Ekonomi İşletme ve Maliye Araştırmaları Dergisi
Journal of Economics, Business and Finance Research
e-ISSN: 2667-503X

Year: 2026 **Volume:** 8 **Issue:** 1 **Pages:**1-26

Article Received Date: 03.10.2025 **Article Accepted Date:** 27.01.2026

Article Published Date: 30.04.2026 **Doi:** 10.38009/ekimad.1795729

Review Article

A Systematic Literature Review of Zero, First, Second, and Third-Party Data in Digital Marketing: The Post-Cookie Era[1]

İbrahim Halil Efendioğlu*

Abstract

This study examines zero, first, second, and third-party data strategies in digital marketing through a systematic literature review (SLR), with a particular focus on the post-cookie era. Guided by the PRISMA 2020 protocol, the study qualitatively synthesizes 25 SSCI-indexed articles selected from the Web of Science Core Collection, covering the period 2021 to May 2025. By structuring the evidence through the Theory, Context, Characteristics, and Methodology (TCCM) framework, the review finds that the deprecation of third-party cookies is not merely a technical disruption. Instead, it represents a strategic shift toward consent-based and relationship-oriented data architectures, where marketing performance is increasingly shaped by legitimacy and governance. Zero-party data (ZPD), intentionally and proactively shared by consumers in exchange for a transparent value trade-off, and first-party data (FPD), behavioral data captured through a brand's own touchpoints, constitute the operational foundation of privacy-sensitive personalization. Second-party data (SPD), shared through managed partnerships, offers a controlled pathway to scale, whereas third-party data (TPD) sourced from external providers is increasingly characterized as a high-variance and risky resource due to declining transparency and "accuracy erosion." The literature highlights three dominant adaptation pathways: strengthening internal data infrastructure (CDP/CRM) to unify first-party signals, replacing deterministic tracking with probabilistic and customer-journey-based modeling approaches, and adopting privacy-preserving technologies such as blockchain. Overall, the study positions "personalization without tracking" as an integrated capability challenge spanning analytics, governance, and organizational design. By addressing the fragmented nature of the current literature identified through the TCCM analysis, this study integrates these findings into the proposed "Marketing Data Re-Architecture Triad," providing a unified strategic roadmap that effectively bridges the theoretical gap in the post-cookie era.

Keywords: *Digital Marketing, Third-party Cookies, Zero-party Data, First-party Data, Privacy Governance, Systematic Literature Review, TCCM Framework*

Jel Classification: *M30, M31*

---

[1] This study was presented at the 2nd International Congress on Social Sciences Research (USBAK), held on May 26–27, 2025, at Istanbul Medipol University.

* Assoc. Prof. Dr. İbrahim Halil Efendioğlu, Gaziantep University, Faculty of Economics and Administrative Sciences, Department of Business Administration, efendioglu@gantep.edu.tr ORCID NO: 0000-0002-4968-375X

Cite: Efendioğlu, İ.H. (2026). A Systematic Literature Review of Zero, First, Second, and Third-Party Data in Digital Marketing: The Post-Cookie Era. *Ekonomi, İşletme ve Maliye Araştırmaları Dergisi,* 8(1), 1-26.

Dijital Pazarlamada Sıfırıncı, Birinci, İkinci ve Üçüncü Taraf Verilere İlişkin Sistematik Literatür Derlemesi: Çerez Sonrası Dönem

Öz

Bu araştırma, dijital pazarlamada sıfırıncı, birinci, ikinci ve üçüncü taraf veri stratejilerini, özellikle çerez sonrası (post-cookie) döneme odaklanarak sistematik bir literatür taraması (SLR) ile incelemektedir. PRISMA 2020 protokolü rehberliğinde yürütülen çalışmada, Web of Science Core Collection veri tabanından seçilen ve 2021-2025 (Mayıs) dönemini kapsayan 25 SSCI indeksli makale nitel sentez yöntemiyle analiz edilmiştir. Kanıtların Teori, Bağlam, Karakteristik ve Metodoloji (TCCM) çerçevesinde yapılandırıldığı inceleme sonucunda, üçüncü taraf çerezlerin kullanımdan kaldırılmasının yalnızca teknik bir aksama olmadığı; pazarlama performansını meşruiyet ve yönetişimin şekillendirdiği, rızaya dayalı ve ilişki odaklı veri mimarilerine doğru stratejik bir kaymayı temsil ettiği belirlenmiştir. Tüketicilerin niyetlerini şeffaf bir değer takası karşılığında proaktif paylaştığı sıfırıncı taraf veriler (ZPD) ve markanın kendi temas noktalarından elde edilen davranışsal birinci taraf veriler (FPD), gizliliğe duyarlı kişiselleştirmenin operasyonel temelini oluşturmaktadır. Yönetilen ortaklıklar aracılığıyla paylaşılan ikinci taraf veriler (SPD) ölçek kazanmak için kontrollü bir yol sunarken, harici sağlayıcılardan alınan üçüncü taraf veriler (TPD), azalan şeffaflık ve "doğruluk erimesi" nedeniyle giderek daha yüksek varyanslı ve riskli bir kaynak olarak nitelendirilmektedir. Literatürde üç temel uyum yolu öne çıkmaktadır: birinci taraf sinyalleri birleştirmek için dahili veri altyapısının (CDP/CRM) güçlendirilmesi, deterministik takibin yerini olasılıksal ve müşteri yolculuğu tabanlı modellemelerin alması ve blok zinciri gibi gizliliği koruyan teknolojilerin benimsenmesidir. Sonuç olarak çalışma, "izleme olmaksızın kişiselleştirmeyi" analitik, yönetişim ve organizasyonel tasarımı kapsayan entegre bir yetenek meydan okuması olarak konumlandırmaktadır. Genel olarak bu çalışma, "izleme olmaksızın kişiselleştirmeyi" analitik, yönetişim ve organizasyonel tasarımı kapsayan entegre bir yetenek meydan okuması olarak konumlandırmaktadır. TCCM analizi aracılığıyla tespit edilen mevcut literatürün parçalı yapısını ele alan bu çalışma, elde edilen bulguları önerilen "Pazarlama Verisi Yeniden Mimari Üçlüsü" içerisinde bütünleştirerek çerez sonrası dönemdeki teorik boşluğu etkili bir şekilde kapatan birleşik bir stratejik yol haritası sunmaktadır.

Anahtar Kelimeler: *Dijital Pazarlama, Üçüncü Taraf Çerezler, Sıfır Taraf Veri, Birinci Taraf Veri, Gizlilik Yönetişimi, Sistematik Literatür Taraması, TCCM Çerçevesi*

Jel Sınıflandırması: *M30, M31*

1. Introduction

Digital marketing is increasingly shaped by data-driven strategies aimed at optimizing customer engagement, delivering personalized experiences, and enhancing advertising effectiveness (Tarabasz, 2024; Theodorakopoulos & Theodoropoulou, 2024). Within this ecosystem, consumer data is classified into four fundamental categories based on its source and collection method: zero-party data (ZPD), voluntarily shared by consumers; first-party data (FPD), obtained from direct interactions between the brand and the consumer; second-party data (SPD), shared among trusted business partners; and third-party data (TPD), collected from various external sources (Karuppuchamy, 2025; Quach et al., 2022).

For many years, businesses have relied heavily on third-party cookies and the resulting TPD strategies to track user activities (Rasaii, 2023). However, increasing global data privacy regulations (such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) and the phased removal of third-party cookies by major browsers are fundamentally transforming how data is managed in marketing processes (Lim & Oh, 2025; Pantelic et al., 2022; Sara & Ayoub, 2024). This shift compels marketers not only to undergo technological transformation but also to develop more ethical, customer-centric data-collection strategies (Çınar & Ateş, 2022; Ruzive et al., 2023).

The current literature indicates that, with the loss of third-party cookies, businesses are shifting toward ZPD and FPD models based on direct consumer interaction (Elmér & Nilsson, 2022; Erceg & Phan, 2024; Sharma, 2023). This strategic shift represents a new value exchange where transparency between brands and consumers becomes a competitive advantage. In particular, artificial

intelligence-powered analytics and CRM systems help sustain personalized strategies by processing these new data layers (Kihn & Lin, 2024; Kumar, 2025).

Despite this, academic literature remains fragmented regarding the integration of these data strategies (ZPD, FPD, SPD, and TPD) in the post-cookie era, the challenges encountered, and the application models. To address this gap, the present study aims to comprehensively map data strategies in digital marketing through a systematic literature review (SLR) following the PRISMA protocol. The study is structured around the following research questions:

RQ1: How are the concepts of zero, first, second, and third-party data defined within the context of digital marketing?

RQ2: How do emerging privacy-preserving technologies and strategies mitigate signal loss while maintaining personalization effectiveness in the post-cookie era?

RQ3: What types of ethical, legal, and operational challenges arise during the transition to privacy-oriented data collection processes?

In addition to mapping and comparing ZPD, FPD, SPD, and TPD in a single SLR, this study makes two primary originality-oriented contributions to the post-cookie literature. First, it provides a theory-driven synthesis of "personalization without tracking," moving beyond purely descriptive taxonomies to offer a mechanism-based explanation of how personalization can be sustained without invasive tracking by linking data types to (i) performance conditions and (ii) legitimacy conditions. Second, it advances a novel conceptual framework, the "Marketing Data Re-Architecture Triad," which integrates first-party strategy, technical signal-loss mitigation, and privacy governance. By addressing the fragmented nature of the current literature identified through the TCCM analysis, this triad translates descriptive findings into a theory-consistent, testable roadmap that effectively bridges the theoretical gap in the post-cookie era.

2. Literature Review

In the domain of digital marketing, ZPD, FPD, SPD, and TPD data play a critical role in enabling firms to understand consumer behavior, design personalized marketing strategies, and optimize advertising targeting (Chanda & Pabalkar, 2024). With the deprecation of third-party cookies, businesses are increasingly shifting toward direct consumer data collection and privacy-friendly data strategies. This transition is not merely technical but represents a fundamental shift in the value exchange between brands and consumers, where transparency becomes a competitive advantage (Acquisti, 2023). Each data category differs in terms of its source, applications, advantages, and inherent challenges.

2.1. Zero-Party Data

Zero-party data (ZPD) is information that consumers intentionally and voluntarily provide to brands with explicit consent. This category represents the most privacy-compliant type of data (Kilinc, 2024). Such data is often collected through surveys, forms, loyalty programs, account settings, or interactive content. In the privacy-first era, especially as third-party cookies phase out, ZPD has become a strategic imperative for eCommerce firms that aim to sustain personalization without relying on opaque tracking practices (Karuppuchamy, 2025). For example, when a consumer specifies preferred product categories on an e-commerce platform or selects favorite items within a mobile app, these inputs qualify as ZPD.

