Rethinking Digital Marketing Ethics in the Metaverse: A Framework for Responsible Engagement

Muhammad Irfan Khalid[1,2(✉)]

[1] Department of Information Systems, University of Agder, 4630 Kristiansand, Norway
muhammad.i.khalid@uia.no, mikhalid@singularlogic.eu
[2] Department of Research and Development and Innovation, Singular Logic, 15561 Athens, Greece

Abstract. The metaverse opens new possibilities for digital marketing but also raises serious ethical concerns, especially around privacy, transparency, and consumer protection. Existing regulations such as the EU General Data Protection Regulation (GDPR), Artificial intelligence Act (AI Act), the Digital Service Act (DSA), Digital Markets Act (DMA), and the Children's Online Privacy Protection Act COPPA (US) offer important ethical principles for digital environments but fall short in addressing the real-time, biometric driven nature of metaverse interactions. This paper presents a comparative analysis of these frameworks, highlighting the regulatory gaps specific to metaverse marketing. To address these gaps, we propose a five-pillar ethical framework that promotes responsible, user-centered marketing in immersive environments. Our analysis concludes that while existing regulations provide a foundation, updated guidance and industry-led practices are essential to ensure user trust, autonomy, and well-being in the evolving digital landscape.

Keywords: Metaverse ethics · Digital marketing · Regulations · GDPR

1 Introduction

The metaverse is an immersive digital environment that exceeds physical reality [1]. It was invented from early innovations like flight simulators and video games, which were later popularized by Neal Stephenson's Snow Crash [2]. The emergence of the metaverse, a persistent network of immersive virtual worlds, is transforming how businesses engage consumers [3]. This convergence of augmented and virtual reality (AR/VR) offers unprecedented opportunities for digital marketing such as brands can create virtual showrooms, sell digital goods, and deliver interactive advertisements within immersive environments. Major companies have already begun experimenting in this space; for example, Nike has launched virtual sneakers and branded experiences to engage users in their own metaverse environments [4].

Published by Springer Nature Switzerland AG 2026
A. Achilleos et al. (Eds.): I3E 2025, LNCS 16079, pp. 362–377, 2026.
https://doi.org/10.1007/978-3-032-06164-5_26

Although extensive research has mapped metaverse's technological innovations, consumer engagement, and commercial opportunities including notable ventures like Gucci's virtual handbag sale [5] and projections of a $56 billion virtual luxury market by 2030 [6], ethical concerns remain underexplored. As businesses increasingly utilize these immersive environments, issues such as consumer privacy, informed consent, extensive biometric and behavioral data collection, algorithmic bias, and psychological manipulation have emerged [7–9]. In an environment where promotional content can blend seamlessly with entertainment, users, especially those unfamiliar with the technology, or children may not even realize they are being targeted by ads [10, 11]. Such blurring boundaries raise dilemmas about informed consent, manipulation of behavior, and the overall fairness of these practices. On the other hand, existing regulations (e.g., GDPR, EU AI Act, COPPA) and Responsible AI principles [12] are insufficient for these challenges. These regulations only partially address these emerging issues.

For instance, the European Union's GDPR [13] mandates consent and data protection by design, but it was written before immersive platforms became reality. New proposals like the AI Act [14] and laws such as the Digital Services Act [15] are relevant, yet no one explicitly covers the real-time, biometric data and hyper-immersive advertising techniques of the metaverse. As a result, marketers and platform operators face uncertainty about how to uphold ethical standards in virtual worlds. This paper addresses this gap by examining current regulatory frameworks and proposing a tailored ethical framework for metaverse marketing. In particular, we aim to ensure user privacy, transparency, and fairness in these novel digital engagements, thereby securing consumer trust and well-being even as technology evolves. This paper addresses the following key questions about ethical digital marketing in the metaverse:

1. How do the technological characteristics of metaverse systems create regulatory compliance challenges for existing privacy frameworks (GDPR, AI Act, COPPA, DSA), and what system design modifications are needed to ensure adequate consumer protection in virtual marketing environments?
2. What are the key components of an ethical framework for metaverse marketing systems that can be operationalized through technical implementation, and how can organizations integrate these ethical principles into their virtual marketing platforms?

2 Background

Existing literature has focused on advocating and achieving the commercial aspects of the technologies related to metaverse such as the use of virtual and augmented realities for marketing purposes. The metaverse presents significant opportunities for marketing, offering immersive 3D environments that allow unique brand experiences and overcome physical limitations [16]. It allows for interactive advertising, virtual product placements, and digital spokespeople, potentially transforming traditional marketing techniques [17]. However, ethical challenges that include data privacy concerns, digital data security, and potential predatory practices [18]. Advertising practices in the metaverse further challenge established disclosure norms [19]. Unlike a clearly labelled sponsored post on a 2D screen, brand messages embedded as dynamic billboards, branded quests, or conversational non-player characters make commercial intent difficult to detect [18–20].

