

The Complete Guide to First-Party Data

OneTrust PreferenceChoice™
CONSENT & PREFERENCE SOFTWARE

E-BOOK | March, 2021

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.

Copyright © 2020 OneTrust LLC. All rights reserved Proprietary & Confidential.

INTRODUCTION: WHY FIRST-PARTY DATA?	3
THE CHANGING STATE OF DATA COLLECTION	4
Factor 1: Laws and Regulations	4
Factor 2: Browser Changes	5
Factor 3: An Emphasis on Transparency and Trust	6
THE 4 DATA TYPES YOU NEED TO KNOW	7
5 LEADING BENEFITS OF FIRST-PARTY DATA	9
9 SOURCES FOR COLLECTING FIRST-PARTY DATA	10
TOOLS FOR COLLECTION AND CONSENT	12
REAL WORLD EXAMPLES	14
THE FUTURE OF DATA IS CONSENT	14

INTRODUCTION: WHY FIRST-PARTY DATA?

\$19.2 Billion

That's the amount of money that was spent just two years ago on third-party data (data collected from sources like websites and platforms, as opposed to the person the data pertains to).

For years, collecting third-party data has been the go-to method to break through to new audiences. But due to numerous changes around data privacy, that's all coming to an end.

We're approaching the **end of third-party cookies**, and this shift is changing how marketers and publishers consider their profession. The elimination of third-party cookies presents challenges for creating hyper-targeted, measurable campaigns. How can you continue delivering the personalization that audiences crave and that drive results?

Despite these challenges, this transition away from third-party data isn't bad for the industry; in fact, it has the potential to be quite the opposite. And what can be easily overlooked is that these "personalized" campaigns that rely on third-party

data might actually diminish trust, as customers grow increasingly wary of brands overstepping boundaries and invading privacy.

If third-party cookies can be replaced with **first-party data**—data directly from customers—then you can provide customized and authentic experiences, encouraging customers to feel more deeply connected and loyal to your brand.

The move from third-party cookies to first-party data presents opportunities to:

1. Learn about your audience's interests, preferences, characteristics, and behaviors—directly from them.
2. More accurately predict future customer behavior, improve your targeting, enhance your marketing campaigns, and hyper-personalize your content.
3. Build transparent relationships about data usage with customers.
4. Recoup revenue lost to third parties in recent years.

In this guide, we outline everything you need to know about first-party data. You'll learn why first-party data benefits your efforts, how and where to collect it, best practices around data collection and usage, and recommended technologies for streamlining your processes. Additionally, we include a few real-world examples of how brands are leveraging first-party data today.

This is your guide to implementing an ROI-driven, first-party data strategy. It's a helpful resource to reference as you work toward your business goals.



THE CHANGING STATE OF DATA COLLECTION

It's important to understand why third-party cookie tracking is coming to an end. Two words: data privacy. As technology continues to rapidly advance, consumers are growing less and less comfortable with being tracked online.

Users want choice and control over their personal data, and industries are listening. Tech giants like Google and Apple are phasing out third-party cookies from their respective browsers in order to provide users a deeper sense of security. Under the GDPR, website visitors now must opt-in to enable third-party cookies.

Laws and regulations, browser changes, and a growing emphasis on transparency and trust are forcing the move away from third-party cookies.

Factor 1: Laws and Regulations

In 2017, economists began referring to data as being **"more valuable than oil."** Today, **87% of consumers** harbor concerns about how their personal information is being used. That's why it's no surprise governments have stepped in to enforce regulations that give individuals more rights over their data. A few of the notable laws

impacting the way third-party data is collected and used include:

Privacy and Electronic Communications Directive (ePrivacy Directive)

The ePrivacy Directive, also known as the Cookie Directive, was the impetus behind cookie consent pop-ups' proliferation.

