Surviving the Cookie Apocalypse:

A Guide for B2B Marketers

PEAKROAD PARTNERS

REACH PEAK PERFORMANCE & PROFITABILITY

As the era of tracking cookies comes to an end, marketers must pivot to a new approach that prioritizes transparency, consent, and privacy.

Contents

Introduction

To accept or deny cookies — that is the question. As consumers, we are used to the familiar pop-up on our webpages. Cookies remember where we have been on the web, providing personalized experiences, and saving our logins and shopping carts. Often, it's convenient, but it's a technology that's easy to exploit.

B2B marketers have evolved to use the data and technology at our fingertips. Our goal is to get better at targeting the right people at the right time to ultimately convert to sales down the road. But as targeted marketing becomes more precise, we often lose trust from our buyers. Where is the line between personalization and privacy?

According to Google, "If digital advertising doesn't evolve to address the growing concerns people have about their privacy and how their personal identity is being used, we risk the future of the free and open web."[1] In 2020, Google announced it will block all third-party cookies. Instead, web products will be powered by privacy-preserving APIs which prevent individual tracking but still deliver results for advertisers and publishers.

72% **of people feel that almost all of what they do online is being tracked by advertisers, technology firms, or other companies.**

81% **say that the potential risks they face because of data collection outweigh the benefits [2]**

[1] Google Ads & Commerce Blog, 2021

[2] Pew Research Center Study, 2019

Who does this affect, and when?

While the timeline has been pushed in the last several years, 2024 marks the year of the cookie apocalypse, and marketers need to know how these changes will impact them.

80% of advertisers have relied on third-party cookies to micro-target ads[3].

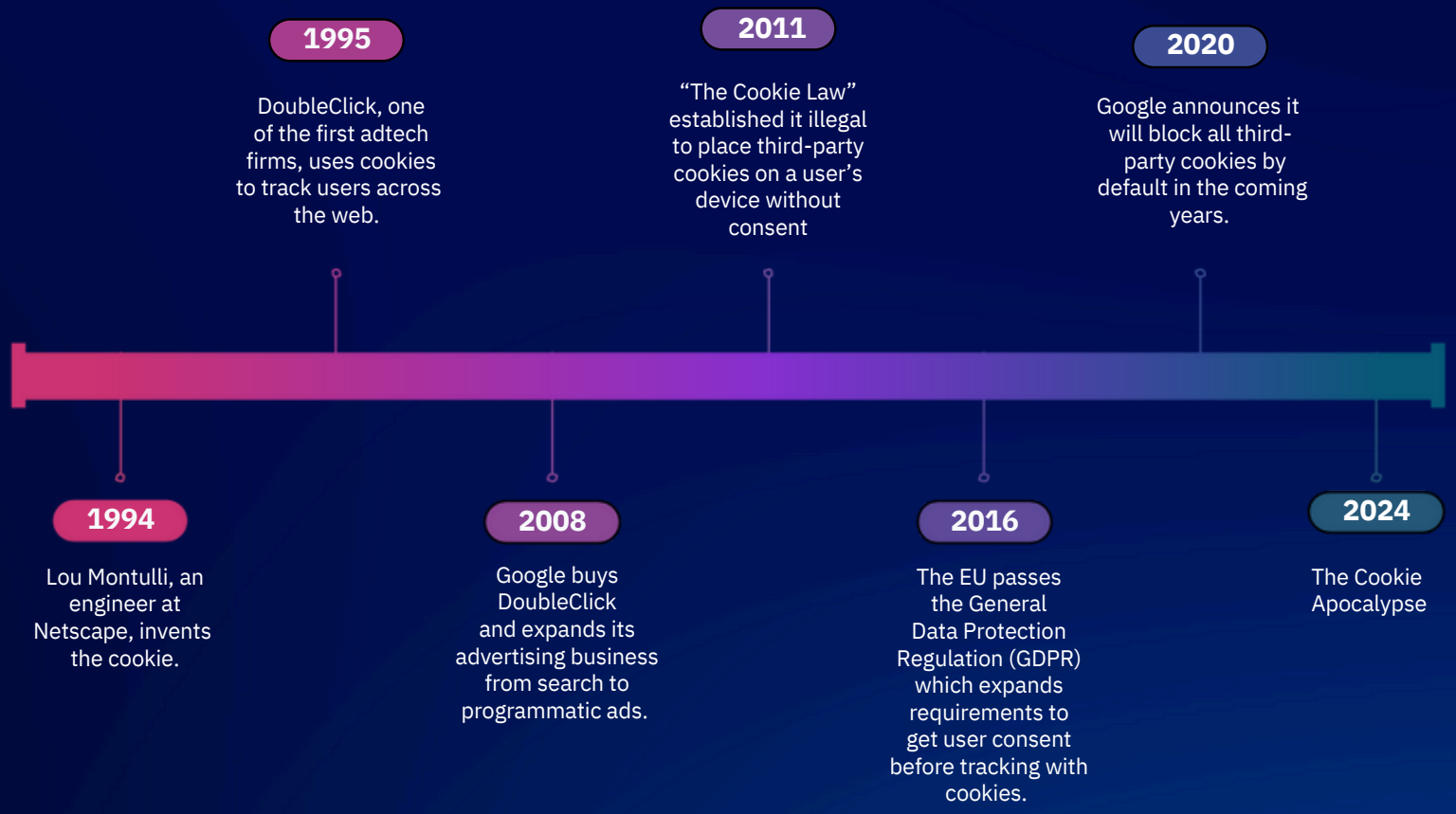
The deprecation of third-party cookies especially affects intent data vendors and account-based marketing (ABM) platforms. Many of these vendors use third-party cookies for user tracking and ad targeting.

