What Comes After Third-Party Cookies?

Everything Marketers, Publishers, and Advertisers Need to Know

OneTrust PreferenceChoice™

CONSENT & PREFERENCE SOFTWARE

E-BOOK | October 2020

TABLE OF CONTENTS

DISCLAIMER

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document.

OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue. OneTrust materials do not guarantee compliance with applicable laws and regulations.

COOKIES: THE CHANGING LANDSCAPE

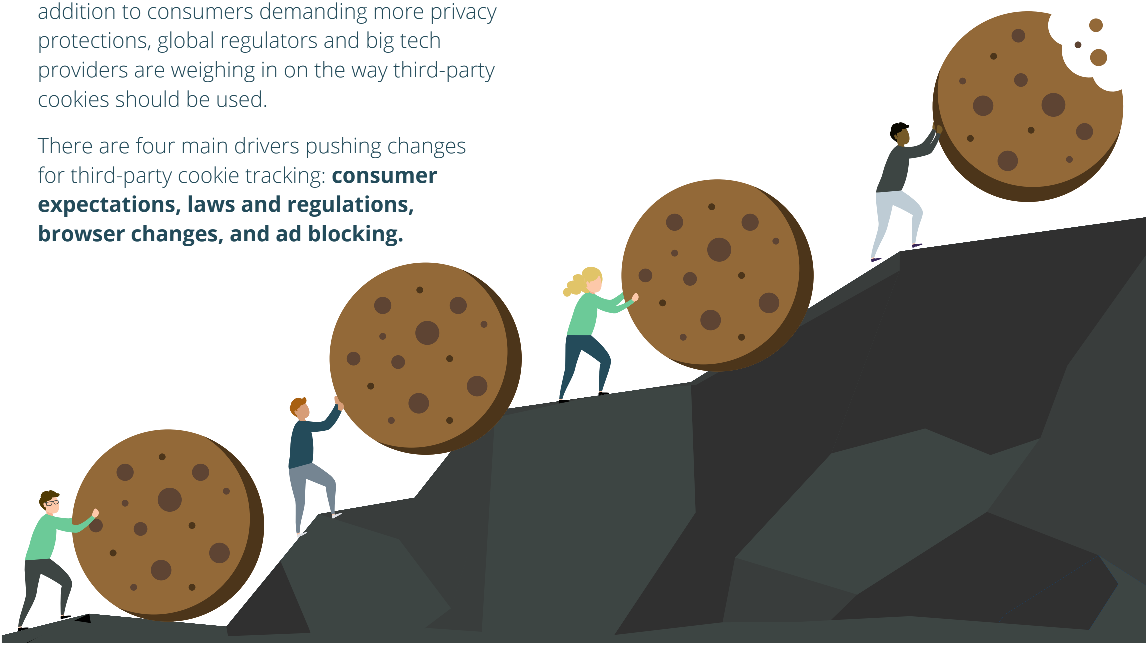
Cookies are small bits of data stored on your computer by a web browser to help tailor digital experiences. Cookies + and other tracking technologies enable personalization by collecting information about consumers' browsing behaviors.

And while there are different types of cookies, most of the changes taking place in modern marketing focus on third-party cookies. First-party cookies are created by the domain a user is actually visiting. **Third-party cookies** are set by a domain that is not the one you're visiting right now. These cookies are typically used for advertising purposes.

For example, have you ever Googled a pair of shoes and then the next time you read a news article, there's an ad for those exact shoes? That isn't magic, it's third-party cookie tracking.

Allowing advertisers to track every consumer's individual move on the internet has raised concerns, and this in turn is driving change. In addition to consumers demanding more privacy protections, global regulators and big tech providers are weighing in on the way third-party cookies should be used.

There are four main drivers pushing changes for third-party cookie tracking: **consumer expectations, laws and regulations, browser changes, and ad blocking.**



CONSUMER EXPECTATIONS

Consumers today genuinely care about transparency and trust from the brands with whom they spend their money:

79%

agreed they'd be willing to share their data if there was a clear benefit to them.

80%

of audiences say they're more likely to purchase from companies they believe protect their personal information.

28%

think they know what consumer product companies best protect their personal information.

(Source: Deloitte)

LAWS AND REGULATIONS

Of the global laws and privacy regulations, three in particular target the use of third-party cookies: the GDPR, the ePrivacy Directive, and the CCPA.

GDPR

Any company that stores or processes personal information about EU citizens within EU states must comply with the GDPR, even if those businesses aren't physically located in the EU.