This type of data provides businesses with highly accurate insights, as it reflects consumers' self-reported preferences. It enables marketers to design personalized advertisements, foster customer loyalty, and enhance overall experiences (Rolando & Mulyono, 2024). Because ZPD relies on declared preferences rather than inferred signals, it can support more precise journey orchestration and anticipatory service while maintaining more substantial alignment with consumers' privacy

expectations (Choi et al., 2025). However, the primary challenge lies in consumers' potential reluctance to disclose such information voluntarily.

2.2. First-Party Data

Firms directly collect first-party data (FPD) from their own customers or users. It originates from sources such as websites, mobile applications, purchase histories, email interactions, and loyalty programs (Ham & Lee, 2025). For instance, a consumer's browsing behavior or purchase history on an e-commerce platform is considered FPD.

The main advantage of FPD is that it belongs entirely to the business and can be managed internally. It is more compliant with privacy regulations and is generally of high quality. However, its scope is typically limited to the existing customer base (Liu & Li, 2024). Therefore, businesses must design strategies to expand data collection by increasing consumer engagement. FPD enables brands to integrate customer-derived signals into marketing analytics and campaign execution, reducing reliance on third parties, strengthening personalization, and protecting privacy (Sousa, 2022). Additionally, FPD strategies offer significant advantages over third-party approaches, including greater control over customer data capture, the ability to develop a deeper understanding of customer behavior and intentions, and easier integration into marketing analytics and operational processes (Latvala et al., 2022).

ZPD refers to data generated when consumers knowingly and explicitly disclose preferences, such as "My size is M," "I prefer vegan products," or "I am interested in these categories," to a brand. In contrast, FPD is the data a brand collects from its direct interactions with consumers (e.g., website or app behavior, purchase history, email engagements, and customer service records).

2.3. Second-Party Data

Second-party data (SPD) refers to another company's FPD that is shared through trusted partnerships or formal data-sharing agreements (Liu & Li, 2024). For example, an airline may share its loyalty program data with a hotel chain. Such data enables more precise campaign targeting and enriches customer experiences.

In practice, SPD allows two brands to match customer lists or segment information in a controlled manner to define target audiences in greater detail (Johnson & Ahmed-Kristensen, 2025). For instance, a ticketing platform's customer email list and segment information can be matched with a social network's user profiles to derive demographic and behavioral profiles of those segments and to identify new prospective customers with similar characteristics (Schneider et al., 2017).

Its primary advantage lies in its high accuracy and reliability, while also offering firms access to potential new customer segments (Block et al., 2025). However, this approach requires establishing trustworthy partnerships and ensuring compliance with legal data-sharing protocols (Sponder & Khan, 2017). Moreover, when the scope of data sharing is not clearly defined, exposing strategic assets such as customer lists to the partner and increasing privacy risks can emerge as critical challenges that must be carefully managed in SPD initiatives.

2.4. Third-Party Data

TPD refers to information gathered from a wide range of external sources and commonly distributed or sold by data providers. Advertising technology companies analyze this data to help marketers build audience segments (Chauhan & Sethi, 2024). For example, consumer browsing behavior captured via cookies and aggregated by external providers constitutes TPD.

This type of data offers the advantage of broad reach, enabling access to new segments (Schneider et al., 2017). Nonetheless, it is increasingly restricted by regulations such as GDPR and CCPA. Furthermore, outdated or inaccurate information poses additional risks. With browser providers

phasing out third-party cookies, reliance on this data category is steadily declining (Fakeyede et al., 2023).

Consequently, third-party data is information collected by external data providers from multiple sources where the brand has no direct relationship with the consumer, and it is typically sold or shared with many firms to enable broad reach and scale in prospecting (Huang, 2025), but it often comes with more variable accuracy, freshness, transparency, and perceived consent complexity; in contrast, zero-party data is information consumers intentionally and proactively tell the brand (e.g., preference centers, surveys), making it highly explicit and usually more reliable for personalization; first-party data is gathered directly by the brand through its own touchpoints (website, app, CRM, in-store, call center), giving the brand strong control and generally higher trustworthiness; and second-party data is essentially another company's first-party data shared through a direct, trusted partnership (e.g., airline and hotel), which is typically more source-defined and higher quality than TPD, but requires partner governance and alignment (Feth et al., 2025; Majeti, 2025).

2.5. Cookies and Their Functions

Cookies are text files that track user behavior and personalize web experiences. They serve functions such as authentication, personalization, analytics, and advertising targeting (Sakalauskas & Kriksciuniene, 2024). Cookies are generally divided into two categories: first-party cookies (collected by the company's own website) and third-party cookies (provided by external entities).

First-party cookies are primarily used for session management, storing user preferences, and tracking site analytics. In contrast, third-party cookies facilitate behavioral targeting, retargeting, and programmatic advertising (Zhou et al., 2024). Due to growing privacy concerns and regulatory interventions, the elimination of third-party cookies has necessitated the development of alternative strategies to address these concerns. These include enhanced FPD collection, device fingerprinting, Google's Privacy Sandbox, and contextual advertising approaches.

The deprecation of third-party cookies is not merely a technical loss of targeting capability. It represents a structural shift that compels digital marketing to be re-architected around consent, transparency, and data governance (Çınar & Ateş, 2022). This rupture is pushing firms to strengthen direct consumer touchpoints and move toward relationship-based data architectures grounded in FPD and ZPD, while also elevating approaches such as contextual targeting and privacy-enhancing technologies to a more strategic role. However, if alternative solutions are designed solely for performance rather than aligned with principles such as data minimization, purpose limitation, retention controls, and accountability, they may trigger trust erosion and compliance risks (Lockitt, 2024). Accordingly, competitive advantage in the post-cookie era is shaped less by simply diversifying data sources and more by a brand's ability to build permission-based data practices supported by a clear consumer value proposition and robust, end-to-end data governance capabilities.

2.6. Theoretical Anchors: Social Exchange Theory and Privacy Paradox

The evolution of data-driven strategies in digital marketing is not merely a technological transition but a psychological and sociological process in which the relationship between consumers and brands is redefined (Behare et al., 2024). To understand the post-cookie data strategies examined in this study, two foundational theories emerge: Social Exchange Theory and the Privacy Paradox.

Social Exchange Theory explains social behaviors through a cost-benefit analysis. From this perspective, consumers view their personal data as a "bargaining chip" and decide to share it based on the balance between expected benefits such as personalized experiences, exclusive discounts, or convenience and potential costs, including the loss of privacy or data security risks (Degutis et al., 2023; Elangovan et al., 2025; Luo, 2002). The collection of ZPD represents the most concrete application of this theory. When consumers proactively disclose their intentions and preferences, they are engaging in a transparent value trade-off (Phan & Erceg, 2024). Consequently, in the post-cookie

era, a brand's success in data acquisition depends no longer on the technical power of tracking technologies but on the credibility and fairness of the value proposition offered to the consumer.

Conversely, the Privacy Paradox offers a critical framework for understanding consumers' contradictory attitudes in digital environments. This concept refers to the gap between individuals' high privacy concerns and their practical behaviors of continuing to share data despite these concerns (Barth & De Jong, 2017). The deprecation of third-party cookies and the tightening of global regulations (e.g., GDPR, CCPA) are direct results of rising societal privacy concerns (Pantelic et al., 2022). However, consumers often continue to disclose data because they are unwilling to sacrifice the comfort of personalized services (Awad & Krishnan, 2006). This paradox creates both an opportunity and a risk for marketers: while consumers declare significant concern, they are inclined to share data with platforms they trust and that possess transparent governance mechanisms. In this context, the death of cookies is a structural break aimed at reducing the tension of the privacy paradox; it compels brands to shift from "hidden tracking" toward "consent-based interaction".

These two theoretical lenses form the bedrock of the strategic framework proposed in this study. While Social Exchange Theory explains the operational value and trade-off mechanism of data, the Privacy Paradox highlights the underlying need for governance and legitimacy in data management.

3. Method

This study employs a Systematic Literature Review (SLR) to synthesize how ZPD, FPD, SPD, and TPD are conceptualized within the digital marketing landscape, particularly in response to heightened privacy expectations and the deprecation of third-party cookies. The review process was conducted and reported in strict accordance with the PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) statement to ensure transparency, objectivity, and replicability (Page et al., 2021).

3.1. Search Strategy and Identification

The Web of Science (WoS) Core Collection was selected as the primary database due to its rigorous indexing of high-impact journals in marketing, management, and information systems. The search was conducted in May 2025 using a comprehensive query designed to capture all facets of data-driven marketing strategies:

Query: (“Zero-Party Data” OR “First-Party Data” OR “Second-Party Data” OR “Third-Party Data”)

The query was executed using the WoS “Topic” search option (Title, Abstract, and Keywords) to maximize retrieval sensitivity, and the results were filtered at the database level to the 2021 to May 2025 publication window before screening.

The initial search returned n = 383 records. Given that the search was conducted within a single high-quality database (WoS) with specific parameters, no duplicate records were identified (n = 0). Thus, all 383 records proceeded to the screening phase.

WoS Core Collection was selected because it provides rigorously indexed, high-impact, peer-reviewed journals across marketing, management, and information systems, thereby supporting transparency and replicability in line with PRISMA 2020 (Page et al., 2021).

3.2. Screening

The screening process was conducted in two distinct stages. First, in the title and abstract screening stage, all 383 records were assessed for topical relevance. Records were excluded if they were unrelated to marketing, published in non-peer-reviewed formats (e.g., editorial notes, book reviews), or focused solely on technical data structures without strategic marketing implications; during this stage, n = 308 records were excluded. Second, in the full-text retrieval stage, the remaining 75 articles

were sought for full-text assessment; all were successfully retrieved and moved to the eligibility phase.

Excluding non-marketing studies, non-peer-reviewed publication types, and papers focused only on technical data structures (without strategic marketing implications) ensured that screening remained aligned with the research questions and preserved the interpretability of the synthesis.

3.3. Eligibility

The n = 75 full-text articles were rigorously assessed against a set of predefined inclusion and exclusion criteria. Studies were deemed eligible if they met the following requirements:

- **Timeframe:** Published between 2021 and 2025 (capturing the post-cookie transition era).
- **Language:** Written in English.
- **Context:** Situated within marketing, advertising, or consumer behavior.
- **Indexing:** Published in journals indexed in the Social Sciences Citation Index (SSCI).
- **Contribution:** Provided empirical or conceptual insights into data strategies, privacy governance, or personalization.

Upon detailed review, n = 33 articles were excluded for not meeting these specific criteria (e.g., non-SSCI status, lack of direct marketing focus, or contextually irrelevant data applications). This resulted in n = 42 studies meeting the formal eligibility criteria.

The 2021–2025 timeframe was chosen to capture the post-cookie transition period. English-only articles were used to maintain coding consistency and comparability. Restricting to SSCI-indexed journals served as a quality threshold, improving the reliability of the evidence base.