Under the ePrivacy Directive, websites that target individuals in the EU must:

- Obtain users' consent before using any cookies (except strictly necessary cookies).
- Tell users about each piece of data the cookies track and their purpose - in plain language.
- Document and store user consent.
- Give users the option to access content and services even if they refuse to allow certain cookies.
- Enable the users to withdraw their consent at any time.

The General Data Protection Regulation (GDPR)

The GDPR is the most comprehensive data protection legislation to date. However, the GDPR only **mentions cookies once** in its 88 pages.

The regulation says:

"Natural persons may be associated with online identifiers provided by their devices, applications, tools, and protocols, such as internet protocol addresses, cookie identifiers, or other identifiers such as radio frequency identification tags. This may leave traces that, particularly when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

Cookies qualify as personal data and are subject to GDPR. This means companies can process user data as long as they've received consent or have a legitimate interest.

THE CHANGING STATE OF DATA COLLECTION

California Consumer Privacy Act (CCPA)

The CCPA classifies cookies as personal information. While the CCPA doesn't make businesses obtain opt-in consent for cookies, it does require them to disclose what information they collect and the purposes of collection. It also says businesses that sell the personal information collected by cookies must inform users of such sales and allow them to opt-out of the sale of their personal information.

California Privacy Rights Act (CPRA)

Passed in November 2020, most of the CPRA's provisions will go into effect on January 1, 2023. This legislation will work in conjunction with the existing CCPA. The most notable change regarding third-party cookies is the provision expanding consumer rights.

Under CPRA, consumers will have the right to opt-out of the sharing of personal information with a third-party for cross-context behavioral advertising (targeted advertising). This change will specifically impact third-party adtech cookie collection and sharing. Organizations under the scope of CPRA

that engage in targeted advertising will need to ensure that they have adequate mechanisms in place to allow consumers the right to opt-out of the sharing of personal information with a third-party.

Factor 2: Browser Changes

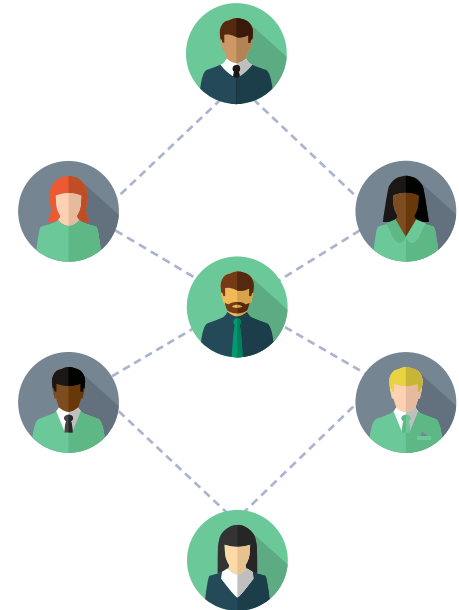
In addition to government regulations, big tech players including Apple, Firefox, and Google are making significant changes to browser settings to protect users' personal data. Here's what each platform is changing:

Apple (Safari): Apple's internet browser Safari **now blocks** all third-party cookie tracking. This means you can no longer follow consumers' online behaviors using tracking technology.

Firefox: In February 2019, Firefox **blocked** all third-party tracking cookies.

Google: In January 2020, Chrome **began to phase** out third-party cookies. They will cease to exist on the browser as of 2022.

These changes are actually making more of an impact on the industry than legislation. Privacy laws are dependent on company and consumer location. But browser changes impact everyone who uses the internet, regardless of location.



THE CHANGING STATE OF DATA COLLECTION

Factor 3: An Emphasis on Transparency and Trust

More and more studies point to this: customers won't engage with companies they don't trust.

In fact, **Salesforce research** shows 75% of customers strongly associate privacy with trust. And 72% will stop buying from a company or using its service due to data privacy concerns.

On the flip side, consumers will share their data with publications and brands they do trust:

- Brands that are upfront about how they use information to target ads can **boost engagement levels by up to 40%**.
- **75% of consumers** are willing to share personal data with a brand they trust.
- **80% of people** are willing to share personal information directly with a brand to receive personalized marketing. But only 16.7% are willing to share this type of data through third parties.