Regarding cookies, under GDPR companies must receive the user's consent before using any cookies (except strictly necessary cookies) and follow these guidelines:

- Inform the audience of what data is being collected and how it's going to be processed
- Document consent
- Ban denial of service because of opt-out or consent decline
- Create an easy withdrawal process with check boxes or simple button click

"When people complain about the privacy risks presented by cookies, they are generally speaking about third-party, persistent, marketing cookies. These cookies can contain significant amounts of information about your online activity, preferences, and location. The chain of responsibility (who can access a cookies' data) for a third-party cookie can get complicated as well, only heightening their potential for abuse. Perhaps because of this, the **use of third-party cookies has been in decline** since the passage of the GDPR."
- GDPR.EU

ePrivacy Directive

The EU ePrivacy Directive applies to everyone running a website within the EU. It's also applicable to businesses that cater to EU residents, even if the business isn't located in the EU.

Also known as the Cookie Directive, the ePrivacy Directive requires companies to:

- Obtain user consent before dropping any cookies, except strictly necessary cookies
- Provide accurate and specific information about the data each cookie tracks and define its purpose clearly and comprehensively
- Document and store user consent
- Allow users to access your services even if they refuse to consent to the use of certain cookies (i.e., no cookie walls)
- Enable users to withdraw their consent as easily as it was for them to give their consent

CCPA

The CCPA applies to all companies that serve California residents and have at least $25 million in annual revenue. Additionally, companies of any size that have personal data of at least 50,000 people or collect more than half of their revenues from the sale of personal data must comply with the regulation.

When it comes to cookies, under CCPA, opting out of a sale and the sharing of personal data is a key focus. Use of third-party cookies could be considered a sale, so consent is often sought as a best practice.

BROWSER CHANGES

Not only are regulators getting involved, but now major tech companies are taking cookie tracking into their own hands and the impact is significant.

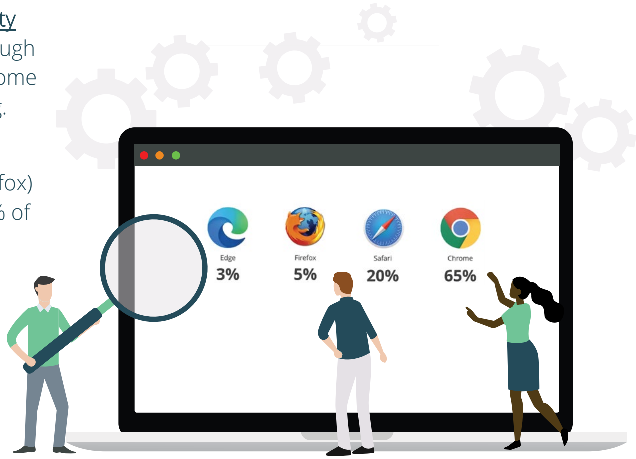
Safari: Apple's internet browser Safari now blocks all third-party cookie tracking. This means companies can no longer follow consumers' habits using commonplace tracking technology.

> "Full third-party cookie blocking makes sure there's no ITP state that can be detected through cookie blocking behavior… ITP's classifier keeps working to detect bounce trackers, tracker conclusion, and link decoration tracking."
> **– John Wilander, WebKit Security & Privacy Engineer Apple**

Firefox: Firefox prides itself on its promise of privacy and security as central aspects of the web browser's experience. And in February 2019, Firefox honored that promise by blocking all third-party tracking cookies.

Google: In the past, Chrome has allowed users to block third-party cookies. But Chrome warns: "Some sites may not work properly when third-party blocking is turned on." In January 2020, Google Chrome began to phase out third-party cookies to end this dilemma for its users. Though this will be a gradual process, by 2022 all Chrome browsers will block third-party cookie tracking.

Today, only 30% of available impressions are rendered on browsers (mostly Safari and Firefox) with no third-party cookies. Chrome uses 65% of the remaining browser usage.



AD BLOCKING

26% of internet users are using ad blockers on their browsers. Not only does this statistic show consumers are more involved with selecting preferences for their own experiences, but it's important to note that ad blockers diminish the value of third-party cookies.

Each of these areas builds on each other. As consumers worry more about their privacy, they'll only become more educated about the topic. This will lead to the growth of ad blocking, browser updates, and privacy regulations to meet expectations.

This can be disruptive for marketers, advertisers, and publishers that have been so reliant on third-party data.

With that being said, what does the future look like for marketing professionals? The big question everyone's asking is, what's next?