3.4. Inclusion and Qualitative Synthesis

In the final stage, the 42 eligible studies underwent a "market-focused" depth analysis to ensure the highest degree of relevance to the research questions. A further 17 studies were excluded because, although they discussed data, their primary focus was not on marketing decision-making or strategic personalization models. Consequently, a final corpus of n = 25 studies was included in the qualitative synthesis. Due to the methodological heterogeneity of the included studies (ranging from conceptual frameworks to diverse empirical designs), a meta-analysis was not performed (n = 0).

More specifically, the corpus is heterogeneous in (i) outcome operationalizations (ad effectiveness, conversion, CLV-related metrics, trust, compliance risk), (ii) unit of analysis (individual disclosure behavior, segment validity, platform-level targeting performance), and (iii) study designs and measures (field experiments, ML-based prediction, conceptual and critical analyses). This diversity prevents extracting commensurable effect sizes under a common metric, making a qualitative synthesis more appropriate for theory-building and mechanism mapping.

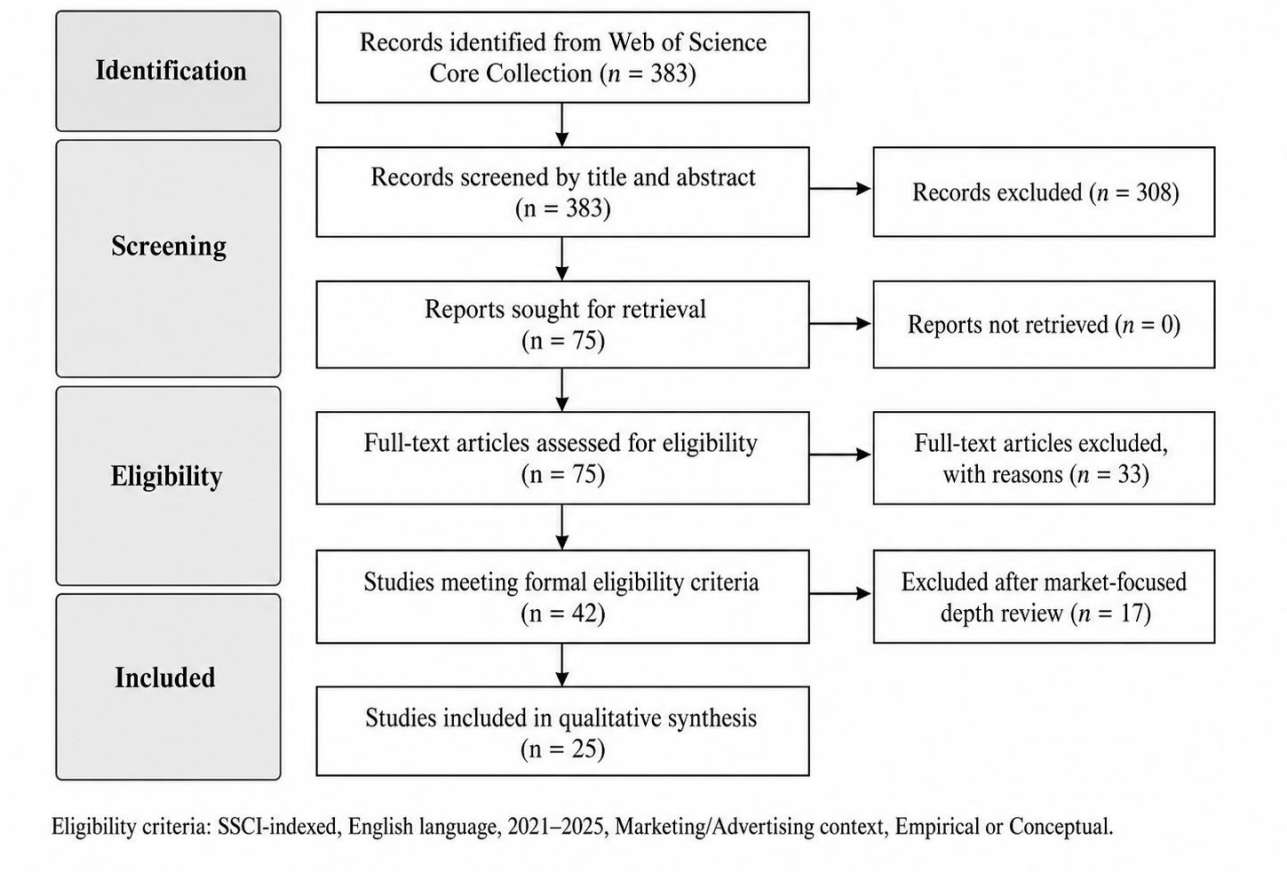
The final “market-focused” review was applied because some papers mentioned data types but did not address marketing decision-making, personalization strategy, or marketing outcomes. A meta-analysis was not conducted due to substantial heterogeneity in designs and measures (Page et al., 2021). The TCCM framework was used to systematically map theoretical, contextual, data-type, and methodological variation (Sharma & Kushwah, 2025). Accordingly, the present review should be read as an interpretive, theory-building synthesis that maps mechanisms, boundary conditions, and governance logics, rather than as a pooled estimate of an average effect size.

To ensure a systematic analysis, the final 25 articles were coded using the TCCM (Theory, Context, Characteristics, Methodology) framework (Sharma & Kushwah, 2025). This allowed for a structured mapping of:

- **Theories** applied (e.g., Privacy Paradox, Social Exchange Theory).
- **Contexts** (e.g., E-commerce, social media, retail).
- **Characteristics** of data types (ZPD, FPD, SPD, TPD).
- **Methodologies** used (e.g., experiments, surveys, case studies).

The complete selection process is visualized in the PRISMA flow diagram (Figure 1).

Figure 1: PRISMA Flow Diagram



4. Findings

Although several included studies originate from high-stakes domains such as healthcare, education, and transportation, they are retained only insofar as they inform marketing-relevant mechanisms (e.g., consent architecture, trust formation, governance capacity, and personalization constraints). In other words, these contexts are treated as boundary conditions that sharpen, rather than dilute, the marketing logic of the post-cookie transition, because they amplify the consequences of privacy governance for marketing outcomes.

The systematic synthesis of the 25 included studies reveals a significant strategic shift in digital marketing data management. This section presents the findings categorized by descriptive trends, methodological rigor, and thematic evolution, with a specific focus on the transition from third-party ecosystems to privacy-centric data models.

4.1. Descriptive Analytics and Publication Trends

The distribution of studies from 2021 to 2025 (May) indicates a burgeoning interest in data privacy and alternative data strategies. While the period began with a focus on data accuracy and social media

metrics (2021, n=5), 2024 (n=8) marked a peak in empirical evaluations of post-cookie technologies. Table 1 provides a comprehensive mapping of the final corpus.

Table 1: Mapping of the Reviewed Literature

Author(s) & Year	Research Context	Data Focus	Methodology	Key Contributions / Findings
Yu et al. (2021)	Social media	TPD	Content Analysis	Identifies significant "noise" and inaccuracy in social media altmetrics, challenging TPD reliability.
Shaw et al. (2021)	Transportation	SPD/TPD	Empirical	Validates the integration of targeted marketing data into specialized sectors like transportation.
Khan & Patire (2021)	Traffic/Ad-Tech	TPD	Experimental	Explores TPD fusion for performance measures, highlighting technical integration complexities.
Gopal et al. (2021)	User Privacy	ZPD/FPD	Longitudinal	Analyzes the "Privacy Paradox," showing users share ZPD when benefits (e.g., safety) are clear.
Chen et al. (2021)	Social Data	TPD	Experimental	Focuses on authenticity verification in outsourced social data to mitigate TPD security risks.
Wu et al. (2022)	Recommender Sys.	TPD	Deep RL	Demonstrates vulnerabilities (poisoning attacks) in recommendation systems using external data.
Polonioli (2022)	Consumer Strat.	ZPD	Conceptual	Critically examines ZPD as a strategic alternative to tracking, emphasizing explicit consent.
Kim (2022)	Smart Services	FPD	Case Study	Designs customer experiences based on iterative FPD engagement cycles in smart systems.
Canaway et al. (2022)	Primary Care	FPD/SPD	Exploratory	Maps perspectives on secondary use of datasets in high-stakes healthcare environments.
Bertheau & Lindner (2022)	Economic Data	TPD	Empirical	Examines the role of external data signals in the energy transition and foreign aid context.
Sanfilippo et al. (2023)	LMS/Education	SPD/TPD	Mixed-Method	Reveals a severe "governance gap" where third-party trackers bypass educational privacy intent.
Neumann et al. (2023)	B2B Marketing	FPD/TPD	Field Experiment	Statistically proves that TPD segments are often no more accurate than random targeting.
McGuigan et al. (2023)	Ad-Tech Industry	TPD	Critical Analysis	Interprets the "privacy pivot" as a strategic move by big platforms to consolidate market power.

Table 1 (Continued): Mapping of the Reviewed Literature

Jiang et al. (2023)	Link Prediction	FPD	Experimental	Proposes local differential privacy frameworks to protect FPD during predictive analytics.
Rauti et al. (2024)	E-Pharmacy	TPD	Network Analysis	Documents high-risk data leaks on online pharmacy sites through unregulated TPD trackers.
Padilla et al. (2024)	Customer Journey	FPD	Probabilistic ML	Positions the customer journey as a primary FPD source using probabilistic modeling.
Nugroho et al. (2024)	AI Interaction	ZPD	Exploratory	Investigates ZPD-like interactions and experience value in Gen-AI (ChatGPT) usage.
Chen et al. (2024a)	Social Science	TPD	Case Study	Highlights the operational hurdles and ethical constraints of collecting social media data.
Chen et al. (2024b)	SME Manufac.	FPD	Empirical	Identifies factors for successful digital transformation in SMEs using internal data flows.
Bordel Sánchez (2024)	Data Marketplace	FPD/SPD	Experimental	Introduces Blockchain for monetizing SPD without exposing individual consumer identities.
Akinnubi et al. (2024)	Social Graphs	SPD/TPD	Case Study	Utilizes knowledge graphs to unify multi-source heterogeneous social network data.
Ahmadi et al. (2024)	Online Ads	FPD/SPD	Field Experiment	Explores audience segment selection as an optimization problem under targeting constraints.
Li et al. (2025)	Finance/Fraud	TPD	Empirical	Analyzes alternative TPD as an external governance mechanism for corporate monitoring.
Leiva-Araos et al. (2025)	Healthcare Mgmt	FPD	Empirical	Optimizes patient management using ML-based FPD analysis in primary healthcare.
Ham & Lee (2025)	Digital Advertising	FPD/TPD	Mixed-Method	Confirms FPD's superiority over TPD in optimizing CLV and designing retargeting.

