, which are small pieces of code set on web browsers to collect relevant information for personalizing web experiences (Mellet & Beauvisage, 2020). These codes are divided into two: first-party and third-party cookies. Deloitte (2020) defines first-party cookies as the cookies placed by website owners to analyze users' preferences and personalize their experiences. In contrast, 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). These cookies pose the highest cybersecurity risks because the user does not know their owners, raising privacy and security concerns (Jegatheesan, 2013). Against this background, there is a need to explore the policy measures that can be used to protect internet users from the threats posed by third-party cookies. This paper defends the policy action taken by Google to block or phase out third-party cookies. It provides justifications for why such an action is warranted and additional recommendations on how to deal with concerns associated with cookies.

Context or Scope of Problem

While cookies alone are not a significant cybersecurity threat, the information they contain can be accessed by unauthorized third parties, leading to privacy violations and exposing users to

cybercrimes. As observed by Sadeghpour and Vlajic (2021), marketing cookies have increasingly become sophisticated to the extent that they can track internet users over a specific period and profile their website preferences. In particular, third-party cookies have become unpopular among consumers who fear that some of the private information stored on websites can be breached (Jegatheesan, 2013). This concern is based on the realization that third-party cookies are produced by different websites from those visited by the user, meaning that consumers are unaware of other entities processing their personal data beyond the owners of websites they have visited. Although the General Data Protection Regulation (GDPR) allows users to provide consent, the users have no control over how the data collected by these entities is used or who uses it once they have consented (Mellet & Beauvisage, 2020). From a consumer perspective, therefore, this lack of control can expose the user to bombardment with unending messages or ads from unknown sources, some of which are not credible or trustworthy. It is worth noting that tracking cookies can gather a lot of personal data, including internet behaviors, location, shopping history, and device specifications. This level of access by unknown entities has been causing significant privacy concerns.

Policy Alternatives

Due to the privacy concerns raised concerning third-party cookies, new data protection regulations have been developed in many countries, allowing users to decide whether they want these cookies to access their browsers. Google has also responded to these concerns by promising to phase third-party cookies out (Deloitte, 2020). This policy will ensure third-party cookies cannot directly influence users' browsing experience, thus giving the users more control over what they share online and who can collect their behavioral data. Consequently, the privacy concerns associated with 'hidden' data collection and use could be avoided. As such, this paper argues that

banning third-party cookies could go a long way to protecting users from the cybersecurity risks discussed above. It also proposes the creation of awareness about cookies technology, how it operates, and the implications of its use by the websites' owners and advertisers. Furthermore, there is a need for the users to be provided with full disclosure on how the information collected from their browsers will be used before consenting.

Policy Recommendations

As indicated in the problem statement, one of the primary concerns regarding third-party cookies is that the users are unaware of other entities processing their personal data beyond the owners of websites they have visited. They also have no control over how the data collected by these entities is used, meaning that it can be used to carry out malicious activities such as online fraud. To this end, the proposal by Google to phase them out from their browsers by 2024 could go a long way toward addressing this concern. However, like any other policy, this move will undoubtedly have benefits and drawbacks for the stakeholders involved. For instance, consumers will lack the personalization aspects provided by the browsers beyond those offered by the website they have visited, thus increasing the possibility of getting irrelevant ads or content suggestions (Deloitte, 2020). Nonetheless, consumers are still likely to continue getting personalized content from the brand or their affiliate companies and brands. Advertisers will also have to find new strategies for conducting online advertisements other than relying on third-party cookies.

Besides phasing third-party cookies, there is also a need to educate internet users about cookies technology, its operations, and its implications. Research indicates that most internet users are unaware of the cookie technology's implications, despite most of them being the younger generation of the information age (Jegatheesan, 2013). This observation suggests the need for awareness regarding what cookies mean and the implications of their operations. According to

Jegatheesan (2013), a significant percentage of internet users are unaware that advertisers and the websites they visit can track their activities using tracking cookies, thus increasing the possibility of consenting to cookies that can cause data and privacy violations. To this end, requiring websites to educate users about cookies could help to address the problem. Another policy measure that could be implemented is to obligate the websites to fully disclose the intended use and user of the information collected through cookies. This disclosure would help the user make informed decisions before giving consent. It would also give a basis for taking action if the information collected from them is used for purposes other than what was stated when consenting. However, for such a policy to yield the desired fruits, standardization of privacy regulations is needed to ensure that actions are universal.

References

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

Jegatheesan, S. (2013). Cookies Invading Our Privacy for Marketing Advertising and Security Issues. *arXiv preprint arXiv:1305.2306*.

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.