When such content is personalized on-the-fly by artificial intelligence (AI) models using sensitive behavioral signals, the line between legitimate persuasion and covert psychological manipulation becomes blurred [21]. Teenagers who fall outside COPPA's statutory protection and other vulnerable users are therefore exposed to intensified, yet poorly governed, marketing influences [22].

Accordingly, metaverse marketing sits at the intersection of cutting-edge technology and lagging regulation. A clear governance gap leaves practitioners without guidance and users without adequate safeguards, heightening the risk of data exploitation, deceptive persuasion, and insufficient protection for minors [17–19, 23]. Despite the existence of influential data-protection statutes like the EU GDPR [13] and the US COPPA [22], contemporary regulatory and ethical frameworks were envisioned for web-and mobile-based marketing rather than for highly immersive, sensor-rich virtual worlds [17–19, 23]. Metaverse platforms continuously capture eye-tracking streams, full-body motion, and emotional cues through VR head-mounted displays and ancillary biometric sensors data categories [24, 25] that neither GDPR's conventional consent mechanisms nor COPPA's age-verification rules anticipated [26].

In practice, it is un-clear how "freely given, specific and informed" consent can be obtained when a user simply crosses the threshold of a 3D shop that begins tracking gaze in real time, or how parental consent can be enforced when children participate behind easily altered avatars. Given these facts, it is imperative to establish clear principles and adapt existing policies to support responsible, user-centric marketing in immersive virtual environments. This paper addresses that need by analyzing how the metaverse's unique technical features such as persistent digital identities, spatial computing, and real-time interaction transform data collection and marketing tactics. We evaluate current regulatory frameworks by identifying their strengths and gaps and then propose an ethical blueprint that anchors marketing practices in privacy, transparency, and fairness. Our goal is to equip stakeholders to harness the metaverse's innovations while fully protecting fundamental consumer rights. Table 1 summarizes the key scholarly works that call for metaverse-specific ethical and regulatory guidance in the marketing context.

3 Research Method

We conducted a systematic literature review (SLR) covering the metaverse, digital marketing, and ethics, using Scopus and the Association for Information Systems (AIS) eLibrary. The review focused on studies published in the last five years and guided by keywords like "digital marketing ethics," "metaverse marketing," and "biometric data regulation." Our search emphasized works that addressed privacy by design, contextual transparency, and user protection. We prioritized studies with theoretical, empirical, or legal perspectives, highlighting gaps in research on the unique ethical challenges posed by the metaverse, where user data and identities are more complex and immersive interactions are the norm.

This paper presents one key finding from that SLR: an exploration of legislative frameworks relevant to ethical digital marketing in the metaverse, particularly the GDPR, AI Act, DSA, and COPPA. These laws were chosen for their focus on privacy, data protection, and user rights critical for responsible marketing in immersive, biometric-driven

environments. We analyzed regulations, reports from regulatory bodies, and academic literature on the legal implications of digital marketing. By cross-referencing these laws with academic sources, as shown in Table 1 and Section 2, we assessed their relevance to the evolving digital marketing landscape.

Table 1. Existing literature that calls for ethical guidelines in metaverse marketing.

Reference	Context/domain	Rationale for guidelines	Key guidelines themes
[9]	Examination of positive and negative aspects of metaverse marketing practices	Identifies dual nature of metaverse marketing highlighting both opportunities & ethical risks that require a balanced regulatory approach	Responsible marketing practices, risk mitigation strategies, balanced stakeholder engagement, ethical innovation frameworks
[23]	Review of ethical use of extended reality	Finds that there is a need for development/application of laws/guidelines to ethical, legal, and social issues with immersive technologies	Ethical guidelines, Privacy /security by design, transparent controls, responsible identity representation
[19]	Review of immersive marketing techniques used in the metaverse, & outlines their potential risks to consumers	Calls for regulating immersive marketing tactics on large-scale platforms.	Immersive rights, experiential authenticity, emotional privacy, behavioral privacy
[25]	Multidisciplinary review of metaverse impacts	Finds that privacy, bias, disinformation and trust issues outpace existing policy, so coordinated norms are needed	Cross-stakeholder governance; privacy-by-design; consumer-protection rules
[26]	VR biometric-identification study	Shows 94 % accuracy in re-identifying users from motion data, exposing urgent privacy gaps	Data-minimization for biometrics; anonymization & retention limits; auditability
[21]	BISE perspective on metaverse challenges	Calls for frameworks to manage interoperability, security and ethical data use	Risk-assessment protocols; interoperability & open standards; data-protection alignment

(*continued*)

Table 1. (*continued*)