4.2. Methodological Synthesis

The literature exhibits a strong leaning toward Quantitative (64%) and Experimental (36%) designs. A shift is observed from simple descriptive analytics to high-complexity predictive modeling (e.g., Bayesian ML and Reinforcement Learning).

Table 2: Methodological Heterogeneity and Sampling Strategies

Method Type	Articles	Sampling/Data Sources
Experimental/ML	Wu (2022), Jiang (2023), Padilla (2024)	Synthetic Graphs, Ad-Log Files, APIs
Empirical (Field/Survey)	Ahmadi (2024), Neumann (2023), Ham (2025)	Facebook/Spotify Ads, B2B Field Tests
Case Study/Exploratory	Kim (2022), Chen (2024), Nugroho (2024)	SME Records, Interview Transcripts
Critical/Conceptual	McGuigan (2023), Polonioli (2022)	Privacy Policies, Theoretical Literature

4.3. Thematic Findings

To exemplify the thematic analysis process, the included studies were first examined through open coding, where recurrent meaning units related to data quality, privacy and governance, technical substitutes for signal loss, and the strategic value of proprietary data were labeled at the "code" level. Next, these codes were consolidated via axial coding into broader code categories. Finally, selective coding was used to aggregate the categories into four overarching themes reported below. Theme boundaries were refined through constant comparison, and a theme was retained when it recurred across at least two independent studies, ensuring analytical robustness and coherence.

Table 3: Example coding structure

Theme	Code categories	Example codes	Evidence base
The Accuracy Crisis of TPD	Data noise, segment validity, targeting effectiveness	"altmetrics noise", "near-random segment accuracy", "accuracy decay"	Yu et al. (2021); Neumann et al. (2023)
Governance and the Privacy Paradox	Policy–practice gap, tracker circumvention, privacy resignation, value exchange	"policy-practice gap", "third-party tracker bypass", "privacy resignation", "explicit value proposition increases ZPD sharing"	Sanfilippo et al. (2023); Rauti et al. (2024); Gopal et al. (2021)
Technical Mitigation of Signal Loss	Probabilistic modeling, cohort targeting, de-identification, SPD partnership infrastructure	"probabilistic models", "cohort-based targeting", "efficiency without individual tracking", "blockchain-enabled SPD monetization"	Padilla et al. (2024); Ahmadi et al. (2024); Bordel Sánchez (2024)
Strategic Supremacy of FPD	Prioritization, CLV-oriented use, retargeting design	"FPD prioritization", "purchase history + site behavior", "CLV calculation", "AHP-based weighting"	Ham & Lee (2025)

The four themes are analytically distinct yet causally connected in the post-cookie transition. The "Accuracy Crisis of TPD" acts as a primary trigger that both accelerates the "Strategic Supremacy of FPD" (firms shift toward proprietary data infrastructures) and stimulates "Technical Mitigation of Signal Loss" (privacy-preserving substitutes seek to maintain performance). In parallel, "Governance and the Privacy Paradox" functions as a cross-cutting constraint and legitimacy filter, shaping which mitigation options are acceptable and how scalable FPD and ZPD architectures can become. When a clear consumer value proposition is communicated, willingness to share ZPD may increase, reinforcing relationship-based data strategies and strengthening the strategic role of FPD (Gopal et al., 2021). Four dominant themes emerge from the qualitative synthesis of the included studies:

4.3.1. The Accuracy Crisis of TPD

A recurring finding is the unreliability of TPD. Yu et al. (2021) found that social media altmetrics often contain significant noise, while Neumann et al. (2023) demonstrated that third-party segments are frequently no more accurate than random targeting. This "accuracy decay" is a primary driver for firms shifting toward proprietary data infrastructures.

4.3.2. Governance and the Privacy Paradox

The literature highlights a severe gap between corporate privacy policies and actual data-sharing practices (Rauti et al., 2024; Sanfilippo et al., 2023). In sectors like healthcare and education, third-party trackers often bypass user intent, leading to "privacy resignation." Conversely, Gopal et al. (2021) suggest that while users fear privacy loss, they are increasingly willing to share ZPD when the value proposition (personalization or safety) is explicit. Although examples from high-stakes domains are discussed, they are used only to illuminate marketing-relevant mechanisms (legitimacy, governance, and signal quality) under cookieless constraints, and all implications are interpreted through a digital marketing strategy lens.

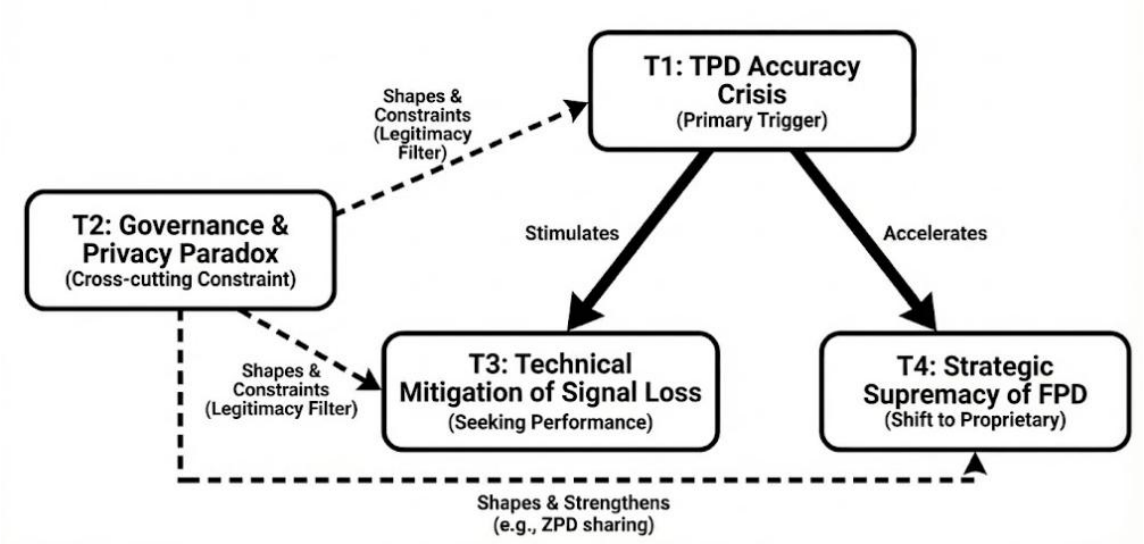
4.3.3. Technical Mitigation of Signal Loss

As third-party cookies vanish, technical innovations are filling the gap. Padilla et al. (2024) and Ahmadi et al. (2024) show that probabilistic models and cohort-based targeting can maintain advertising efficiency without individual tracking. Furthermore, Bordel Sánchez (2024) introduces Blockchain as a means to monetize SPD partnerships without exposing raw consumer identities.

4.3.4. Strategic Supremacy of FPD

The most significant strategic finding is the empirical confirmation of FPD's superiority. Ham & Lee (2025) utilize an Analytic Hierarchy Process (AHP) to show that advertisers now prioritize FPD (purchase history, site behavior) over any external source for calculating CLV and designing retargeting campaigns.

Figure 2: Thematic Relationship Map



Note: This figure was created by the author for the purposes of this study.

The findings obtained during the post-cookie transition clearly reveal the dynamic and causal interactions between the themes. The accuracy crisis of TPD acts as a primary trigger that both accelerates the strategic supremacy of FPD and stimulates technical solutions aimed at mitigating signal loss. In this process, the theme of governance and the privacy paradox functions as a legitimacy

filter determining which technical options are acceptable, while also serving as a cross-cutting constraint that shapes how FPD and ZPD architectures can be scaled through the value proposition. This relational structure, visualized in Figure 2, confirms that firms are restructuring not only their technical toolsets but also their data-driven strategic infrastructures under these constraints.

4.3.5. Cross-Theory Contrasts and Contradictory Evidence

A key contribution of this synthesis is that the reviewed stream does not converge on a single behavioral logic of disclosure. Social Exchange Theory implies that explicit and credible benefit framing should increase ZPD contribution because consumers rationally trade data for value. However, the Privacy Paradox and evidence of "privacy resignation" indicate that heightened concern can coexist with continued disclosure, while simultaneously degrading data quality through fatigue, distrust, or reduced engagement. This tension suggests that the outcome is not "more or less sharing" per se, but the stability and validity of the resulting data signal.

Importantly, the literature also provides a critical counterpoint that complicates firm-centric narratives of "privacy-first progress." Some studies interpret parts of AdTech's privacy pivot as strategic repositioning to preserve market power, implying that "privacy" may function rhetorically even when underlying incentives remain extractive. Therefore, post-cookie strategy should be evaluated not only by technical compliance claims but by observable governance design and verifiable reductions in opaque tracking.

Taken together, the contradictory findings can be reconciled by treating context and governance capacity as moderators. In high-stakes settings, the value proposition is more risk-sensitive and trust-dependent, making legitimacy mechanisms (transparency, perceived control, accountability) a stronger determinant of whether ZPD and FPD strategies produce durable marketing advantage.

4.4. TCCM Framework Synthesis

To provide a structured roadmap for future research and to synthesize the current state of the field, the findings are organized according to the TCCM framework. This framework identifies the foundational pillars of the transition toward privacy-centric data strategies. To exemplify the synthesis, Table 4 maps each TCCM pillar to representative research foci, variables, and illustrative research questions derived from the reviewed stream. This makes explicit how theory, context, characteristics, and methodology align and where gaps emerge.

- **Theory:** The reviewed literature predominantly utilizes Social Exchange Theory to explain the value exchange in ZPD sharing, where consumers trade personal information for perceived benefits. Furthermore, the Privacy Paradox remains a central theoretical lens, addressing the conflict between users' privacy concerns and their actual data-sharing behaviors. For example, a Social Exchange perspective can be operationalized by modeling "perceived benefit" (e.g., personalization, convenience, safety) and "perceived cost" (e.g., privacy risk, control loss) as antecedents of ZPD disclosure intention, while the Privacy Paradox lens can be reflected in the divergence between stated concerns and observed disclosure behavior.
- **Context:** While early research was heavily concentrated on E-commerce and Social Media platforms, there is a clear emerging focus on high-stakes sectors such as B2B Marketing, Healthcare (E-pharmacy), and Transportation. This shift indicates that data privacy is no longer just a retail concern but a cross-industry strategic imperative. As an illustration, in e-commerce the primary outcome is often ad effectiveness or conversion, whereas in e-pharmacy or transportation the dominant outcome may shift toward trust, perceived safety, and compliance-driven acceptance of data practices, indicating that the "value proposition" in ZPD sharing becomes more risk-sensitive and domain-specific.
- **Characteristics:** There is a definitive shift in data attributes moving from Aggregated and Inferred datasets (TPD) characterized by high volume but low precision, toward Individual

and Explicit data (ZPD and TPD) which offer lower volume but higher intent precision and ethical compliance. This shift can be exemplified by contrasting (i) TPD segments inferred from browsing traces (high reach, uncertain validity) with (ii) ZPD preferences declared via account settings, quizzes, or preference centers (lower reach, higher intent precision and consent clarity). In practice, this re-balances optimization from "scale-first targeting" toward "quality-first relationship data," where the unit of value is not volume but verifiable intent and permission.