[3] Epsilon Research Study, 2020

Don’t miss the survival checklist at the end of this eBook, complete with key questions to ask your marketing vendors.

Cookies 101: A Brief Overview

Did you know that cookies date back to 1994? A cookie — or html cookie, http cookie, internet cookie, or browser cookie — is a text file used to identify individual users browsing the web. Invented as a tool to help websites remember users, the original intent was to limit the memory to sessions on a singular page and to maintain user privacy. But then the third-party cookie entered the game. The third-party cookie can track visitor activities from one site to another. With this feature, advertisers can target a specific person with ads for products they seemed interested in.



There are several types of tracking cookies used on the internet, each serving different purposes.

Here's an overview of the most common types:

With increasing privacy concerns, many of these tracking cookies, especially third-party cookies, are being restricted or banned by regulations such as GDPR and CCPA, and by browser developers like Google and Apple. Marketers and advertisers are now forced to explore alternative methods, like first-party data collection and privacy-first solutions, to maintain personalization and engagement.

1. First-Party Cookies

- **Definition**: Cookies set by the website the user is visiting directly.
- **Purpose**: Used to remember user preferences, keep users logged in, and enhance the overall experience on the site.
- **Example**: A cookie storing your shopping cart information or login details for a specific website.

2. Third-Party Cookies

- **Definition**: Cookies set by a domain other than the one the user is currently visiting, often from external advertising or analytics companies.
- **Purpose:** Used primarily for tracking users across different sites to collect data for **advertising, retargeting, or behavioral analysis.**
- **Example:** Cookies from an ad network that track users across multiple websites to serve personalized ads.

3. Session Cookies

- **Definition**: Temporary cookies that are erased when the user closes the browser.
- **Purpose**: Used to keep track of a user's session on a website, like keeping them logged in while browsing multiple pages.
- **Example**: A cookie that remembers your inputs in an online form while you navigate through different sections of a website.

4. Persistent Cookies

- **Definition**: Cookies that remain stored on the user's device for a specific period, even after the session ends or the browser is closed.
- **Purpose**: Used for long-term tracking and remembering user preferences, authentication, or behavior across multiple sessions.
- **Example**: A cookie that remembers login credentials or language preferences for future visits.

5. Secure Cookies

- **Definition**: Cookies that are only transmitted over secure (HTTPS) connections.
- **Purpose**: Used to protect sensitive data from being transmitted insecurely, reducing the risk of interception.
- **Example**: A cookie storing session information for an online banking website.

6. HttpOnly Cookies

- **Definition**: Cookies that cannot be accessed by client-side scripts like JavaScript, increasing security.
- **Purpose**: Typically used to store session identifiers or other sensitive information to protect against cross-site scripting (XSS) attacks.
- **Example**: A cookie storing authentication information for a secure login.

7. SameSite Cookies

- **Definition**: Cookies with restrictions on when they are sent based on the originating site and the current site.
- **Purpose**: Used to mitigate cross-site request forgery (CSRF) attacks by controlling whether cookies are sent in cross-site requests.
- **Example**: Cookies used for managing secure authentication between different sites under the same brand.

8. Super Cookies

- **Definition**: Extremely persistent cookies that are stored outside regular cookie storage locations and are difficult to delete.
- **Purpose**: Used by some companies or advertisers to continue tracking users even after they delete their cookies.
- **Example**: Tracking mechanisms that can regenerate deleted cookies through browser loopholes.

