

## The Rise of First-Party Data: How Marketers can Build Trust and Deliver Value in the Privacy Safe Era

Ananya Jha

Partner Lead, USA

### ABSTRACT

The digital marketing landscape is undergoing a profound transformation as privacy concerns and regulatory changes have brought about the decline of third-party cookies. This transition ushers in a new era in which advertisers can no longer rely on the comprehensive tracking capabilities that these cookies provided. This research paper explores the challenges and opportunities facing marketers in the post-cookie era. It examines the importance of building trust with consumers by prioritizing transparency in data collection and usage, emphasizing a clear value exchange to encourage data sharing.

Furthermore, the paper explores strategic adjustments required to reach target audiences. It analyzes the shift towards first-party data, focusing on building direct relationships with customers to gather insights. It also examines the potential of emerging technologies to create personalized, privacy-conscious marketing experiences. Finally, the paper highlights how success in this evolving landscape depends on prioritizing user privacy, delivering value alongside transparency, and embracing innovative marketing approaches.

### \*Corresponding author

Ananya Jha, Partner Lead, USA.

**Received:** December 06, 2022; **Accepted:** December 13, 2022; **Published:** December 20, 2022

**Keywords:** Digital Marketing, Third Party Cookie Deprecation, First Party Data, Data Integration, Marketing Effectiveness, Consumer Privacy, Creative Personalization, Privacy Regulations

### Introduction

First-party cookies are typically produced and stored on the user's device by the website that the user is viewing. Such cookies are frequently utilized to improve user experience and some of the site's essential capabilities. For example, first-party cookies can recognize returning customers so that they don't have to use the login and password to check in on subsequent trips. Third-party cookies are generated and stored on the user's device by a website other than the one being visited. They are created when a user accesses a website that contains parts from other sites, such as third-party photos or advertisements.

For example, whenever a person views an embedded video on a website, the video server will store cookies on their device. These cookies monitor user preferences and recommend related films when they visit the same video website.

The post-cookie era calls for marketers to embrace a mindset of experimentation and agility. Staying updated on the latest technological innovations and regulatory changes will be essential for maintaining success. Successful marketers will be those who focus on nurturing customer relationships, understanding the value of privacy, and delivering genuine value in every interaction. It requires a collaborative approach where marketers must work closely with data analytics and infrastructure teams, data scientists, and other stakeholders to create a holistic data strategy that

prioritizes privacy, transparency, and value for customers.

For years, the success of digital marketing heavily relied on third-party cookies, small text files that websites store to track online behavior across various sites. This allowed marketers to target advertising, personalize user experiences, and measure campaign effectiveness. However, the tide is shifting. Rising privacy concerns, regulatory bodies like the GDPR, and tech giants such as Apple and Google phasing out third-party cookies have created a sense of urgency for marketers to adapt to the post-cookie world.

This paper investigates how marketers can evolve their strategies to remain effective while respecting consumer privacy. It places a strong emphasis on re-establishing trust with customers through transparency, clear communication about data practices, and demonstrating the value exchange in customer interactions.

### Related Work

This literature review examines relevant scholarly work and industry reports to analyze the challenges, potential solutions, and the importance of trust in marketing strategies for the post-cookie world.

### Challenges of the Post-Cookie Era

The removal of third-party cookies will make it much more difficult for advertisers to track users around the internet and deliver them customized advertising messages. Furthermore, the elimination of cookies will make it more difficult for publishers to monetise their websites by eliminating the ability to offer targeted advertising [1].

By 2022, rules aimed at protecting consumer privacy-particularly the California Consumer Privacy Act-and large technology businesses will require users' explicit permission to share and use data generated by digital interactions. Because consumers are often uninformed of how their data is used and may not consent to sharing their data, the \$152 billion US digital advertising sector could lose access to most third-party data, which has driven programmatic advertising [2].

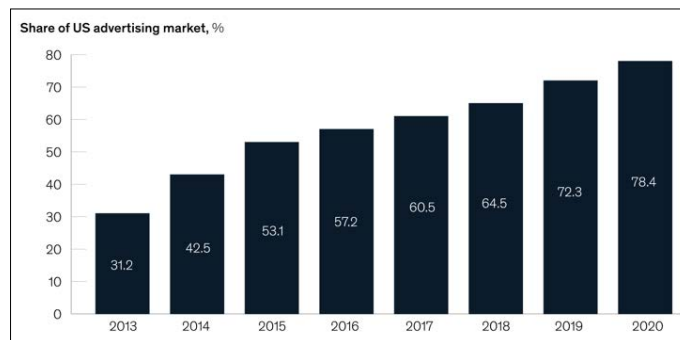


Figure 1: Spending on Programmatic Media has Increased as a % of US Advertising Market [2]

### Privacy Concerns

Data monetization and data sharing, which are enabled by organizations' use of digital technologies, can intensify technology-privacy issues among customers, regulators, and businesses. Figure 2 depicts a framework for understanding their individual ways to handle such tensions, which is based on structuration theory.