- **Methodology:** The research landscape is transitioning from descriptive and cross-sectional surveys toward Field Experiments (conducted on platforms like Facebook and Spotify) and Predictive Machine Learning Models (Bayesian frameworks, Deep RL). This methodological evolution reflects the need for causal inference and technical solutions to "signal loss" in the post-cookie era. For example, field experiments can test whether privacy-forward prompts (e.g., explicit benefit framing) increase ZPD contribution and downstream conversion, while predictive models can estimate purchase propensity under reduced identifier availability, using privacy-preserving features (e.g., cohorts, contextual signals) rather than individual-level tracking.

Table 4: TCCM mapping for the post-cookie data strategy

TCCM	What the literature emphasizes	Example operationalization	Example research question
Theory	Value exchange and paradoxical disclosure	Benefits vs. costs → ZPD disclosure; concern behavior gap	When does perceived value override privacy concern in ZPD sharing?
Context	Expansion beyond retail into high-stakes sectors	E-commerce vs. e-pharmacy vs. transportation outcomes	Do privacy-first strategies yield stronger trust effects in high-stakes contexts than in retail?
Characteristics	From inferred scale to explicit permission and intent	TPD inferred segments vs. ZPD declared preferences	How does intent precision mediate the performance of campaigns when identifiers are limited?
Methodology	Shift toward causal and technical approaches	Field experiments; Bayesian/Deep RL prediction under signal loss	Which privacy-preserving signals best recover performance in cookieless targeting?

Finally, the TCCM synthesis indicates an integrative logic: theoretical mechanisms (value exchange. paradox) shape how privacy is interpreted in each context; contexts determine which data characteristics are viable (e.g., permission strength, risk tolerance); and these jointly motivate methodological choices (experiments for causality; ML for signal loss). This integrated view clarifies that "post-cookie" change is not only a media technology shift but a coupled transformation of governance, consumer psychology, and data architecture.

5. Discussion

This SLR systematically documents the structural transformation that unfolded in digital marketing between 2021 and 2025. Specifically, it captures the shift from a passive tracking regime anchored in TPD toward permission-based and relationship-centric data architectures built on ZPD, FPD, and SPD. The findings indicate that the "post-cookie" era is not merely a measurement or targeting challenge. It is also a new competitive arena defined by the ownership, governance, and legitimacy of data assets that constitute the core input of marketing strategy. Accordingly, this discussion treats

data types not only as technical categories, but as distinct "value production regimes" differentiated by accuracy, scale, transparency, and governance requirements.

The reviewed studies show that the classic "source-based" taxonomy of data types has evolved into a more strategically explanatory distinction in the post-cookie environment. Data now differs not only by where it originates, but by the legitimacy mechanism through which it is produced and activated. As a declared form of information that consumers knowingly and willingly provide, ZPD represents the category where consent and perceived control are most explicit (Kilinc, 2024; Polonioli, 2022). In this respect, ZPD reframes personalization away from "tracking" and toward "explicit declaration" and "reciprocal benefit." At the same time, the literature emphasizes that ZPD's sustainability depends on how clearly consumers perceive the value they receive in exchange for the information they provide. When the value proposition is made salient, consumers can become more willing to share data despite privacy concerns (Gopal et al., 2021). FPD, by contrast, has become the "strategic core" of post-cookie data strategy in terms of both regulatory alignment and quality, because it is behavioral and transactional data generated across a brand's own touchpoints (Latvala et al., 2022; Sousa, 2022). Within this SLR, the rise of FPD can be explained through two main mechanisms. First, FPD offers higher operational fit for performance-oriented processes such as Customer Lifetime Value (CLV) optimization and retargeting (Ham & Lee, 2025). Second, FPD aligns more strongly with internal organizational capabilities for governance, security, and accountability due to the brand's greater control over collection and use (Liu & Li, 2024). SPD functions as a "bridge strategy" to mitigate scale constraints, as it reflects another actor's FPD shared through trusted partnerships or formal agreements (Schneider et al., 2017). The strategic value of SPD lies in its ability to partially approximate the scale advantage of TPD while maintaining a more source-defined and contract-based governance structure. However, SPD also generates distinctive governance costs. When the scope of data sharing is ambiguous, competitive assets may be exposed and privacy risks may increase, making partnership governance a central managerial challenge (Schneider et al., 2017; Sponder and Khan, 2017). TPD, in turn, is reconceptualized in the reviewed literature through two interrelated problems. The first is "accuracy decay," driven by growing concerns about validity and freshness (Yu et al., 2021). The second is "governance failure," reflected in data-sharing practices that expand beyond policy claims in real-world implementation (Sanfilippo et al., 2023; Rauti et al., 2024). Evidence from Neumann et al. (2023) further indicates that third-party segments can perform no better than random targeting in certain contexts, undermining not only the ethical and legal legitimacy of TPD but also its performance-based rationale. For this reason, the SLR positions TPD not as the standard input that reliably delivers scale, but as a resource characterized by high variance in accuracy and elevated governance risk. Against this backdrop, a shared direction in the literature is to move beyond a "trust. transparency continuum" toward a more explanatory mechanism: the "trust. value exchange" model. On the consumer side, perceived control and transparency become micro-foundations of data quality. On the firm side, governance capacity that embeds these mechanisms into organizational processes becomes a key determinant of personalization performance (Çınar & Ateş, 2022; Quach et al., 2022).

The findings suggest that the loss of cookies has produced a three-track adaptation pathway in marketing analytics. The first track is the shift from deterministic, individual-level tracking toward probabilistic modeling and journey-based inference. Padilla et al. (2024) show that the customer journey can be reconceptualized as a robust source of information and that signal loss can be mitigated through more advanced probabilistic frameworks. Ahmadi et al. (2024) further indicate that, in an environment of overwhelming targeting options, segment selection itself becomes a strategic optimization problem. This reframes post-cookie targeting around not only "who to target" but also "under which targeting constraints" targeting should occur. The second track consists of technologies that enable a privacy-preserving data economy. Studies such as Jiang et al. (2023) demonstrate the potential of local differential privacy approaches to establish a more formalized balance between data utility and privacy protection. Bordel Sánchez (2024) argues that blockchain-based tokenization and

privacy-preserving algorithms can enable SPD-like data marketplaces that create value without exposing raw consumer identities, advancing the ambition of scaling data sharing without identity disclosure. Taken together, these streams signal a shift away from "personalization by hiding PII" and toward "personalization without needing PII." The third track is the re-engineering of organizational data architecture. As FPD rises in strategic importance, the need for CDP and CRM-centric integration intensifies, making the collection, unification, and activation of data an internal strategic capability (Kihn & Lin, 2024; Sousa, 2022). Importantly, technology alone is insufficient. Value creation depends on designing data processes together with consent, purpose limitation, retention policies, and sharing protocols as an integrated governance blueprint (Lim & Oh, 2025; Pantelic et al., 2022).

One of the most consequential conclusions of this SLR is that privacy has become more than regulatory compliance. It is increasingly a governance capability that produces data quality and brand value. The reviewed studies show that, particularly in high-stakes sectors such as healthcare and education, third-party trackers can leak data in ways that exceed user intent, and the persistent gap between "policy present" and "implementation absent" remains a structural problem (Sanfilippo et al., 2023; Rauti et al., 2024). This creates a dual-layer risk for brands: legal and reputational exposure on the one hand, and weakened relationship-based data strategies due to privacy fatigue or privacy resignation and the resulting decline in data quality on the other (Gopal et al., 2021). On the operational side, the "dark side" of FPD centralization becomes more visible. While accumulating large volumes of FPD can strengthen personalization, it can also expand the attack surface. Findings from Wu et al. (2022) indicate that learning systems may be vulnerable to poisoning attacks, pushing data strategy debates into the domain of cybersecurity and model integrity. Thus, "privacy-first marketing" requires not only consent management but also embedding "secure-by-design" and "accountable-by-design" principles into marketing technology stacks. The literature also produces a normative tension. McGuigan et al. (2023) interpret AdTech's pivot to privacy, in some cases, as a strategic repositioning aimed at preserving market power, raising the risk that "privacy" becomes a rhetorical instrument in the marketplace. This critical perspective balances the SLR's main narrative and clarifies a core point: success in the post-cookie era depends not only on better algorithms or alternative data sources, but on building a data value chain that is legitimate to consumers, accountable within firms, and transparent in the market. The synthesis of this SLR proposes integrating post-cookie data strategies through a three-component structure:

Data asset architecture: ZPD, FPD, SPD, and TPD each have distinct profiles in accuracy, coverage, and cost. While FPD becomes the core asset for CLV and retargeting processes (Ham & Lee, 2025), SPD offers a complementary layer that helps address scale limitations (Schneider et al., 2017). TPD, by contrast, increasingly resembles a high-risk, high-variance resource due to accuracy and governance uncertainty (Neumann et al., 2023; Yu et al., 2021).

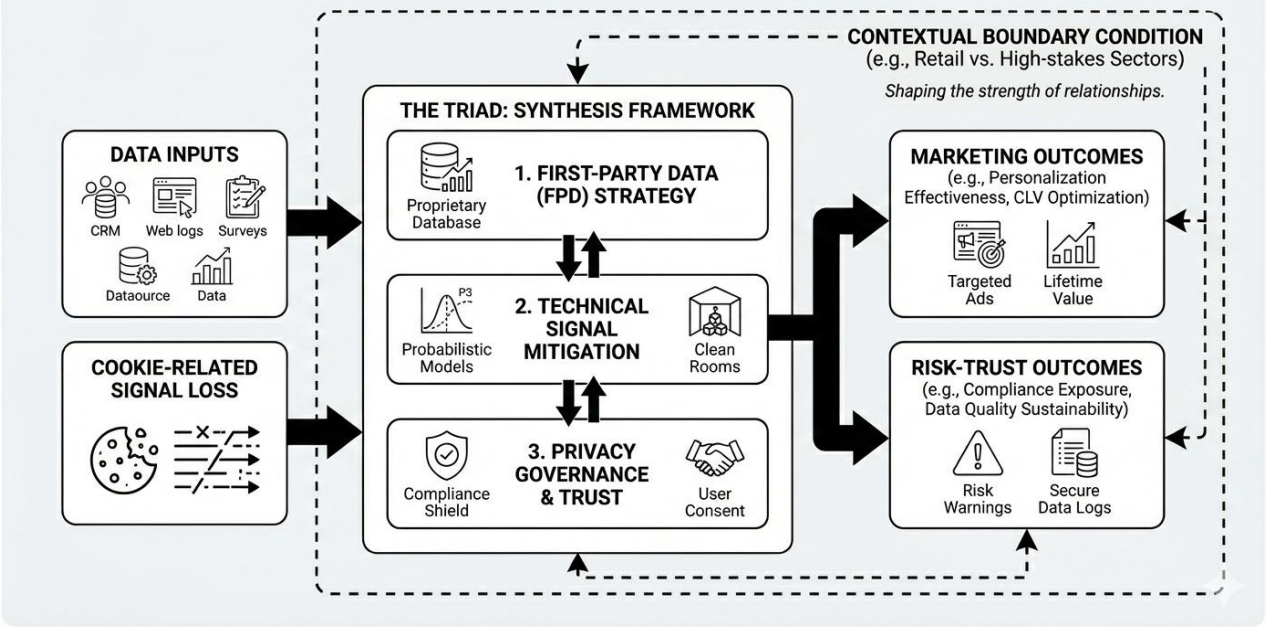
Legitimacy mechanism: ZPD and FPD generate legitimacy through relationship-based consent architectures, where transparency and perceived control shape data quality (Gopal et al., 2021; Quach et al., 2022). TPD and some SPD implementations rely more heavily on contracts, intermediaries, and technical safeguards, making governance design inseparable from strategy (Lim and Oh, 2025; Sanfilippo et al., 2023).