Consumers want to trust companies and receive personalized experiences. And they're willing to trade their data for it. It just needs to be shared only with the company given permission to use it.

Moving forward, businesses and organizations need to readjust their marketing strategies to be more transparent about data usage and build trust with their audiences.



THE 4 DATA TYPES YOU NEED TO KNOW

Between privacy legislation, browser changes, and consumer demand, it's clear that third-party cookies are being depreciated—and so marketers and publishers must start the transition away from third-party data. What kind of data is there left to leverage?

First-party and third-party data are the most common. But there are actually four different types of data to be aware of.

1. Zero-Party Data

This is data your customers directly and intentionally share with you. It can include purchase intentions, personal context, and how the individual wants the brand to recognize them.

The best way to collect zero-party data is to ask for information in exchange for something of value to the customer. This could be through a survey, customized product recommendations, or a free resource such as an eBook.

2. First-Party Data

First-party data is a direct reflection of your audience. It's collected from:

- Website and app analytics
- Your CRM
- Social media profiles
- Subscription-based emails or products
- Surveys
- Customer feedback

The main difference between first-party data and zero-party data is that collecting zero-party data solicits a direct interaction from your audience. On the other hand, first-party data gives you insights from analytics and user behaviors.

3. Second-Party Data

Second-party data is data you don't collect yourself. It's typically used between trusted partners who come to an agreement to share audience insights for mutually beneficial reasons.

You collect second-party data and first-party data the same way. The only difference is you receive it from someone else.

4. Third-Party Data

Third-party data is any data collected by a business that doesn't have any direct link to the visitor or customer.

Companies collect third-party data by purchasing it. The companies selling third-party data typically research random sample sizes. For this reason, this data is typically less reliable than zero, first- or second-party data.

THE 4 DATA TYPES YOU NEED TO KNOW

Data Type	What is it?	Example	Data Quality	Targeting Reach
Zero-Party Data	Data provided directly by consumers, usually addressing communication preferences.	<ul style="list-style-type: none">• Personal information• Potentially sensitive data (political opinions, for example)• Intentional behaviors• Preferences	High	Exact
First-Party Data	Also originating directly from consumers, first-party data may be collected to support a transaction or as a support or service requirement.	<ul style="list-style-type: none">• Behaviors or actions from your website, app, or product• Email or SMS interactions• Purchase history	High	Exact
Second-Party Data	Second-party data usually refers to someone else's first-party data. Purchasing data from another organization or sharing data through a partnership falls within this category.	<ul style="list-style-type: none">• Behaviors or actions from another company's website, app, or product• Emails or SMS interactions• Purchase history	Narrow	Narrow
Third-Party Data	Data collected by an organization that doesn't have any direct link to the customer. Usually, the data is collected by data aggregators to sell it to other companies.	<ul style="list-style-type: none">• Demographics• Behavioral• Contextual	Narrow	Narrow

5 LEADING BENEFITS OF FIRST-PARTY DATA

With other data sets to choose from, there's a good reason marketers and publishers value first-party data the most. It offers the best return on investment in terms of who your audience is and what their habits are. Here are five reasons first-party data is valuable:

1. Increase Relevance

First-party data takes the guesswork out of determining who your audience is since it's collected directly from their behaviors and preferences.

2. More Accurate Data

With first-party data, you eliminate the middleman. Data that comes straight from the source is more likely to be accurate. It's also easier to manage privacy-related issues because you know exactly where the data originated.

3. Immediate Availability

Odds are, you have access to first-party data right now. It's stored in your CRM. And if you're hoping to start collecting data with consent, you can implement a preference management platform.

