EVERSANA INTOUCH®

First and Third-Party Cookies – Privacy Implications on Paid Media

Executive Summary

In this POV, we outline how valuable data from first-party and third-party cookies fuel your paid media strategy as well as your larger digital ecosystem. However, state-specific privacy legislation has dramatic and sometimes unique implications on how you should handle user data on your brand site. We provide recommendations on how to approach this in an ever-changing landscape.

Introduction

For almost two decades, third-party cookies and user privacy coexisted amiably. Were there lurking fears and sideways glances? Perhaps. But nothing exceedingly insidious transpired, at least not until the 2016 election when Cambridge Analytica harvested data from 87 million Facebook profiles to provide analytical assistance to certain campaigns. From there it seemed like there were a series of cascading incidents, each worse than the next, all involving high profile data breaches from public companies. You could make the argument that the first high profile breach started with the Ashley Madison data breach in 2015. Although it did make national headlines, it only impacted 32 million users and was met with a collective shoulder shrug as nobody knew anyone who used that kind of site … right?

But other high profile data breaches followed, each with serious consequences for impacted individuals:

- In 2017, Yahoo discovered that over 3 billion user accounts were compromised.
- Also in 2017, Equifax, one of the three major credit reporting agencies, lost sensitive, financial data on 148 million people.
- In 2018, Marriott announced that hackers stole data on 500 million guests.
- In 2021, LinkedIn reported that data on over 700 million users was up for sale on the Dark Web, including personal phone numbers.

After Cambridge Analytica and the rise of high-profile data breaches, a very different — and far more privacy sensitive — world emerged. Europe took the mantle almost immediately instituting their General Data Protection and Regulation (GDPR), which governs data collection, consent, usage, data subject rights, and data retention and deletion. Ultimately the GDPR gives EU residents far more agency over their data and has inspired regulation across 12 additional countries outside of the EU, including the United States, as a result.

In this POV, we delve deeper into this regulation by providing an overview of cookies including how they work, the different types, and the impact on a website experience. Further, we discuss the effects cookies have on a brand's website and recommendations to navigate the ever-changing privacy legislature.

Cookies: What They Are and How They Work

Cookies are small blocks of data created by a web server during a browsing session that are then placed on the user's computer or mobile or tablet device.

- **First-party cookies** are set by the domain a user is visiting at the time, helping to deliver a positive user experience. These are typically used to remember log-in information or language preferences.
- **Third-party cookies** are set by domains other than the one a user is visiting. These are typically used for online advertising purposes.

Cookies can further be divided into the following categories. As you can see below, a cookie can be both a first-party cookie and a performance cookie.

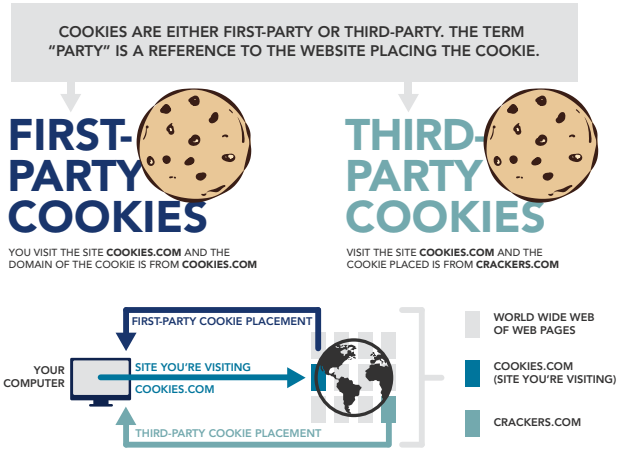
1. **Performance cookies (first-party)** are responsible for gathering data on how users act on a website. Data points such as pages most visited by the user, as well as the types of content that a user engages with, are all tracked by first-party performance cookies. This helps to answer questions like, "did a user watch a video or download a doctor discussion guide?" They also help keep track of error messages received by the user.