Activation logic: Post-cookie activation requires more probabilistic inference, more model-based optimization, and more privacy-preserving computation (Jiang et al., 2023; Padilla et al., 2024). In this context, technologies such as blockchain may scale SPD-like partnerships (Bordel Sánchez, 2024), while security vulnerabilities and model manipulation risks make the activation layer itself a target for oversight (Wu et al., 2022).

Figure 3 presents the Triad: Synthesis Framework, a holistic approach developed to address cookie-driven signal loss by integrating first-party data strategy, technical signal-loss mitigation, and privacy

governance with trust-building. The framework treats both traditional data inputs (e.g., CRM systems, web logs, surveys, and other brand-controlled sources) and cookie-related signal loss as core inputs, which are then processed through a three-layer triad. First, firms strengthen data sovereignty through a proprietary FPD strategy that consolidates owned data assets. Second, they compensate for measurement and targeting disruption via technical mitigation mechanisms, such as probabilistic modeling and secure activation environments (e.g., clean rooms). Third, they establish a legitimacy and trust basis through privacy governance, including consent and compliance safeguards that function as a "compliance shield." By linking these triad components to both marketing outcomes (e.g., personalization effectiveness, customer lifetime value optimization, and targeted advertising performance) and risk–trust outcomes (e.g., reduced compliance exposure, sustainable data quality, and secure data logging), the model clarifies the logic of the synthesis. Importantly, context operates as a boundary condition, implying that the strength and configuration of these relationships may differ between lower-risk retail settings and high-stakes domains. This triad consolidates dispersed findings into a single strategic picture: post-cookie competition is shifting from a race for "more data" toward a race for "more legitimate data and safer activation."

Figure 3: The Marketing Data Re-Architecture Triad for the Post-Cookie Era



Note: This figure was created by the author for the purposes of this study.

To strengthen the theoretical linkages in Figure 3, the synthesis is expressed as theory-informed propositions. P1 (Social Exchange): clearer value propositions and greater perceived control increase the stability and usefulness of voluntarily shared data (especially ZPD), improving personalization outcomes rather than merely increasing disclosure volume. P2 (Privacy Paradox and resignation): privacy concern may coexist with continued disclosure, yet it can reduce signal quality through fatigue, distrust, or disengagement, making governance design critical for data validity. P3 (Governance as a moderator): strong privacy governance and accountability increase the feasibility and legitimacy of technical mitigation options (e.g., probabilistic modeling, secure activation environments), reducing compliance exposure while sustaining performance. P4 (Strategic supremacy of FPD): as third-party accuracy decays, firms with stronger proprietary FPD infrastructures and governance capacity are more likely to outperform brokered signals in CLV-oriented targeting and retargeting. Context remains a boundary condition, implying that the strength of these relationships differs between low-risk retail settings and high-stakes sectors.

5.1. Theoretical Contributions

This SLR advances theory by explaining the post-cookie transition as a structural break in the logic of personalization, not merely a disruption in measurement infrastructure. Prior privacy-focused syntheses have largely consolidated constructs, taxonomies, and consumer decision mechanisms across broad contexts or specific settings (Pelteret and Ophoff, 2016; Sun et al., 2024; Unny, 2023), while foundational work in marketing and law has foregrounded privacy governance and consumer protection principles (Corones and Davis, 2017; Martin and Murphy, 2017). Building on these streams, our review theorizes cookie deprecation as an ecosystem-level shock that reorders the relative strategic value of data assets and forces a shift from scale-oriented tracking to legitimacy-oriented data production. In doing so, it reframes the cookieless transition as a market-wide reallocation from externally brokered signals (TPD) to relationship-based and permissioned data architectures (ZPD, FPD, and SPD), thereby offering a theoretically grounded account of why "data ownership and governance" become first-order determinants of marketing advantage in the privacy-first era (Çınar and Ateş, 2022; Lim and Oh, 2025; Quach et al., 2022). This strengthens the paper's originality by moving beyond a descriptive taxonomy toward an integrated explanation of how performance, legitimacy, and governance jointly shape post-cookie marketing advantage. Accordingly, Figure 3 is positioned as a theory-consistent bridge that links consumer-level disclosure mechanisms to firm-level data architecture and activation choices.

Second, the review reconceptualizes the Privacy Paradox beyond an individual-level attitude, behavior inconsistency and positions it as a generative mechanism that redesigns the data ecosystem. Specifically, our synthesis shows that the quality and sustainability of ZPD increasingly depends on the clarity of the value proposition and consumers' perceived control, meaning that privacy calculus is better treated as a micro-foundation of data quality rather than only a constraint on data collection (Gopal et al., 2021; Polonioli, 2022). On the firm side, governance capacity and internal data architecture emerge as performance conditions for personalization, because they determine whether explicit consent and accountability can be operationalized at scale across touchpoints and activation pipelines (Ham & Lee, 2025; Sousa, 2022). This repositioning breaks the legacy assumption that tracking is functionally synonymous with personalization and instead frames "personalization without tracking" as a socio-managerial design problem, where transparency, perceived control, and accountability design substitute for opaque signal extraction as the basis of targeting legitimacy and effectiveness (Ham & Lee, 2025; Neumann et al., 2023).

Third, the SLR provides a multi-level theoretical bridge between technical signal loss and managerial strategy by integrating evidence on performance, risk, and governance into a unified explanation of post-cookie outcomes. Empirical findings indicating the performance gap between FPD and TPD support the claim that the old scale advantage of third-party ecosystems is increasingly offset by accuracy decay and governance uncertainty (Ham & Lee, 2025; Neumann et al., 2023; Yu et al., 2021). At the same time, the literature on operational vulnerability shows that privacy-resilient data strategies do not automatically reduce risk. Centralized FPD infrastructures can expand the attack surface, while AI-driven systems can be exposed to manipulation, implying that marketing capability in the post-cookie era must be co-theorized with security and model integrity rather than treated as a purely analytics-driven competence (Rauti et al., 2024; Sanfilippo et al., 2023; Wu et al., 2022). In this way, the review extends dominant cookieless narratives that are often limited to measurement, attribution, and operational adaptation by embedding them within a broader governance-performance trade-off framework (Elmér and Nilsson, 2022; Erceg, 2024; Mantovaara, 2022; Ruzive et al., 2023).

Finally, the review advances boundary-based theorizing of data ownership and sharing by showing how emerging technologies are used to redraw the limits of legitimate data exchange. Blockchain and decentralized identifiers, together with privacy-preserving computation, are theorized not only as technical fixes but as boundary-setting mechanisms that aim to enable value creation through SPD-like collaboration while reducing identity exposure and strengthening governance conditions (Bordel Sánchez, 2024; Jiang et al., 2023). This contribution enriches Information Boundary Theory by

illustrating how firms attempt to re-specify "who owns what data," "under which rules," and "for which activation purposes" in an era where legitimacy is increasingly audited by regulators, platforms, and consumers (Lim & Oh, 2025; Pantelic et al., 2022). Collectively, these theoretical moves shift the field from descriptive accounts of cookie deprecation toward an integrative explanation of how consumer privacy decisions, governance mechanisms, and alternative data capabilities jointly shape post-cookie personalization effectiveness and strategic differentiation.

5.2. Practical Contributions

This SLR translates the post-cookie transition into actionable implications for firms, technology teams, and regulators. The central practical message is that moving toward FPD and ZPD is not a tactical replacement for third-party cookies, but a strategic redesign of marketing capability. Advantage increasingly depends on building robust internal data infrastructure, sustaining consumer cooperation through credible value exchange, and embedding governance and security into activation processes rather than treating them as after-the-fact compliance.

For marketing managers, the evidence suggests that proprietary data, especially FPD, delivers stronger effectiveness and controllability than legacy third-party approaches, while TPD is increasingly associated with accuracy decay and governance uncertainty (Ham & Lee, 2025; Neumann et al., 2023; Yu et al., 2021). Accordingly, firms should prioritize CDP and CRM integration to unify first-party signals across touchpoints and to turn fragmented traces into decision-ready assets through data quality routines and standardization (Kihn &Lin, 2024; Latvala et al., 2022; Sousa, 2022). For ZPD, sustainable personalization requires transparent, user-centric value-exchange design. Tools such as preference centers, interactive onboarding, and explainable personalization can make benefits immediate and reinforce perceived control, improving both trust and the quality of declared data used for personalization (Gopal et al., 2021; Kilinc, 2024; Polonioli, 2022; Quach et al., 2022).

SPD can partially restore scale, but only under strict partnership governance. Firms should implement "clean" protocols, including clear purpose limitation, minimization, retention rules, auditability, and secure matching to reduce identity exposure (Schneider et al., 2017; Sponder and Khan, 2017). Emerging privacy-preserving exchange designs, including blockchain-enabled mechanisms, may support SPD value creation when coupled with enforceable accountability (Bordel Sánchez, 2024; Jiang et al., 2023). For TPD, the implication is not total abandonment but disciplined use. If employed for prospecting or enrichment, TPD should be treated as a high-variance input and subjected to benchmarking against FPD baselines, freshness and bias checks, and continuous validation (Neumann et al., 2023; Yu et al., 2021).

For AI and technology teams, the literature underscores secure-by-design architectures and model integrity controls, since centralizing FPD and relying on ML-based activation can expand the attack surface (Wu et al., 2022). For policymakers, persistent gaps between privacy policy and actual tracking practices indicate the need for enforceable standards and sector-specific oversight, especially in high-stakes domains, to enable a market where privacy-resilient personalization is both credible and scalable (Lim and Oh, 2025; Pantelic et al., 2022; Rauti et al., 2024; Sanfilippo et al., 2023).