		Reactive	Proactive
Consumer data protection behavior	Information	<ul style="list-style-type: none"> <li><b>Falsification:</b> provide fake information in public posts or when asked by online service providers</li> <li><b>Avoidance:</b> refuse to provide information</li> <li><b>Self-censorship:</b> delete or edit past posts; contact the company to remove personal details; remove tags or unfriending</li> </ul>	<ul style="list-style-type: none"> <li><b>Restraint:</b> minimize user-generated content, such as social media posts and comments</li> <li><b>Encrypted communications:</b> email encryption or anonymous re-mailers; passwords for sensitive documents/data</li> <li><b>Non-digital alternatives:</b> face-to-face, traditional media</li> </ul>
	Permission	<ul style="list-style-type: none"> <li><b>Withdrawal:</b> remove cookies from browsers and computers; adopt ad blockers; delete apps when asked for information</li> <li><b>Fortification of identification:</b> change passwords after data breaches</li> <li><b>Communication termination:</b> opt-out from mailing lists and from other communications</li> </ul>	<ul style="list-style-type: none"> <li><b>Screening:</b> check server security (i.e., https); check the privacy policy</li> <li><b>Restriction:</b> turn off location-based access; change cookie settings</li> <li><b>Identity masking:</b> private browsing; virtual private networks (VPNs); The Onion Router</li> <li><b>Security consolidation:</b> use privacy-enhancing technologies such as pop-up window blockers, firewalls, and other internet security programs</li> </ul>
Data privacy regulation	Privacy policy	<ul style="list-style-type: none"> <li><b>Availability and visibility</b> of the privacy policy</li> </ul>	<ul style="list-style-type: none"> <li><b>Specification and promotion of consumer rights</b> in relation to data privacy</li> </ul>
	Managerial practices, enforcement	<ul style="list-style-type: none"> <li><b>Penalty for non-compliance</b></li> <li><b>Disclosure</b> of data breaches to customers and regulators</li> </ul>	<ul style="list-style-type: none"> <li>Obtain consumers' <b>consent</b> for the collection, use, and dissemination of personal information</li> <li>Provide consumers <b>access</b> to their own data and right to opt out, request to remove their data, or stop sharing it with third parties</li> <li><b>Privacy impact assessment and data protection governance</b></li> </ul>
Firm responses	Privacy approach	<ul style="list-style-type: none"> <li><b>Local approach:</b> aim to meet specific, local privacy regulations and laws</li> </ul>	<ul style="list-style-type: none"> <li><b>Universal approach:</b> tackle global privacy framework in a coordinated manner, and in anticipation of the changes in the overall regulatory framework, often targeting the most restrictive legal requirements</li> </ul>
	Privacy process	<ul style="list-style-type: none"> <li><b>Privacy as a feature:</b> privacy is only a value-added component of a product/service</li> <li>Improve <b>data security</b> by investing in cyber security technologies such as two-factor authentication, encryption, and tokens.</li> <li>Automated and standardized procedures to facilitate the <b>removal, transfer, or recovery of data</b>, especially upon customers' request.</li> </ul>	<ul style="list-style-type: none"> <li><b>Privacy by design:</b> privacy is embedded in all business processes, products, and services from the beginning to the final stage; security and privacy are default options for consumers</li> <li><b>Data collection:</b> zero party data</li> <li><b>Data discovery, categorization, and flow mapping:</b> categorizing types of data to ensure that firms only collect data that they actually need</li> <li><b>Ecosystem innovation:</b> involving third parties in data governance policy for more accountable business practices</li> </ul>

Figure 2: Privacy Responses Among Consumers, Regulators, and Firms [3]

### Building Trust in a Privacy-Focused Landscape

The most prepared advertisers create consumer experiences in which consumers voluntarily consent to sharing data (for example, transparency about data collection, insight into value exchange, and data collecting seamlessly integrated into user experience) [2].

The ideal experience varies greatly by industry, yet the demand for it drives many of the advertisers to innovate. For example, the most sophisticated organizations have separate customer experience segments that collaborate with media, IT, and legal to responsibly acquire and handle consumer data [2].

Building relationships is a crucial goal for products and services that are worth considering. However, for products with minimal attention or no direct link to customers, lifestyle content is a frequent workaround and can be branded as a separate digital experience from the parent brand, such as a CPG company’s cookery website [2].

### Strategy and Implementation

Harnessing First-Party Data: Advanced marketers link all data sources to have complete understanding of their target audience in order to enable personalized messaging and customer experience [4]. However, as illustrated in Figure 3, access and integration of first party data largely varies across industries and across companies as well

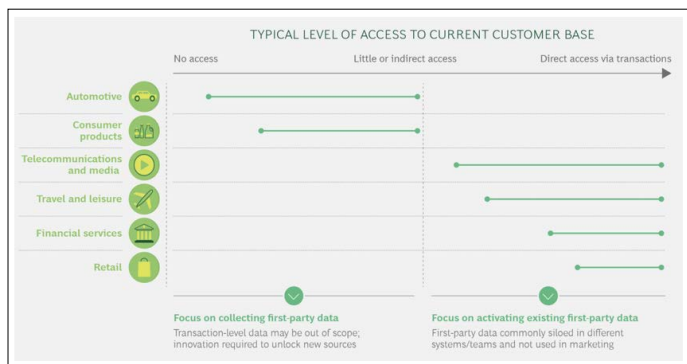


Figure 3: Variation in First Party Data Access Across Industries [4]

Subscription based companies like Netflix and New York Times automatically collect first party data at the time of account signup. Based on our consumption pattern, Netflix provides personalized recommendations and viewing experience.