26%
of internet users are using **ad blockers** on their browsers

WHAT'S NEXT: THE FUTURE OF COOKIES

Only 36% of marketers say they have a good understanding of the third-party cookie crackdown. On the other hand, for years publishers and advertisers have heavily relied on these cookies to track website visitors, improve the user experience, and collect data that helps target ads to the right audiences.

While many professionals are starting to think about weaning themselves off cookies, the truth is the removal of cookies changes the game for the entire industry. Without access to key data to improve marketing or ad performance, everyone is left wondering, "Where do we go from here?"

Here's what marketers, publishers, and advertisers need to know about the future of cookies, and the opportunity it presents to build trust and transparency with customers.

First- and Zero-Party Data

As third-party cookies go away, businesses should shift their strategy to identify and capture personalization preferences and data by leveraging a combination of first-party and zero-party data capture through progressive profiling. This allows businesses to build trust while providing the control and personalization your consumers want.

In addition to capturing first and zero-party data, publishers and advertisers in the ad tech landscape are exploring different strategies such as leveraging contextual advertising or more direct advertising deals.

OneTrust PreferenceChoice™
CONSENT & PREFERENCE SOFTWARE

Steps to Build a New Strategy in a Post Third-Party Cookie World

Step 1: Shifting Core Focus Areas

Changes to third-party cookie tracking don't change the deliverables that come with being a marketing leader. Rather, there need to be changes in the way those goals are met.

First, there needs to be a shift in three main focus areas for all marketers: audience, brand, and reporting.

Audience

Marketers are responsible for building out CRM data, driving demand generation, and nurturing and supporting the sales cycle. To achieve this, they need to reach their audience and gain permission to communicate with them.

Moving forward, marketers will need to explicitly receive consent and an opt-in in order to earn that reach. Ultimately, that will come from building trust.

Brand

Marketers are also responsible for driving the brand awareness and messaging of their business and products. They own the customer communication and ultimately create brand advocates.

But without third-party data, they'll need to shift their communication strategies with consumers privacy-first promise. This means applying open and transparent language about how the brand will be collecting, sharing, and using consumer data.

Reporting

Lastly, marketers are responsible for knowing how their campaigns are performing. This means full visibility into how many leads were generated, the CPL, the ROI, and all the attribution that makes finding these numbers possible.

Since third-party data is going away, capturing data from users in a transparent way will be even more important for marketers moving forward.

For marketers, publishers, and advertisers alike, it's important to think about privacy and building trust with audiences in a way that actually impacts the KPIs for which they are accountable they're tasked. The good news is, there's a huge opportunity to be at the forefront of promoting privacy policies and earning trust.

> "Data that comes from customers themselves is, almost by definition, the most valuable tool you have- and you don't have to pay a social media company to get it."
> **- AdWeek**

Step 2: Build Your Consent and Preferences Strategy

In order to establish trust and transparency with customers moving forward, marketers, publishers, and advertisers alike will need to build an internal privacy strategy.

Your consent and preferences strategy should aim to achieve five goals:

1. **Put users in control.**
   Give users choices that go beyond compliance options under global privacy regulations that apply to your organization. Allow your users to choose how they want to communicate and share data with you.
2. **Have an opt-down, not opt-out, strategy.**
   Defend against high unsubscribe rates to protect your marketable database keeping them as low as possible. Presenting multiple options for your audience to opt down from communications instead of opt out will both help your unsubscribe rate and empower your audience to get the communications they want.
3. **Show custom preferences & profile data.**
   Ensure it's easy for customers to choose their specific communication channels (phone, email, SMS).
4. **Monitor engagement insights and analytics.**
   Track analytics about opt-in and unsubscribe rates to help you quantify trust.
5. **Sync marketing and IT systems.**
   Capture and centralize all consents and preferences. Ensure they sync with all other systems used to communicate with your audiences. Guarantee you're delivering on your brand promise and respecting the way with which your audience prefers to be communicated.

Step 3: Elements of a Trust Center and Best Practices

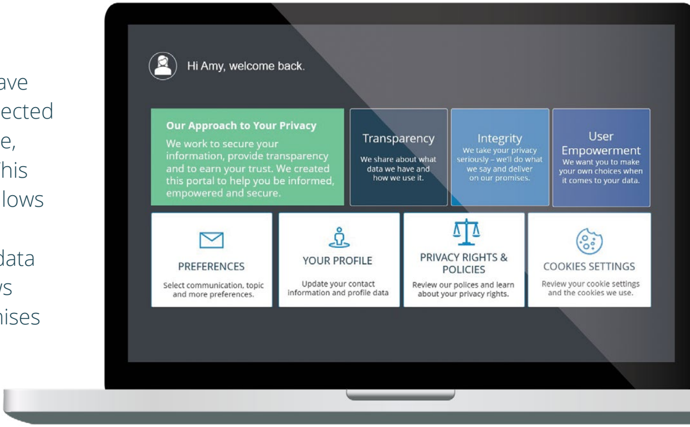
Next, it's important to leverage a Trust Center to educate and provide transparency to your audience. A Trust Center serves as a way for users to freely make choices about their consent and preferences. But it's also a strategic opportunity for brands to highlight their commitment to their users' privacy.