2. **Tracking cookies (third-party)** are placed on a website by advertisers (not the actual site) to allow for cross-site tracking. They also gather user information with the goal of then showing that user a relevant, targeted ad that is based on their interests. Before major tech companies like Google and Apple instituted new privacy policies, and legislature like GDPR was adopted, third-party cookies could live indefinitely on a user's browser, tracking them across other sites until their cache was cleared. Regardless of whether a user opts out of third-party tracking cookies as a visitor to a particular site, the industry is preparing for third-party cookie deprecation. Most notably, Google announced (and subsequently pushed back) that they will be phasing out third-party cookies in Chrome. This is now slated to begin in 2024 and will continue into the second half of the year.

    a. **Social media cookies** are used to connect a website to a third-party social media platform such as Facebook/Instagram, LinkedIn, or Reddit. These cookies help track a user's activity on a website in order to retarget and/or serve them relevant social media ads based on the user's behavior.

Cookies Accepted: A Brand's Opportunity

When a user accepts a cookie on a brand's website, this presents the brand with the opportunity to create a more personalized experience that should elevate engagement, as well as the user's overall satisfaction of the experience. More and more, omnichannel and next-best-action strategies are being employed by pharma brands to take advantage of a user's website activity, then inform where that user is in their journey. This allows the pharma brand to personalize the website experience and/or provide a more tailored message through retargeted media. This data can inform not only dynamic creative optimization execution, but also basic retargeting efforts where users receive a retargeted banner message based on the content they viewed or interacted with on the site. In addition, it can fuel more orchestrated trigger-based message executions. This is beneficial to the user in that they will no longer see ads they are not interested in or ads that are not relevant.



Source: Design by Vertical Measures

Another benefit of having a user explicitly opt-in to targeting cookies is that the opt-in action opens additional possibilities for targeting. For example, the Network Advertising Initiative (NAI) advises that advertisers in sensitive disease states provide an explicit opt-in experience on the patient website for any retargeting activities. If that language is included in the brand's overall cookie acceptance policy, it may serve that requirement.

Measurement/Analytics solutions also may depend on users to accept cookies, from ad server conversions, to understanding site behavior and actions, to defining a quality visit. While some media measurement partners are prioritizing tagless solutions moving forward, many still use cookies to provide a more robust level of data.

Cookies Declined: A Brand's Impact

The following tactics may be drastically affected when a user opts-out or declines the use of cookies on your brand's site:

- **Omnichannel:** The ability to deliver a seamless and consistent customer experience across multiple digital channels is greatly diminished.
- **Trigger Strategies on Digital Media and Website:** Trigger-based targeting strategies often rely on cookies to track user behavior in order to trigger an action such as an email deployment or programmatic display banner and could be severely limited when cookies are declined.
- **Media Performance-Based Optimizations:** Analytics won't be able to track onsite actions from those driven to the site by paid media channels, thereby limiting the ability to optimize media performance beyond impression and click activity (though the behaviors of users that do accept could potentially be used directionally, depending on scale).
- **Media Retargeting:** Retargeting effectiveness is greatly reduced as brands won't be able to create retargeting pools, or they will be very small, based on previous engagement with the brand. For those users that do accept cookies, there will be a considerably smaller pool of users available. But because the users that remain have actively opted-in, meaning they are hand-raisers, they may be more willing and eager to engage. If the pool of users that have opted-in becomes too small, tactics will need to be evaluated to ensure digital marketing objectives are met.

So how do you make sure users are accepting versus declining cookies on your brand's site? First, you need to understand the current privacy laws and regulations where your brand is in market.

Current Legislative State

While the U.S. does not have a federal cookie law, five states in the U.S., including California, Colorado, Connecticut, Utah and Virginia, have enacted consumer privacy rights laws in 2023. These laws require businesses to provide website visitors the opportunity to opt-out of tracking, the "sale or sharing of personal information," and the ability to limit the use of sensitive personal information collected on those websites (most commonly through third-party cookies). While the laws referenced above in each state are all similar, there are a few key differences that should be highlighted.

More specifically, each consumer privacy law has its own definition of a consumer, what is considered their personal information, and finally, what rights the consumer has, if any, over the sharing or sale of their data.