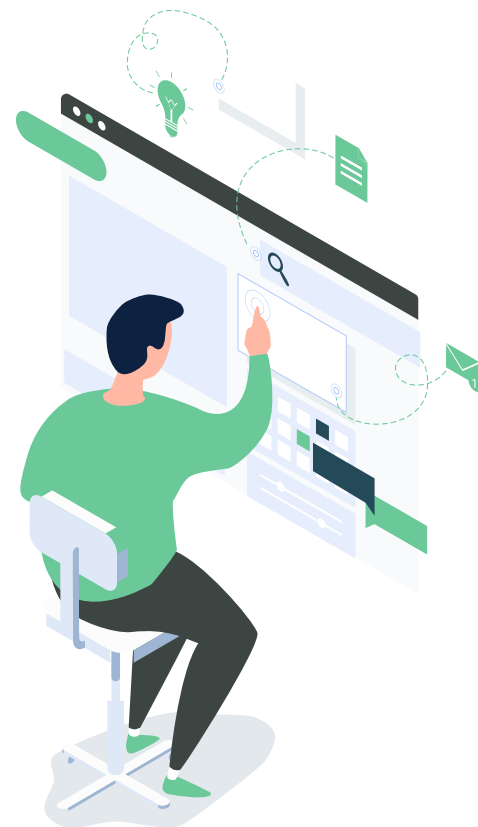
4. Less Money

Because it's your data, there's no cost associated with first-party data. The only cost is the advertising you use to draw users to your website and the tools you use to measure the insights, which you were probably paying for anyway.

5. Better Customer Experience

80% of frequent shoppers say they'll only shop with brands that personalize their experiences. While third-party data could get you in front of more audiences, those audiences aren't necessarily relevant. And that could have been doing you more harm than good as **70% of millennials** get frustrated by brands that send them irrelevant content.

First-party data allows you to gauge customer intent and position in the buying journey. By seeing what your audiences are interested in, you can personalize their experiences by suggesting products and content your customers want to see.



9 SOURCES FOR COLLECTING FIRST-PARTY DATA

Buyers shop across multiple channels and multiple devices, using an average of almost six touchpoints when purchasing an item. Your customers must be able to easily navigate between each touchpoint to make a purchase.

What's equally important is gaining and maintaining visibility into the channels driving results and the ones that need optimizing. Luckily, first-party data is collected from a range of sources that give you varied and abundant insight into your omnichannel performance.

Here are 9 sources from which you can collect first-party data:

1. Website: Your website provides a wealth of data about your customers. From names and email addresses, to visitor behavior and transactions, it's loaded with intel.

2. Mobile web: The mobile version of a website can collect most of the same data as a desktop version. However, not all mobile devices allow the use of JavaScript or cookies. Encouraging users to log into a site allows you to collect meaningful interactions, even in a cookie-less environment.

3. Mobile apps: App users are your most enthusiastic supporters. New tools such as Google Analytics 4 allow you to define which user events are meaningful so you can log and measure them.

4. Subscription data: Much like app data, people who subscribe to receive your content show a major interest in your brand. Use subscription data to analyze who's signing up, where they are, and what types of content they're engaging with. This will give you a much more informed idea of who you should be targeting.

5. Email and SMS: Email and text data tells you who opened, clicked, and unsubscribed from your emails. Dig deeper into that data to segment audiences based on their actions.

6. Point of sale and CRM: Knowing your customer's shopping history allows an incredible amount of personalization to take place. What's more, this intel can show you what's selling, what isn't, and where.

7. Call centers: Bill Gates said, "Your most unhappy customers are your greatest source of learning." That's why some of your most valuable feedback lands in the walls of your call center. Often, it's where problems come to the surface. Non-sensitive data about customer interactions and help desk items can provide insights that many of your competitors overlook.



9 SOURCES FOR COLLECTING FIRST-PARTY DATA

8. Social media: Use your social data to see who's following you, liking your posts, and commenting. This is another avenue to see who your audience is. By exploring their profiles, you can understand their desires. What do they care about? What other brands are they following?

The content of the messages and comments people send you can also give you information about what people think about your brand, content, and products. You can then use the exact language of your audience for your future campaigns.