6. Conclusion

This systematic literature review mapped the strategic evolution of digital marketing data in the privacy-first era by synthesizing 25 high-impact studies published between 2021 and May 2025. The review confirms that third-party cookie deprecation represents more than a technical disruption. It constitutes an ecosystem-level inflection point that redefines how personalization can be legitimately produced, governed, and scaled. Across the corpus, a consistent pattern emerges: third-party data (TPD), once the backbone of programmatic advertising, is increasingly portrayed as a volatile asset characterized by accuracy decay, limited transparency, and heightened governance risk (Neumann et

al., 2023; Sanfilippo et al., 2023; Yu et al., 2021). In contrast, first-party data (FPD) and zero-party data (ZPD) are positioned as strategic cornerstones of contemporary personalization, not only because they are more controllable and regulation-aligned, but because they enable a relationship-centric logic anchored in explicit consent and clearer accountability (Ham and Lee, 2025; Polonioli, 2022; Sousa, 2022).

A second overarching conclusion concerns the emerging feasibility of "Personalization without Tracking." The evidence indicates that signal loss in the post-cookie transition is being partially offset by a combination of probabilistic and journey-based modeling, privacy-preserving computation, and new forms of governed data collaboration. AI-driven inference frameworks, differential privacy, and blockchain-enabled exchange mechanisms are increasingly discussed as ways to sustain marketing effectiveness while reducing identity exposure and strengthening legitimacy conditions (Bordel Sánchez, 2024; Jiang et al., 2023; Padilla et al., 2024). Taken together, these developments suggest that post-cookie personalization is becoming less dependent on opaque cross-site surveillance and more dependent on the ability to convert trust, transparency, and governance design into data quality and activation capability. In this sense, the SLR bridges technical accounts of tracking loss with a strategic understanding of how firms are re-architecting data assets and decision systems to compete in privacy-first markets, offering both a theoretical baseline for scholars and an actionable roadmap for practitioners.

6.1. Limitations

Despite the rigor of the PRISMA-based review process, several limitations should be acknowledged. First, the search was limited to the Web of Science Core Collection and to English-language, peer-reviewed journal articles. Although non-marketing high-stakes contexts (e.g., healthcare, education, transportation) were retained only when they illuminated marketing-relevant mechanisms, their inclusion may still dilute a purely marketing-centric interpretation; therefore, the generalizability of some themes should be evaluated with attention to contextual boundary conditions. Consequently, relevant insights from grey literature (e.g., regulatory documents, industry reports, practitioner white papers, and conference proceedings) may be underrepresented, even though such sources can be influential in rapidly evolving domains. Second, the review includes studies published up to May 2025. Given the fast pace of platform updates and the emergence of AI-enabled privacy technologies, more recent developments in cookieless targeting and measurement are not captured. Third, the included studies are methodologically diverse, ranging from conceptual papers and case studies to field experiments and machine-learning-based analyses. While this breadth improves conceptual coverage, it reduces comparability across studies and precludes a quantitative meta-analysis, making qualitative synthesis the most appropriate approach. Finally, the final corpus (n = 25) should be interpreted as a focused, high-quality evidence base rather than a statistically representative sample of all post-cookie research. The SSCI criterion and the 2021–2025 time window were applied to ensure reliability and topical relevance, and the additional market-focused filter was used to retain studies directly informing marketing decision-making and personalization strategy. Accordingly, the main contribution of this SLR is to synthesize mechanisms and theory-consistent insights, not to estimate pooled average effect sizes.

6.2. Future Research Directions

The cookieless transition opens several high-value avenues for future research. First, longitudinal and panel-based designs are needed to test whether the shift toward ZPD and FPD produces sustained trust and loyalty gains, or whether privacy fatigue and disclosure fatigue reduce the completeness and reliability of self-reported preferences over time (Gopal et al., 2021; Polonioli, 2022). Second, future work should develop sector-specific governance models that reflect the distinct ethical and legal requirements of high-stakes industries such as healthcare, education, and transportation, where third-party tracking and leakage risks are particularly consequential and where "one-size-fits-all" consent

frameworks may be insufficient (Sanfilippo et al., 2023; Rauti et al., 2024; Shaw et al., 2021). Third, research should examine the "dark side" of FPD at scale, including the possibility of data concentration and monopolistic advantage, as well as security threats arising from centralized repositories that create single points of failure for both privacy and model integrity (Wu et al., 2022). Fourth, additional empirical work is needed on privacy-preserving machine learning and synthetic data, especially on whether replacing PII with generated or federated signals can preserve predictive performance while reducing privacy risk, and under which governance conditions such approaches remain auditable and fair (Jiang et al., 2023). Finally, the field would benefit from economic quantification of the privacy-first transition by estimating the cost–benefit trade-offs of moving from low-cost TPD to higher-engagement ZPD and infrastructure-intensive FPD, including effects on ROI, measurement accuracy, and long-term customer equity. Such research would provide firms with a clearer business rationale for ethical data transformation and would help policymakers anticipate the market-level consequences of privacy regulation (Lim and Oh, 2025; Pantelic et al., 2022).

AUTHOR CONTRIBUTION

All sections of this study were completed by İbrahim Halil Efendioğlu.

CONFLICT OF INTEREST STATEMENT

There are no financial conflicts of interest with any institution, organization, or individual, and no conflicts of interest exist among the authors.

ETHICAL STATEMENT ON THE USE OF ARTIFICIAL INTELLIGENCE AND OTHER CONSIDERATIONS

During the preparation of this manuscript, [ChatGPT 5.0] was used in a limited capacity for language editing purposes. The content creation, analyses, and scientific evaluations were carried out entirely by the author.

REFERENCES

Acquisti, A. (2023). The economics of privacy at a crossroads. *Economics of Privacy. University of Chicago Press*.

Ahmadi, I., Abou Nabout, N., Skiera, B., Maleki, E., ve Fladenhofer, J. (2024). Overwhelming targeting options: Selecting audience segments for online advertising. *International Journal of Research in Marketing, 41*(1), 24–40. https://doi.org/10.1016/j.ijresmar.2023.08.004

Akinnubi, A., Alassad, M., Amure, R., & Agarwal, N. (2024). KG-CFSA: a comprehensive approach for analyzing multi-source heterogeneous social network knowledge graph. *Social Network Analysis and Mining*, *14*(1), 159. https://doi.org/10.1007/s13278-024-01320-y

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 13-28. https://doi.org/10.2307/25148715

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature

review. *Telematics and informatics*, *34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Behare, N., Chaudhari, M., Sharma, S., Sane, A. C., Kharate, S., Waghulkar, S., ... & Pawar, P. (2024). Emerging trends in data-driven marketing. *Data-Driven Marketing for Strategic Success*, 323-358. https://doi.org/10.4018/979-8-3693-3455-3.ch012

Bertheau, P., & Lindner, R. (2022). Financing sustainable development? The role of foreign aid in Southeast Asia's energy transition. *Sustainable Development*, *30*(1), 96-109. https://doi.org/10.1002/sd.2231

Bordel Sánchez, B., Alcarria, R., Ladid, L., & Machalek, A. (2024). Using privacy-preserving algorithms and blockchain tokens to monetize industrial data in digital marketplaces. *Computers*, *13*(4), 104. https://doi.org/10.3390/computers13040104

Canaway, R., Boyle, D., Manski-Nankervis, J. A., & Gray, K. (2022). Identifying primary care datasets and perspectives on their secondary use: a survey of Australian data users and custodians. *BMC Medical Informatics and Decision Making*, *22*(1), 94. https://doi.org/10.1186/s12911-022-01830-9

Chanda, R., & Pabalkar, V. (2024, October). How to personalize in a cookie-less world. In *AIP Conference Proceedings* (Vol. 3209, No. 1). AIP Publishing. https://doi.org/10.1063/5.0228693

Chauhan, D., & Sethi, D. (2024, April). Unlocking the Power of First-Party Data: Innovative Geo contextual Targeting for Advertiser. In *International Conference on Business Intelligence and Data Analytics* (pp. 213-225). Springer Nature. https://doi.org/10.1007/978-981-97-7717 4_15

Chen, H., Qu, Q., Lin, Y., Chen, X., & Li, K. (2021). Authenticity verification on social data outsourcing. *Computers & Security*, *100*, 102077. https://doi.org/10.1016/j.cose.2020.102077

Chen, Y., Sherren, K., Lee, K. Y., McCay-Peet, L., Xue, S., & Smit, M. (2024a). From theory to practice: insights and hurdles in collecting social media data for social science research. *Frontiers in Big Data*, *7*, 1379921. https://doi.org/10.3389/fdata.2024.1379921

Chen, Q., Lyu, X., & Chen, J. (2024b). Identification and Analysis of Key Factors Affecting Digital Transformation of Small and Medium-Sized Manufacturing Enterprises. *SAGE Open*, *14*(4), 21582440241279693. https://doi.org/10.1177/21582440241279693

Choi, W., Kim, H. Y., Choi, B., & Moon, J. (2025). Development of a fashion recommendation system with consumers' zero-party data applying the CART decision-tree model. *Journal of Fashion Marketing and Management: An International Journal*, 1-25. https://doi.org/10.1108/JFMM-07-2024-0284

Çınar, N., & Ateş, S. (2022). Data privacy in digital advertising: Towards a post-third-party cookie era. In M. Filimowicz (Ed.), *Privacy: Algorithms and society* (1st ed., p. 23). Routledge.

Degutis, M., Urbonavičius, S., Hollebeek, L. D., & Anselmsson, J. (2023). Consumers' willingness to disclose their personal data in e-commerce: A reciprocity-based social exchange perspective. *Journal of Retailing and Consumer Services*, *74*, 103385. https://doi.org/10.1016/j.jretconser.2023.103385

Elangovan, N., Nagarathinam, A., Elangovan, S., Chellassamy, A., ve Rangasamy, S. (2025). Leveraging data sharing for enhanced experiences in service industries: Role of experience orientation and privacy calculus. In M. Sinha, A. Bhandari, S. S. Priya, ve S. Kabiraj (Eds.), *Marketing intelligence, Part A: Understanding customers in the era of digitalization*. Emerald Publishing Limited. https://doi.org/10.1108/978-1-83549-418-920251003

Elmér, J., & Nilsson, J. (2022). *A future without third-party cookies: A study of how Swedish small and medium-sized marketing agencies are affected by the loss of third-party cookies and how potential change strategies are communicated* (Thesis No. 2022:002) [Master's thesis, University of Gothenburg]. GUPEA.

Erceg, V., & Phan, V. (2024). *Removal of third-party cookies: Exploring Swedish retailers responses towards a cookieless future* [Bachelor's thesis, Lund University].