9. Zombie Cookies

- **Definition**: Cookies that automatically reappear after being deleted.
- **Purpose**: Used for tracking users persistently, even when they try to remove tracking mechanisms.
- **Example**: Cookies that are recreated from backup data on the server side or by other tracking mechanisms.

First-Party Cookies vs. Third-Party Cookies

To truly understand the impact this change will have, let's break down the difference between first-party and third-party cookies. The distinction is based on who the cookie belongs to.

First-Party Cookies	Third-Party Cookies
• Belong to the owner of the website. • Created by host domain. Purpose is to • manage a single browsing session. Example: A first-party cookie can remember where on the website a user is visiting, and the changes made — like adding to a shopping cart. This information can only be accessed by the owner of the website.	• Belong to someone other than the website owner (e.g. ad tech platform) • Stored by browser on a user's computer so a third-party can gather the user profile. Purpose is to track • user activity across the web. Example: Third-party cookies are mostly used for advertising activities. Websites can make money by renting ad space. Third parties can place cookies via a tracking pixel or ad.

Cookies CAN: collect user information, track user behavior, remember the products and ads we clicked on, and know location and device.

Cookies CANNOT: obtain personal information from your computer, view passwords, or share viruses.

The War on Third-Party Cookies — And the Consequences

In the early 2000s, cookie usage was running rampant. A study by the Wall Street Journal in 2010 found that over 3,000 tracking files were installed on a test computer by over 50 sites.4 In 2011, we got the “Cookie Law,” that made it illegal to place third-party cookies on a user’s device without consent. With various legal directives over the last 20+ years, data privacy is a persistent trend that isn’t going anywhere. And while Google announced its imminent phase-out of third-party cookies, Safari and Firefox have already disabled the trackers.

The future of advertising is [third-party] cookie-less, and marketers and advertisers need to pivot to future- proof their strategies.

4 The Wall Street Journal, 2010

Surviving the Apocalypse: Strategies for B2B Marketers

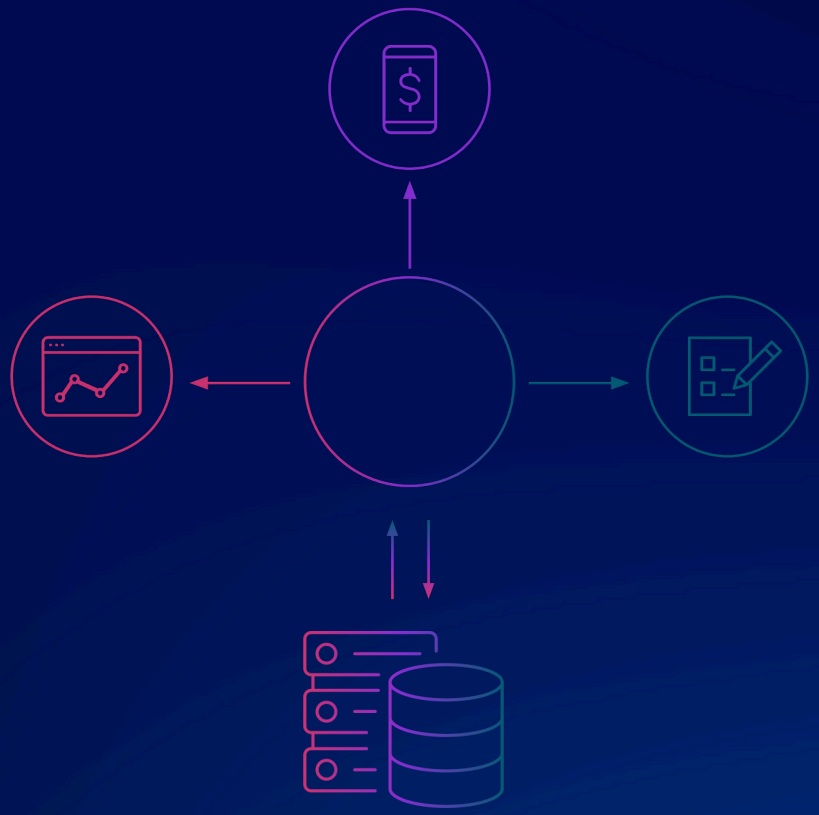
But the future of B2B marketing is not all doom and gloom — we have good news. There is a path to survival, with many emerging technologies and strategies that provide audience targeting value and privacy compliance. Considering these changes to the data privacy landscape — and challenges — you'll need to make sure your digital marketing programs are set up for success. Here are a few forward-thinking strategies.

1 Focus on First-Party Data

Without third-party cookies, marketers will need to focus on first-party data. This data is collected directly from your website or app, such as contact information, purchase history, and website activity.