9. Survey and customer feedback data: There's nothing wrong with directly asking your customers for feedback. Whether you shoot out a survey, or merely read your Facebook messenger, these insights can help you get a better idea of your customers' demographics, opinions of your products, and communication preferences.



TOOLS FOR COLLECTION AND CONSENT

You can collect first-party data from a number of sources. But collecting the data is not the primary issue. More significant challenges include:

1. Collecting data in a compliant manner.

2. Aggregating data from all possible sources to form a holistic view of your audience.

Achieving both of these is crucial for making first-party data work for you and it will involve investment in new technologies.

The CCPA and GDPR redefined how a company receives, stores, and distributes customer data. The general rules are to keep the processing and use of data transparent, collect consent for data, and allow users to update their data and opt-out.

But as we all know, compliance laws change rapidly. Keeping up is a job in itself. To maintain compliance while also building trust with your customer, you'll need to invest in an AI-powered consent tool. One or both of the below may be a helpful addition to your tech stack:

1. Consent Management Platform (CMP)

Consent Management Platforms are probably the easiest software solution to understand. They do exactly what their name says. CMPs provide a user interface and back-end integrations that allow individuals to manage their consent settings and then have those settings enforced.

Most commonly, CMP is used when referring to **cookie banners** – those banners you see on every website. Yes, they're CMPs! CMPs directly address specific regulations. Most commonly, these include PECR (E-privacy Directive), GDPR, and CCPA.

Take these key factors into consideration when selecting and implementing a CMP:

- The ability to automate compliance. In other words, it should provide the correct consent models based on jurisdiction, such as an opt-in for GDPR and an opt-out for CCPA - all in real-time.
- Scalability. Ask, "Can this CMP meet my traffic needs? Can I set one set of rules across all of my digital properties?"

- Cross-device/domain consent
- Single-time deployment
- UI customization to ensure an on-brand experience

2. Preference Center

A Preference Center is a key component of a preference management strategy. A Preference Center should also be a compliance enabler and capture required regulatory consent. But it should feature additional capabilities beyond this, including capturing zero- and first-party data and integration with your martech stack

If you think about email marketing as a regulatory consent requirement under GDPR, a CMP will most likely provide a binary option for consent at the email marketing level. However, this provides no means for individuals to control and personalize their experience with your brand.

Preference Centers allow you to take the required consent and offer increased personalization options such as frequency of communication and choice of relevant topics. This is a win for

TOOLS FOR COLLECTION AND CONSENT

marketers and publishers looking to provide a personalized experience for audiences.

By providing this level of personalization and control, you'll find your opt-out rates decline as consumers choose to use these options. At the same time, your conversion rates will rise as consumers receive content in which they're actually interested.

An effective Preference Center will include:

- Highly configurable and customizable consent and preference options
- A flexible data model
- Robotic process automation for integrations: CRM, email marketing, lead gen.
- A full API suite
- Omni-channel capturing of data
- Choice across identity verification: SMS OTP, Email, CIAM

How to Put First-Party Data to Use

For first-party data to be valuable to both you and your customers, you'll need to build your process around three steps.

The first is building a strategy that supports broader business objectives. The second is collection: gathering, storing, cleansing, and combining consumer data from multiple sources. The third step is test and activation. You'll put the data to work for marketing activities at all stages of the buyer cycle.

1. Build a Strategy

In this stage, you need to clearly identify the data you need in order to effectively reach your business goals.

Then, set priorities for each customer segment. For example, one segment is your current customers. Think about how you can use first-party data to up- or cross-sell, predict or prevent churn, or re-energize them with a customized experience. Also, consider how you can use your customer lists to target new prospects with lookalike lists.

2. Collection

Next, determine what technologies and resources you need to invest in to walk away with a holistic view of your data.

In addition to the sources that collect your data (website, social, CRM), you'll need a platform that ensures you can automate compliance across the globe and a CMP that connects your data from all sources. If you don't have the resources to manage or invest in these technologies, consider working with a partner who might be able to help.