- California (CPRA): Cookies are "opt-out." Consent is not needed to collect any information through cookies — but you must allow the consumer to opt-out vis à visa Do Not Sell/Share link and the website cookie banners. There are contractual requirements for "service providers" and "third parties."
    - If a vendor is only deploying strictly necessary, functional, or performance cookies, they should be a "service provider," and the vendor has processing restrictions (i.e., they cannot "sell" or "share" data, cannot aggregate or combine cookie data with other personal information, etc.).
    - If a vendor is deploying targeted cookies, they do not have the same restriction, yet they remain subject to all other CPRA requirements. Your Data Processing Agreements must make that distinction.
- Virginia (VCDPA) and Colorado (CPA): Cookies are "opt-in" ***if the cookies collect sensitive personal information***. So, if you plan on using cookies to collect sensitive personal info, the cookie banner must preemptively disallow (i.e., uncheck the targeted cookie box) cookies.

Global Privacy Control: The California AG and the Colorado AG have each issued regulations that force companies to comply with Global Privacy Control (GPC). It's a browser setting that tracks a user's preferences (e.g., DNS, cookies, DNT) across websites visited using the browser. For example, if someone using Firefox GPC clicks the DNS link and only allows "strictly necessary" cookies on Amazon, those preferences should default when that user visits Target.

Our Recommendations

Based on these findings and the ever-changing status of current legislation, we propose the following recommendations:

- **Weigh The Pros and Cons:** Understand your company's guidance, interpretation of current legislation, and risk tolerance. Additionally, understand the impact of your approach to cookie acceptance on all areas of your digital marketing – website analytics, website user experience, paid media targeting, media performance/ analytics, and omnichannel strategy.

- **Get Specific When Possible:** Various states have consumer privacy laws that could impact user cookie acceptance. Have an implementation strategy in place that takes a state-by-state approach where possible. Depending on the state, a more conservative approach (with greater impact to your digital ecosystem) may be employed, based on variables such as:
    - The exact language you use within the cookie acceptance banner
    - The user's ability to "X" out of the cookie banner
    - The level to which a user can set their own preferences
- **Stay Up to Date:** Lean in on your agency or utilize your own legal team for advice to stay current as state-specific privacy legislation continues to evolve. Additional states will have legislation with implementation dates in 2024.
- **Categorize Cookies:** Depending on how data from certain cookies will be used, work with your legal team to determine if those particular cookies can be considered "functional" and therefore not opted-out by users.
- **Draft and Implement Cookie Policies:** To mitigate potential risks and demonstrate your commitment to user privacy, consider drafting and implementing formal written policies and procedures to establish clear guidelines and practices related to your company's use of cookies. This could include internal and external policies and procedures (i.e., an internal cookie strategy policy vs. an external "Cookie Policy" included in your Privacy Policy on your website or hyperlinked at the bottom of your website's homepage).
- **Test and Learn for the Future:** Additionally, think beyond how you handle user cookie acceptance on your site, and continue to evolve media plans to prepare for third-party cookie depreciation at an industry-wide level. Continue to test targeting solutions that don't rely on cookies, build robust first-party data and audiences where possible, lean into contextual environments where it makes sense, and explore measurement partners that use their own first-party partner integrations, rather than relying solely on cookies.

To optimize how users accept/decline cookies when they land on your website, it's best to collaborate with website/user experience experts. We're happy to connect you to ours at EVERSANA INTOUCH!

Conclusion

As state-specific privacy legislation evolves and larger industry-wide changes to user data privacy unfold, it is critical to stay abreast of the latest updates and develop a flexible approach to both your website data acceptance and paid media strategy that compliantly maximizes the use of data where possible.

To learn more about the impact of privacy legislation on paid media and your brand, contact us.

Contributors

Tina Breithaupt, SVP, Media Services, EVERSANA INTOUCH

Justin Chase, EVP, Media, EVERSANA INTOUCH

Joshua Poole, SVP, Media Services, EVERSANA INTOUCH