Exploring the Digital Trail: Pros and Cons of Third-Party Cookies

Adava Jefferson

Cookies (not the tasty dessert) are digital morsels that we routinely accept without much thought. They quietly track our online activities, yet their true nature remains a mystery to many users. Internet cookies are text files with small pieces of data which identify your computer as you use the internet.[1] These cookies are then used to tailor and improve the web browsing experience for each individual user.[2] There are two kinds of internet cookies, first-party cookies, and third-party cookies.[3] First-party cookies are generally safer and directly created by the website you are using at the time.[4] Third-party cookies are more concerning because they are generated by websites that are different from the page a user is currently on.[5] They also allow advertisers or analytics companies to track browsing history on any website which contains their ads.[6] There are many concerns when dealing with third-party cookies. Those concerns include data privacy,[7] user consent,[8] and potential malware or hackers.[9] Due to the uncertain nature of third-party cookies, some browsers are working on phasing them out.[10] In this blog, I will elaborate on how third-party cookies work, the rules and regulations in place, and what the future of third-party cookies may look like.

Taking a step back from the first-party and third-party cookie distinction, cookies may be either session cookies or persistent cookies.[11] Session cookies are used only when a user is navigating a website, while persistent cookies remain on a computer indefinitely.[12] Session cookies are used to make things like the "back" button work while persistent cookies assist with authentication and tracking.[13] Third-party cookies are significant because they track user data across several websites, instead of tracking only data on the owner's website, like first-party cookies.[14] Third-party cookies work by being incorporated into a website's third-party JavaScript.[15] When the cookie is created, the creator determines whether it becomes a third-party cookie, or a first-party (same-site) cookie.[16]

---

[1] *What Are Cookies?*, KAPERSKY, https://usa.kaspersky.com/resource-center/definitions/cookies (last visited Mar. 30, 2024).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *See What Is CCPA and How to Comply*, IRONCLAD, https://ironcladapp.com/journal/contract-management/what-is-ccpa/ (last visited Mar. 30, 2024).
[8] *See Understanding Cookie Compliance: Cookie Consent, Cookie Policies, GDPR, CCPA, and Other Privacy Laws Explained*, SECURE PRIV. (Jan. 4, 2024), https://secureprivacy.ai/blog/understanding-cookie-compliance.
[9] *See Cookies Hacking*, IMPERVA, https://www.imperva.com/learn/application-security/cookies-hacking/ (last visited Mar. 30, 2024).
[10] Philippa Wain, *Google Chrome Starts Blocking Data Tracking Cookies*, BBC (Jan. 4, 2024), https://www.bbc.com/news/technology-67882315.
[11] Kapersky, *supra* note 1.
[12] *Id.*
[13] *Id.*
[14] Kinza Yasar, *Third-Party Cookie*, TECHTARGET, https://www.techtarget.com/whatis/definition/third-party-cookie (last updated May 2023).
[15] *Id.*
[16] *Id.*

When a user begins browsing online or performing actions on a website, the cookie designation (first-party or third-party) determines if and when the cookies are sent along with the response.[17] When thinking about the third-party cookie process, it is helpful to consider the content you may interact with while scrolling through social media. As an illustration, engaging with ads promoting concerts rather than makeup items could result in receiving more advertisements centered around concerts and music, rather than skincare and makeup products. Although it is beneficial to acknowledge that third-party cookies can customize content for individuals, it is crucial to consider the limitations and regulations involved.

Third-party cookies are beneficial because they allow the variety of ads to be personalized, but they are not perfect. These cookies are still susceptible to attacks by online hackers and malware.[18] Cookie hacking is a cyber-attack where an attacker steals a user's session cookie to gain access to their account or sensitive information.[19] This hacking may result in unauthorized access to sensitive information, identity theft, financial loss, loss of privacy, and legal consequences for failure to adequately protect user data.[20] Users may attempt to protect themselves from these cyber-attacks by using https, using web frameworks to manage session cookies, changing the session key after authentication, and using time based restrictions.[21]

While there are no federal regulations for the use of cookies in America, there are state-level restrictions, and foreign regulations which illustrate efforts to control how and when third-party cookies are used.[22] In California, the current regulation in place is the California Privacy Rights Act (CPRA), which replaced the California Consumer Privacy Act (CCPA) this year, which was first introduced in 2018.[23] This state-level act can be compared with the EU's General Data Protection Regulation (GDPR) in a few significant ways.[24] Both the CPRA and GDPR require the option to opt-out of the sale and sharing of personal information, including targeted advertising by third parties.[25] Unlike the GDPR, the CPRA does not require users to opt-in for data collection unless they are under the age of 16.[26] This may raise questions of how the government can enforce compliance with this regulation. A final point of comparison is the requirement consequence of noncompliance. Under the CPRA, there is a higher fine for violation against minors, while the GDPR has the same standard for any violations.[27] Beyond legal mandates, internet browsers are independently taking action by reducing their reliance on third-party cookies.

Google Chrome is spearheading efforts among its counterparts to restrict the usage of third-party cookies.[28] In a new feature of the Chrome browser, third-party cookies will be disabled.[29] While this feature will initially be available to only 1% of global users, there are plans

---

[17] *Id.*
[18] *Cookies Hacking, supra* note 9.
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *The Complete Guide to California Privacy Rights Act (CPRA) [with Infographics]*, COOKIEYES (May 4, 2021), https://www.cookieyes.com/blog/cpra-californias-new-privacy-law/.
[23] *CCPA vs GDPR. What's the Difference? [With Infographic]*, COOKIEYES (Feb. 15, 2022), https://www.cookieyes.com/blog/ccpa-vs-gdpr/.
[24] *Id.*
[25] *Id*; *The Complete Guide to California Privacy Rights Act (CPRA) [with Infographics] supra* note 22.
[26] *Id.*
[27] *CCPA vs GDPR. What's the Difference? [With Infographic,] supra* note 23.
[28] *See* Wain, *supra* note 10.
[29] *Id.*

to have a full rollout later this year.[30] This effort to make the internet more private may be at the detriment of advertisers.[31] This is because businesses may have no idea who their audience is, leading to issues regarding generating revenue from advertising.[32] With one major browser now opposing third-party cookies, the anticipation builds as we wait to see if others will follow suit.

Third-party cookies, small pieces of data stored by websites, have served as an integral part of personalizing the online experience. However, unchecked, their use poses significant privacy risks, allowing for extensive user tracking and profiling without specific consent. In defense of these dangers, both individual states within the United States and the EU have implemented regulations to safeguard users, such as the CPRA and GDPR. Moreover, major internet browser Google Chrome has taken proactive steps to limit the usage of third-party cookies, hinting at a move towards greater user control of online data. As we continue to navigate this evolving landscape, the importance of striking a balance between personalized user content and user privacy becomes clearer. Considering personal factors is crucial when determining whether to endorse or limit support for third-party cookies, and I hope this blog has given enough insight to help make your opinion clear.

---

[30] *Id.*

[31] *Id.*

[32] Hamza Shaban, *Massive Changes Coming to Google Chrome Threaten to Reshape the Modern Internet*, YAHOO! FIN. (Mar. 24, 2024, 12:00 PM), https://finance.yahoo.com/news/massive-changes-coming-to-google-chrome-threaten-to-reshape-the-modern-internet-160044166.html.