Other industries and companies may not have such a straightforward relationship with data or may not have all the data pipes connected. This requires an organizational drive to invest in technology and align business strategy to measurement and marketing strategies as illustrated in Figure 4.

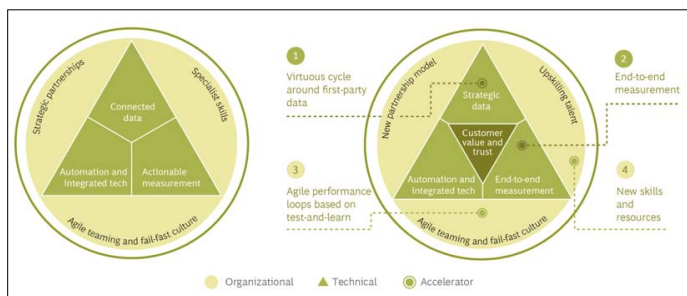


Figure 4: Digital Marketing Enablers Across the Organization [5]

In addition to strong data integration of first party data, there needs to be increased adoption of conversion modeling and predictive analytics based on the first party data in order to improve marketing effectiveness measurement. This also calls for a culture of agility - agility in terms of staying updated with new regulations, agility to test, learn and scale new technologies and agility in the organization to embrace the new measurement world which could be less unified and more dependent on predictive metrics instead of deterministic metrics.

An example beyond the subscription business model is North face who were able to leverage centralized tagging and analytics to quickly adapt to consumer needs and their search behavior within the site to catalog their products according to how the consumer was looking for it. This enabled them to 3X revenue and conversions. Usage of first party data with robust data integration not only influences the website customer experience but also informs the personalized creative messaging strategy thereby improving marketing effectiveness and business outcomes.

### Conclusion and Future Work

The deprecation of the third-party cookie is a catalyst for a more privacy-centric and responsible form of digital marketing. While it marks the end of an era, it should be viewed as the start of a more ethical, consumer-centric approach to digital marketing. This new era necessitates a mindset shift for marketers and requires investment in new technologies, data infrastructure and approaches. By demonstrating transparency regarding data collection and adhering to clear consent mechanisms, marketers can rebuild confidence with customers. Prioritizing first-party data and providing customers with compelling value in exchange for their information will be paramount. Investing in emerging technologies, such as AI-powered personalization and alternative targeting techniques, will be crucial for navigating this landscape [6,7].

The ongoing evolution of the digital marketing landscape and changes in privacy regulations pose both challenges and opportunities for future research and exploration. Here are some key areas for future work:

- **Impact of Privacy Laws:** Privacy laws are rapidly emerging across the globe. Future research could focus on the evolution of laws and its impact on marketers
- **Consumer Sentiment Research:** Longitudinal studies on examining changing consumer attitudes toward privacy and their expectations surrounding data collection and personalization will be crucial to shape customer-centric marketing strategies.
- **Emerging Technologies:** Investigating the potential of new technologies like differential privacy, privacy-preserving advertising solutions, and decentralized identity management can help define the future of privacy-conscious marketing.

By focusing on the core principles of trust, transparency, and value, marketers can successfully navigate these changes while delivering personalized and engaging experiences that respect user privacy and build long-term customer relationships.

### References

1. Forbes (2022) The Slow Death of Third-Party Cookies. <https://www.forbes.com/sites/theyec/2022/09/12/the-slow-death-of-third-party-cookies/?sh=112e67d34026>.
2. (2021) The Demise of Third-Party Cookies and Identifiers. McKinsey & Company <https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-demise-of-third-party-cookies-and-identifiers>.

3. Quach S, Thaichon P, Martin KD, Weaven S, Palmatier RW (2022) Digital technologies: tensions in privacy and data. J. of the Acad. Mark. Sci 50: 1299-1323.
4. Shilpa Patel, Dominic Field, Henry Leon (2020) Responsible Marketing with First-Party Data. Boston Consulting Group <https://www.bcg.com/publications/2020/responsible-marketing-with-first-party-data>.
5. Kristi Rogers, Javier Perez Moino, Henry Leon, Alberto Poncela (2021) The Fast Track to Digital Marketing Maturity. Boston Consulting Group <https://www.bcg.com/publications/2021/the-fast-track-to-digital-marketing-maturity>.
6. (2021) Experts Say the New Normal in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges. Pew Research Center <https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges/>
7. (2021) Sustainable First-Party Data Strategy. Think with <https://www.thinkwithgoogle.com/futureofmarketing/digitaltransformation/sustainable-first-party-data-strategy/>.

**Copyright:** ©2022 Ananya Jha. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.