3. Test and Activate

Once the strategy, tech, and data are in place, it's time to test. Make sure your automations are functioning and your hypotheses are accurate. If anything is off, adjust as needed.

Over time, you'll discover how segmented audiences react to different campaigns and offers. Analyze those insights to make more informed marketing decisions and drive better results. While everything we've discussed around first-party data sounds great, you're likely wondering what it looks like in action. The two sections below contain

REAL-WORLD EXAMPLES

examples to provide you with this insight. Keep in mind, there's an opportunity for overlap between types. These are just a few examples of common use cases.

Examples of Using First-Party Data for Marketers:

1. Build Lookalike Audiences

Reaching new audiences is still possible with first-party data. And you can actually build even more qualified audiences by building lookalike lists.

Lookalike audiences consist of the people or customers likely to be interested in your service or product. All you need to do is determine what customers are ideal, and create a segmented list.

From there, you can upload that info into Google or Facebook. The platforms will only serve your ads to people who "look" or "behave" like your target audience. Now you're only sending ads to people who are most likely to engage with your products or services.

The screenshot shows the 'Create an Audience From a Customer List' window in Facebook Ad Manager. It has a close button (X) in the top right corner. The window is divided into two main steps:

- Step 1: Add Customer List** (indicated by a circled '1'). It includes a 'Show Tips' link. Below the heading, it says: 'Before uploading your list, make sure you have enough identifiers in the correct format. The list needs to be in a CSV or TXT format.' There is a 'Download List Template (.csv)' button. Below that is a large dashed box for file upload, containing the text 'Drag and drop your file here or' and an 'Upload File' button.
- Step 2: Name Your Audience** (indicated by a circled '2'). It features a text input field with the placeholder 'Name your audience', a character count '50', and a clear button (X). To the right of the input field is an 'Add Description' link.

At the bottom of the window, there are three buttons: 'Cancel', 'Back', and 'Next'.

Source: Facebook Ad Manager, Creating Audience From Customer List


REAL-WORLD EXAMPLES

2. Create Personalized Emails and Automation


First-party data and personalization go hand in hand. The data you collect about website visitors gives insight into their interests and needs. It's now your job to use that information to serve them content that feels relevant and personalized.

Email is a perfect way to do this. If you're a retail store, you can use purchase history and website page visits to serve your customers products they want to see. If you're a B2B marketer, you can use website page visits to serve prospects relevant blogs, eBooks, and nurture emails.

SARAH- THESE ARE SO YOU.




Open Toe Zebra Pump
\$48.99


451 people are shopping this right now!


Shop

Boss Babe Booty
\$69.99


233 people are shopping this right now!

Shop

Cheetah Vala Heel
\$82.99


147 people are shopping this right now!

Shop

REAL-WORLD EXAMPLES

3. Show Website Users What They Want to See

Much like personalizing your emails, you can use first-party data to personalize the website content your visitors see.

Let's say your work for a B2B company targeting two different audiences: brands and agencies. You've created an eBook for each and want to show a smart pop up banner on your home page. You can integrate your CRM and website to show visitors from each industry the eBook relevant to them:

Of course, if you don't have their industry listed in the CRM, you can add it to your forms so that information is available moving forward.

For brand segments:



For agency segments:



REAL-WORLD EXAMPLES

4. Create Dynamic Graphics

With first-party data, your targeting strategy can get granular. This means you can build dynamic ads that contain messages based on a range of factors. Think previous user behavior, location, and intent.

For example, if you're a marketer at an airline, you could use your first-party data in a demand-side platform (DSP). Display this ad to a customer who recently purchased a one-way ticket from New York City to Los Angeles:

By leveraging your first-party data, you could predict that the traveler will return to New York in the near future.



REAL-WORLD EXAMPLES

Examples of Using First-Party Data for Publishers

Publishers can use first-party data in a lot of the same ways marketers can. But there are some differences. Because publishers typically attract tens of thousands of people to their websites with just content, there are different ways to use first-party data to benefit both your publication and readers.