Fakeyede, O. G., Okeleke, P. A., Hassan, A., Iwuanyanwu, U., Adaramodu, O. R., & Oyewole, O. O. (2023). Navigating data privacy through IT audits: GDPR, CCPA, and beyond. *International Journal of Research in Engineering and Science*, *11*(11), 45-58.

Feth, D., Jung, C., & Eitel, A. (2025). Concepts for data sovereignty in digital value chains: Data cockpits data usage control data trustees. In New Digital Work II: Digital Sovereignty of Companies and Organizations (pp. 75-92). Cham: Springer Nature Switzerland.

Gopal, R. D., Hidaji, H., Patterson, R. A., & Yaraghi, N. (2021). Dark clouds and silver linings: impact of COVID-19 on internet users' privacy. *JAMIA open*, *4*(4), ooab100. https://doi.org/10.1093/jamiaopen/ooab100

Ham, M., & Lee, S. W. (2025). Personal data strategies in digital advertising: Can first-party data outshine third-party data?. *International Journal of Information Management*, *80*, 102852. https://doi.org/10.1016/j.ijinfomgt.2024.102852

Huang, M. L. (2025). Digital Privacy in the Age of Surveillance: A Comparative Study of GDPR and CCPA. *OTS Canadian Journal*, *4*(7), 65-74. https://doi.org/10.58840/1t99rb13

Jiang, L., Yan, Y., Tian, Z., Xiong, Z., & Han, Q. (2023). Personalized sampling graph collection with local differential privacy for link prediction. *World wide web*, *26*(5), 2669-2689. https://doi.org/10.1007/s11280-023-01136-4

Johnson, K., & Ahmed-Kristensen, S. (2025). Exploring the Role of Human Data in Data-Driven Design. *Proceedings of the Design Society*, *5*, 1743-1752. https://doi.org/10.1017/pds.2025.10188

Karuppuchamy, S. (2025). Embracing Privacy: How Zero-Party Data is Shaping the Future of eCommerce. *Journal of Computer Science and Technology Studies*, *7*(6), 63-71. https://doi.org/10.32996/jcsts

Khan, S. M., & Patire, A. D. (2021). Third-party data fusion to estimate freeway performance measures. *Transportation Research Record*, *2675*(11), 1139-1153. https://doi.org/10.1177/03611981211024240

Kihn, M., & Lin, A. C. (2024). *Customer 360: How Data, AI, and Trust Change Everything*. John Wiley & Sons.

Kilinc, T. (2024). How does the customer experience benefit from better customer data?. *Applied Marketing Analytics*, *10*(3), 216-226. https://doi.org/10.69554/NMQI7891

Kim, Y. S. (2022). Customer experience design for smart product-service systems based on the terations of experience–evaluate–engage using customer experience data. *Sustainability*, *15*(1), 686. https://doi.org/10.3390/su15010686

Kumar, N. (2025). *Intelligent Integration: Leveraging AI for Seamless ERP and CRM Connectivity*. Naveen Kumar.

Latvala, L., Horn, J., & Bruno, B. (2022). Thriving in the age of privacy regulation: A first-party data strategy. *Applied Marketing Analytics*, *7*(3), 211–220.

Leiva-Araos, A., Contreras, C., Kaushal, H., & Prodanoff, Z. (2025). Predictive Optimization of Patient No-Show Management in Primary Healthcare Using Machine Learning. *Journal of Medical Systems*, *49*(1), 7. https://doi.org/10.1007/s10916-025-02143-w

Li, E., Wang, Z., & Zhao, L. (2025). Alternative data as an external governance mechanism. *Corporate Governance: An International Review*. Advance online publication. https://doi.org/10.1111/corg.12641

Lim, S., & Oh, J. (2025). Navigating Privacy: A Global Comparative Analysis of Data Protection Laws. *IET Information Security*, *2025*(1), 5536763. https://doi.org/10.1049/ise2/5536763

Liu, X., & Li, X. B. (2024). Cost-effective acquisition of first-party data for business analytics. *INFORMS Journal on Computing*, *36*(5), 1242-1260. https://doi.org/10.1287/ijoc.2022.0037.

Lockitt, P. (2024). *Zero-party data: Why advertisers should be comfortable sharing data sovereignty* [Honors Capstone project, Syracuse University]. Surface at Syracuse University.

Luo, X. (2002). Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial marketing management*, *31*(2), 111-118. https://doi.org/10.1016/S0019-8501(01)00182-1

Majeti, V. S. K. (2025). Mastering Data Privacy and Security in CRM with AI: A Technical Perspective. Journal of Computer Science and Technology Studies, 7(5), 946-953. https://doi.org/10.32996/jcsts

McGuigan, L., West, S. M., Sivan-Sevilla, I., & Parham, P. (2023). The after party: Cynical esignation in Adtech's pivot to privacy. *Big Data & Society*, *10*(2), 20539517231203665. https://doi.org/10.1177/20539517231203665

Neumann, N., Tucker, C. E., Subramanyam, K., & Marshall, J. (2023). Is first-or third-party audience data more effective for reaching the 'right'customers? The case of IT decision makers. *Quantitative marketing and economics*, *21*(4), 519-571. https://doi.org/10.1007/s11129-023-09268-7

Nugroho, A., Putro, N. H. P. S., Syamsi, K., Mutiaraningrum, I., & WulTeacher's experience u sing ChatGPT in language teaching: An exploratory study. *Computers in the Schools*, 1-20. https://doi.org/10.1080/07380569.2024.24411 61

Padilla, N., Ascarza, E., & Netzer, O. (2024) Hoffmann, T. C., Mulrow, C. D., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Pantelic, O., Jovic, K., & Krstovic, S. (2022). Cookies implementation analysis and the impact on user privacy regarding GDPR and CCPA regulations. *Sustainability*, *14*(9), 5015. https://doi.org/10.3390/su14095015

Polonioli, A. (2022). Zero party data between hype and hope. *Frontiers in big Data*, *5*, 943372. https://doi.org/10.3389/fdata.2022.943372

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science, 50*(6), 1299-1323. https://doi.org/10.1007/s11747-022-00845-y

Rasaii, A., Singh, S., Gosain, D., & Gasser, O. (2023, March). Exploring the cookieverse: A multi perspective analysis of web cookies. In *International Conference on Passive and Active Network Measurement* (pp. 623-651). Cham: Springer Nature Switzerland.

Rauti, S., Carlsson, R., Mickelsson, S., Mäkilä, T., Heino, T., Pirjatanniemi, E., & Leppänen, V. (2024). Analyzing third-party data leaks on online pharmacy websites. *Health and Technology*, *14*(2), 375-392. https://doi.org/10.1007/s12553-024-00819-w

Rolando, B., & Mulyono, H. (2024). Unlocking the power of data: Effective data-driven marketing strategies to engage Millennial consumers. *Transekonomika: Akuntansi, Bisnis Dan Keuangan*, *4*(3), 303-321. https://doi.org/10.55047/transekonomika.v4i3.662

Ruzive, B., Masengu, R., & Muchenje, C. (2023). Reduction of third-party cookies – Its effects in digital marketing transformation. S. H. Al Rubaie, A. A. Al Shahri, & A. A. Al Qamashoui (Ed.), *Strategies for business transformation - Accelerators for sustainable growth* (ss. 245 260). University of Technology and Applied Sciences- Al Mussanah.

Sakalauskas, V., & Kriksciuniene, D. (2024). Personalized advertising in E-commerce: using clickstream data to target high-value customers. *Algorithms*, *17*(1), 27. https://doi.org/10.3390/a17010027

Sanfilippo, M. R., Apthorpe, N., Brehm, K., & Shvartzshnaider, Y. (2023). Privacy governance not included: analysis of third parties in learning management systems. *Information and Learning Sciences*, *124*(9/10), 326-348. https://doi.org/10.1108/ILS-04-2023-0033

Sara, Z., & Ayoub, A. (2024). The impact of third-party cookies on the perception of e-commerce professionals in Algeria. *Brazilian Journal of Business*, *6*(4), e74705-e74705. https://doi.org/10.34140/bjbv6n4-029

Schneider, M. J., Jagpal, S., Gupta, S., Li, S., & Yu, Y. (2017). Protecting customer privacy when marketing with second-party data. *International Journal of Research in Marketing*, *34*(3), 593-603. https://doi.org/10.1016/j.ijresmar.2017.02.003

Sharma, M. (2023). How business-to-business and business-to-consumer marketers can future-proof their digital marketing strategies. *Journal of Digital & Social Media Marketing*, *11*(2), 128 154.

Sharma, C., & Kushwah, S. (2025). Mapping the theory of consumption values: a systematic review using the TCCM approach. *Journal of Consumer Behaviour*, *24*(2), 562-610. https://doi.org/10.1002/cb.2434

Sponder, M., & Khan, G. F. (2017). Understanding and working with third-party data. In Digital Analytics for Marketing (pp. 145-166). Routledge.

Shaw, F. A., Wang, X., Mokhtarian, P. L., & Watkins, K. E. (2021). Supplementing transportationdata sources with targeted marketing data: Applications, integration, and internalvalidation. *Transportation Research Part A: Policy and Practice*, *149*, 150-169. https://doi.org/10.1016/j.tra.2021.04.021

Sousa, T. B. (2022, July 6–10). *Customer data platforms: A pattern language for digital marketing optimization with first-party data*. EuroPLoP '22: 27th European Conference on Pattern Languages of Programs, Irsee, Germany. https://doi.org/10.1145/3551902.3551984

Tarabasz, A. (2024). The impact of digital on marketing strategy. In P. B. Pires, J. D. Santos, & I. V. Pereira (Eds.), *Digital marketing: Analyzing its transversal impact* (pp. 21–37). CRC Press. https://doi.org/10.1201/9781003384960

Theodorakopoulos, L., & Theodoropoulou, A. (2024). Leveraging big data analytics for understanding consumer behavior in digital marketing: A systematic review. *Human Behavior and Emerging Technologies*, *2024*(1), 3641502. https://doi.org/10.1155/2024/3641502

Wu, Z. W., Chen, C. T., & Huang, S. H. (2022). Poisoning attacks against knowledge graph-based recommendation systems using deep reinforcement learning. *Neural Computing and Applications*, 1-19. https://doi.org/10.1007/s00521-021-06573-8

Yu, H., Murat, B., Li, L., & Xiao, T. (2021). How accurate are Twitter and Facebook altmetrics data? A comparative content analysis. *Scientometrics*, *126*, 4437-4463. https://doi.org/10.1007/s11192-021-03954-7

Zhou, A., Metaxa, D., Kim, Y. M., & Jaidka, K. (2024). User-Centric Behavioral Tracking: Lessons from Three Case Studies with Do-It-Yourself Computational Pipelines. *Journal of Advertising*, *53*(5), 791-809. https://doi.org/10.1080/00913367.2024.2403613