To achieve this, a Trust Center should contain five sections:

1. The company's mission statement in regard to user privacy
On the homepage of the preference management center, there should be a mission statement that explains the company's approach to privacy. Similar to an "about us" page, this should be a key pillar of the brand promise in regard to user data privacy protection.

2. A user preferences section
Next, there should be a section or tab with communication preferences that allows users to easily opt in, opt down, or opt out of different forms of communication. This includes email, phone, and SMS. Additionally, companies should provide options for the user to choose the frequency in which they're communicated with, as well as a log of their individual consent history.

3. A user profile
Under the profile section, users should have full access to the data a company has collected about them. This might include their name, emails, phone numbers, addresses, etc. This section has two key advantages. First, it allows the user to fill in any gaps or correct any data that needs updating, (meaning less data management for brands). Second, it allows organizations to uphold their brand promises about complete transparency.



Hi Amy, welcome back.

Our Approach to Your Privacy
We work to secure your information, provide transparency and to earn your trust. We created this portal to help you be informed, empowered and secure.

Transparency
We share about what data we have and how we use it.

Integrity
We take your privacy seriously – we'll do what we say and deliver on our promises.

User Empowerment
We want you to make your own choices when it comes to your data.

PREFERENCES
Select communication, topic and more preferences.

YOUR PROFILE
Update your contact information and profile data

PRIVACY RIGHTS & POLICIES
Review our polices and learn about your privacy rights.

COOKIES SETTINGS
Review your cookie settings and the cookies we use.

The user profile is also a practical place to add additional sections called "experiential preferences" where users can input data based on their preferences. This allows organizations to create much more personalized experiences with their audiences. For example, you might want to provide a section for them to fill in their T-shirt sizes or beverage choices, depending on your industry.

4. The company's privacy rights policy

In addition to housing the company's privacy and security notices, this section needs to make it easy for consumers to submit consumer requests, access the organization's third-party processors list, and view the company's terms and conditions.

5. User cookie settings

Under this section, it's important for the organization to explain to its users exactly what kind of cookies are being tracked, as well as a definition of what those cookies are used for. Here, consumers should have the ability to opt in or opt out of cookie tracking.

Setting up a Trust Center is the first step to transition their mindsets from being reliant on third-party cookies, and finding new ways to capitalize on first-party data.

The goals of providing consent and preference management to users is:

1. **Allowing your organization to be completely transparent.**
2. **Honoring your brand promise and respecting your users' data across all the organizational systems and tech stacks.**
3. **Not only meeting, but going beyond global regulations in regard to managing user privacy data.**

As third-party cookies end, the most valuable component to your work will be building trust with customers through a better understanding of what they want. Including preference management in your strategy can expand options available to customers, enhance the user experience, deliver personalization, and reduce opt-outs/unsubscribes. You can show customers you're listening to what they want, while also respecting and protecting their privacy.

To learn more about how preference management plays a key role in a world beyond cookies, sign up for a **free trial** or **connect with one of our team members today.**

RESOURCES

There is certainly more to come in the "after-cookies" era.

And it's crucial for organizations to keep up with the ever-changing landscape to ensure compliance and honor the promise committed to users. Here are some excellent resources to keep marketers and publishers in-the-know regarding any changes for cookies and global privacy regulations:

The End of Third-Party Cookies: What's Next?
Third-party cookies are coming to an end. What comes next? Watch this recorded virtual session to review the timeline for the end of third-party cookies and the current privacy landscape that is driving the changes.

Consent Beyond Cookies: How You Can Authentically Build Audience Trust
In this 45-minute webinar marketers can learn how to build trust with customers through a focus of transparency.

OneTrust DataGuidance
OneTrust DataGuidance is a regulatory software platform updated daily. This is a go-to for marketers and publishers who want to keep up with privacy and legal research guidance.

OneTrust PreferenceChoice™

CONSENT & PREFERENCE SOFTWARE

PreferenceChoice Website
www.preferencechoice.com

PreferenceChoice Blog & Resources
Click Here for blog and resources

Follow us on LinkedIn
Click Here for LinkedIn