1. Use a Paywall

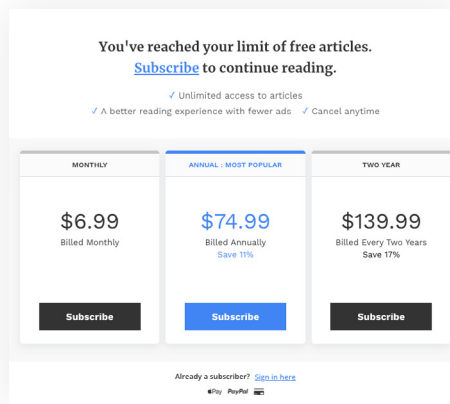
This serves as a way to both collect data and monetize readership. It provides a sense of exclusivity for readers, as they get control over the data they're sharing in exchange for higher quality and more valuable content.

The downside, of course, is creating a barrier to prospects. It could scare off readers who don't want to pay.

A few good ways to combat that downsides are to:

- Provide a certain number of free articles per month.

- Host “paywall down” events that tie into special occasions.
- Offer paywall discounts for actions like filling out surveys.
- Host exclusive membership-only paywalls where users just need to create an account, no payment required.

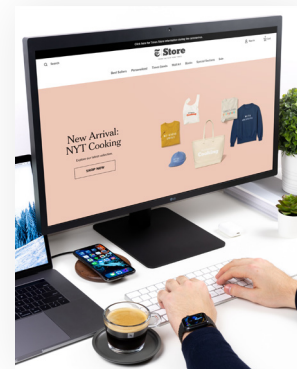


Source: Forbes

2. Host an eCommerce Site

Another unique method that combines first-party data collection and monetization is hosting an eCommerce platform. This allows the reader to see direct value from a shopping experience. Note, it's important readers fully understand how their data is being used.

While this can be lucrative, it needs to make sense as an offer for the publications. It can be challenging. A publisher to watch is The New York Times. Check out its eCommerce store here.