In addition, there is “zero-party” or permission-based data. This is data that users explicitly provide to you through form fills, surveys, and polls. Encourage your visitors to share their information in exchange for valuable content, such as ebooks, webinars, and free trials.

If you don’t have one already, implement a customer relationship management (CRM) system to organize and analyze your customer data. This will help you personalize marketing efforts and improve customer experiences.



2 Expand Intent Signal Coverage

Some intent data vendors, use alternative identifiers to monitor target-buyer research activities and buying behaviors. For example, with access to numerous sources and types of digital data — including IP addresses, mobile ad IDs (MAIDs), hashed email address (HEMs), and more — Intentsify transforms disparate behavioral data points into actionable account and buying- group intelligence. B2B marketers and sellers gain a holistic view of buying-group activities, research patterns, and readiness, without the use of third-party cookies. Multiple data sources converge into one identity graph that provides high quality buyer-intent intelligence (as well as the ability to activate that intelligence via digital marketing programs).

By using a comprehensive identity graph, marketers and sellers can enhance full-funnel intent activation solutions such as lead generation and digital advertising.

3 Stay Informed and Compliant

Get acquainted with applicable data privacy regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Regularly monitor any changes and train your team on privacy practices and the ethical use of data.

And there's more...

In addition to the well-known GDPR (General Data Protection Regulation) in the European Union and CCPA (California Consumer Privacy Act) in the U.S., several other state and federal regulations are either being proposed or are already in effect. Marketers need to be aware of these emerging data privacy laws as they continue to evolve. Below are some significant regulations and trends that are likely to impact marketers in the near future:

1. CPRA (California Privacy Rights Act)

- **Status**: Passed (takes full effect in 2023)
- **Summary**: This is an update to CCPA, which strengthens consumer rights and introduces new obligations for businesses.
- **Key Impacts for Marketers:**
  - Establishes a new enforcement agency (California Privacy Protection Agency).
  - Introduces the right to correct inaccurate personal information.
  - Expands opt-out rights for the sale and sharing of personal data.
  - Requires businesses to honor user requests not to use personal data for behavioral advertising.

2. Virginia Consumer Data Protection Act (VCDPA)

- **Status**: Passed (Effective January 1, 2023)
- **Summary**: Virginia's law is similar to GDPR and CCPA but has some distinctions.
- **Key Impacts for Marketers:**
  - Gives consumers rights over how their personal data is processed, including the right to access, delete, and correct data.
  - Allows users to opt-out of targeted advertising.
  - This applies to businesses that process data from more than 100,000 consumers or derive more than 50% of revenue from selling personal data.

3. Colorado Privacy Act (CPA)

- **Status**: Passed (Effective July 1, 2023)
- **Summary**: Colorado's privacy law aligns closely with Virginia's VCDPA and California's CPRA.
- **Key Impacts for Marketers:**
  - Requires businesses to provide consumers with clear ways to opt-out of targeted advertising and the sale of their data.
  - Grants consumers rights to access, correct, delete, and move their data.
  - Obligates businesses to implement data minimization and purpose limitation strategies.

4. Connecticut Data Privacy Act (CTDPA)

- **Status**: Passed (Effective July 1, 2023)
- **Summary**: Similar to Colorado and Virginia's laws, Connecticut's legislation focuses on consumer data rights and the responsibilities of businesses.
- **Key Impacts for Marketers:**
  - Grants consumers the right to opt out of targeted advertising, data sales, and profiling.
  - Requires businesses to provide a privacy notice, disclose data collection, and give users the right to correct or delete data.

5. Utah Consumer Privacy Act (UCPA)

- **Status**: Passed (Effective December 31, 2023)
- **Summary**: Utah's privacy law is more business-friendly but still aims to protect consumer data.
- **Key Impacts for Marketers:**
  - Provides consumers the right to opt out of the sale of personal data and targeted advertising.
  - Requires businesses to disclose their data collection practices clearly..

6. New York Privacy Act (NYPA)

- **Status**: Proposed
- **Summary**: New York's Privacy Act is more stringent than CCPA, focusing on accountability and consumer rights.
- **Key Impacts for Marketers (if passed):**
  - Introduces fiduciary responsibility, which means businesses must prioritize consumer data protection over profit.
  - Provides consumers rights to access, delete, and correct their data.
  - Requires businesses to implement risk assessments and provide greater transparency around data processing.

7. Washington Privacy Act (WPA)

- **Status**: Proposed (failed to pass but may resurface)
- **Summary**: Washington has introduced various versions of its privacy law, which closely mirrors GDPR.
- **Key Impacts for Marketers (if passed):**
  - Grants consumers rights over their data, including deletion, access, and correction rights.
  - Requires businesses to conduct data protection assessments.
  - Places limits on the processing of sensitive data and targeted advertising.