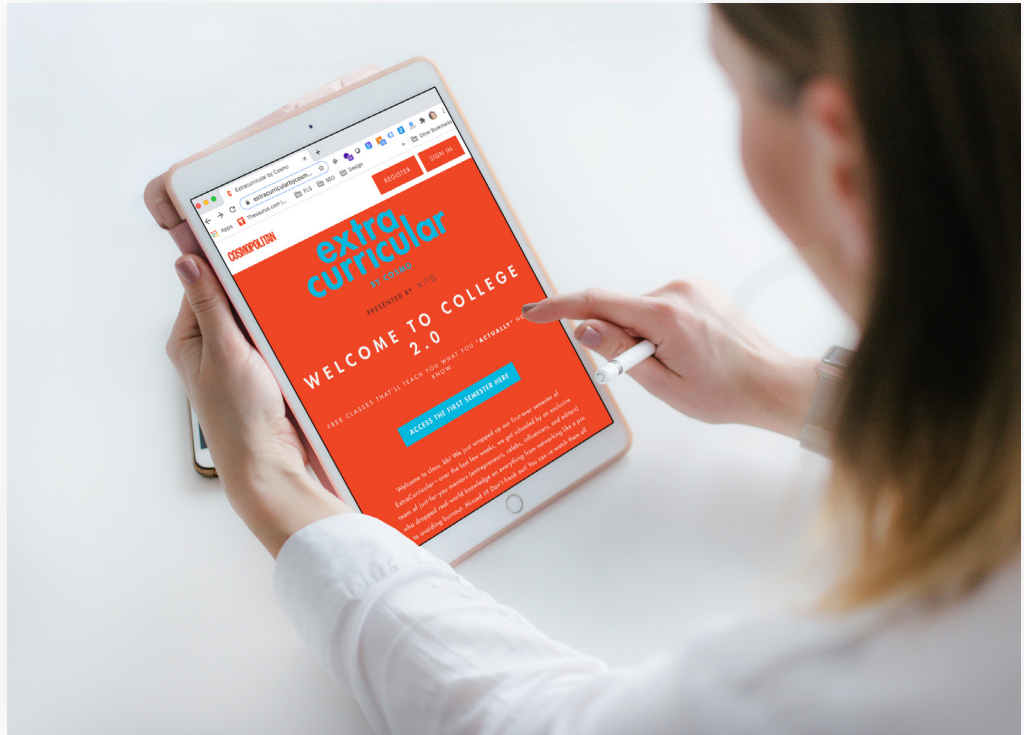
Source: NYT Store

REAL-WORLD EXAMPLES

3. Partner to Create Exclusive Content

If you have a niche audience who's highly engaged, this might be a good fit for you. Some publications are finding ways to host exclusive educational content with paid memberships. Again, this is a way not only to collect first-party data, but to monetize partnerships, too.

For example, Cosmopolitan partnered with XP5 to create a portal called College 2.0. It's a portal of classes hosted by entrepreneurs, celebrities, influencers, and editors. Topics range from interviewing and money, to psychology and time-management. To get access, users just need to buy one of Cosmo's subscriptions, (either \$2 a month or \$20 a month depending on the amount and frequency of content desired).



Source: Cosmopolitan

THE FUTURE OF DATA IS CONSENT

Implementing a first-party data strategy isn't about you, your company, or its campaign results. While those are certainly important, the ultimate goal is to put your customers - and the privacy of their data - first.

Being transparent with customers about how you use their data will be a make-or-break factor when it comes to your first-party data strategy.

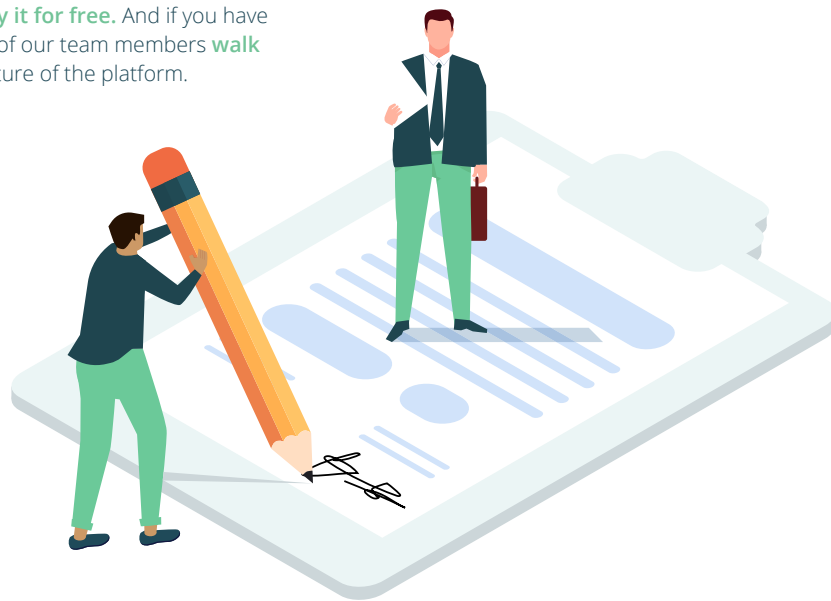
This new, customer-centric approach to advertising, marketing, and sales activities needs to be implemented with a privacy-first mindset. That means complying with global privacy regulations and collecting user consent and preferences across channels, domains, and devices.

You have two clear options to do this.

- 1. You can invest in a variety of tools and integrate them.**
- 2. You can use an all-in-one consent and preference management tool.**

If you prefer a one-stop-shop, OneTrust **PreferenceChoice** is the solution. Stacked with mobile app compliance, universal consent management, CMP, preference management, and more, it's the ultimate tool for making your first-party data strategy come to life.

Best part is, you can **try it for free**. And if you have any questions, let one of our team members **walk you through** each feature of the platform.



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