8. Federal Privacy Law Proposals

While the U.S. does not yet have a comprehensive federal data privacy law, several bills have been proposed. These include:

American Data Privacy Protection Act (ADPPA)

- **Status**: Proposed
- **Summary**: This bipartisan bill aims to establish a nationwide standard for data privacy.
- Key Impacts for Marketers (if passed):
  - Introduces a clear federal framework for personal data handling.
  - Could preempt state laws, streamlining compliance but potentially weakening some state-level protections.
  - Gives consumers the right to opt out of targeted advertising and data sales.

9. Online Privacy Act (OPA)

- **Status**: Proposed
- **Summary**: Focuses on creating federal privacy standards, aiming to empower consumers with data rights.
- **Key Impacts for Marketers (if passed):**
  - Gives users more control over their personal data.
  - Establishes the Digital Privacy Agency to enforce privacy laws.
  - Provides strict requirements around consent for data collection and use.

10. Children and Teens' Online Privacy Protection Act (COPPA update)

- **Status**: Proposed
- **Summary**: An update to the Children's Online Privacy Protection Act (COPPA), this bill focuses on stricter privacy measures for children under 16.
- **Key Impacts for Marketers (if passed):**
  - Expands protections for teens, prohibiting data collection from children under 16 without consent.
  - Prohibits behavioral advertising targeted at minors.

Key Takeaways for Marketers

- **Shift to First-Party Data**: With the growing list of privacy regulations, marketers must shift their focus to collecting and leveraging first-party data, which is more compliant and sustainable.
- **Contextual Advertising:** As targeted advertising faces more restrictions, contextual advertising (ads based on the content being viewed, not personal data) is seeing a resurgence.
- **Enhanced Transparency**: Marketers must offer clearer explanations of data collection practices, with a focus on building trust with consumers.

Staying ahead of these emerging laws will be crucial for marketers to avoid hefty fines and maintain customer trust in the evolving landscape of data privacy.

Future-Proofed Marketing Programs

Next, let's dive into how intent data powers digital marketing programs. For many B2B marketers, audience targeting is falling short, and they aren't getting the most bang for their buck.

80% of marketers are not extremely confident in their ability to reach the right audiences programmatically5

1 in 3 marketers say wasted spend is their biggest advertising concern6

5 eMarketer Report
6 Merkle Study

Targeting only by IP address isn't enough to reach the entire audience. And many display ad solutions cannot ensure that the right messages are getting to the right people. That's where having a precise identity graph changes the game.

By expanding your reach and sharpening your targeting, you can increase conversions and accelerate pipeline. AI-enabled solutions can synthesize multi-sourced intent signals to identify in-market accounts, their research stage, and the issues they care about. Imagine stage and interest-relevant ads being served to selected personas at prioritized accounts. That's the future of digital advertising in a cookie-less world.

Check out our handy checklist to see if you're ready to survive the cookie apocalypse. →

Your Survival Checklist

1. Assess your current state

Do you know how your organization is using third-party cookies?

Make a list of teams, use cases, and systems that are impacted.

2. Discuss the Cookie Apocalypse with current vendors

How do your vendors use third-party cookies?

How do they collect data without third-party cookies?

What alternative identifiers are they using?

How do they measure the effectiveness of campaigns without third-party cookies?

Do they have a plan moving forward to future-proof their business?

3. Identify new solutions you'll need

Does your intent data provider use AI to understand research behavior?

Does your intent data provider offer a content syndication solution?

Do you have one provider for lead generation and ad solutions?

Are those programs activated based on intent signals?

PEAKROAD PARTNERS
REACH PEAK PERFORMANCE & PROFITABILITY

+1 740-2PEAKRD | 740-273-2573

801 West Big Beaver Rd
Suite 300
Troy, MI 48048

Email: info@peakroad.com

The impending "cookie apocalypse" marks a significant turning point in the world of digital marketing, and **the time to act is now.** As tracking cookies are phased out, marketers face a fundamental shift in how they reach and engage their audiences.

At Peak Road Partners, our team of experts is here to help you navigate this transformation with confidence. Whether through targeted projects or serving as your fractional strategic CMO, we offer comprehensive marketing support tailored to your unique needs.

From building first-party data strategies to implementing privacy-first solutions, we can help you stay ahead of the curve, ensuring your marketing remains effective and future-proof. **Don’t wait for tomorrow’s challenges—partner with us today and be prepared for what’s coming next.**