Reference	Context/domain	Rationale for guidelines	Key guidelines themes
[27]	Comprehensive survey of tech & challenges	Identifies security/privacy deficits and urges common standards	Identity management schemes; security-by-design; harmonized legal standards
[24]	Analysis of unprecedented privacy risks	Details intrusive data-harvesting attacks, stressing need for new safeguards	Privacy-by-design; user-centric controls; intrusion-detection mechanisms

4 Analysis of Current Regulatory Frameworks

Several existing laws and regulations provide a starting point for metaverse marketing ethics. Here we present a simplified overview of four key frameworks (GDPR, EU AI Act, the Digital Services Act DSA, and COPPA) focusing on what they cover and where they fall short in the metaverse context. Figure 1 and Table 2 present a detailed comparison of each regulation's applicability to metaverse marketing, identifying specific regulatory gaps and enforcement challenges.

4.1 General Data Protection Regulation

The GDPR is a comprehensive data protection law that gives EU residents control over their personal data. It requires organizations to have a lawful basis (such as explicit consent) for processing personal data, to minimize data collection, and to implement privacy by design and default [13]. These provisions are highly relevant to metaverse platforms. For instance, any collection of biometric data (facial expressions, heart rate, etc.) for marketing would be considered processing of personal data and thus covered by GDPR's strict rules.

GDPR also grants users rights like access to their data and deletion. GDPR does not explicitly anticipate continuous, real-time data streams from immersive devices. Questions remain on how to interpret consent in an always-on VR setting or how to handle sensitive biometric indicators that VR might collect by necessity (are they "special category" data?). Also, enforcement in a borderless virtual world is tricky as metaverse platforms can be accessed globally, raising jurisdictional challenges despite GDPR's reach. GDPR sets important principles which align well with privacy by design and transparency pillars but offers limited practical guidance for the nuances of metaverse technologies.

4.2 EU Artificial Intelligence Act

The AI Act is an EU regulation that regulates AI systems based on their risk level [14]. It categorizes certain AI applications as "high-risk" (for example, AI used in biometric identification or in systems affecting people's rights) and imposes requirements like

transparency, human oversight, and robustness for those systems. In metaverse marketing, AI could be used for emotion recognition, personalized content delivery, or chatbots interacting with users [28]. These might be deemed high-risk if they significantly affect user autonomy or emotions. The AI Act would then require companies to conduct risk assessments and possibly register these AI models with authorities. The AI Act does not explicitly mention metaverse or virtual reality.

Many marketing algorithms might slip under the radar if they are not formally classified as AI or not in a high-risk category. For instance, a subtle algorithm that adjusts ad content based on a user's expressions might not evidently fall under the Act's listed high-risk use cases, even though it perhaps should. Also, the Act focuses on AI governance but not on broader marketing ethics. Therefore, it would not directly address whether an immersive ad is manipulative and only consider the AI component. From our proposed five pillars framework (in Fig. 2), the AI Act could enforce parts of fairness & non-manipulation pillar by discouraging manipulative AI-driven practices, but it leaves several questions on how to apply these rules to metaverse advertising technology.

4.3 Digital Services Act

The DSA is a recent EU law aimed at making online platforms more accountable for content and user protection. It mandates transparency in online advertising, requiring large platforms to clearly label ads and inform users why they were targeted [15]. It also addresses content moderation and illegal content, and for the biggest platforms (termed "Very Large Online Platforms"), it has additional obligations like risk mitigation for societal harms [29]. In a metaverse scenario, if a virtual world or social VR platform has a substantial user base, the DSA would likely consider it under these rules. For example, an immersive platform would need to ensure that advertisements are identifiable as ads to users, just as social media must do. The DSA was written mainly with traditional platforms (like social networks or video-sharing sites) in mind. It does not explicitly cover 3D immersive experiences [15].

Implementing its requirements in VR could be non-trivial. For example, what does an "ad label" look like in augmented reality? The law does not say anything about this part. Moreover, some metaverse environments might be decentralized or smaller community-driven platforms that do not efficiently fit the DSA's thresholds or definitions (for instance, who is the "platform operator" in a fully decentralized world?). The DSA's sister law, the Digital Markets Act [30], targets anti-competitive practices of large tech companies (gatekeepers) but similarly does not consider virtual economies in detail [15]. So, DSA specifies a framework for contextual transparency (forcing disclosure of ads) and some accountability for platforms, but metaverse-specific guidance is lacking. It is expected that regulators would likely need to issue clarifications on how DSA obligations translate to AR/VR contexts.

4.4 Children's Online Privacy Protection Act

COPPA is an American law designed to protect children under 13 by obliging child-directed online services or any service that knowingly hosts children to obtain verifiable parental consent, disclose data practices, and curb behavioral advertising [22]. When

applied to the metaverse, a platform that targets or incidentally serves U.S. children must in theory satisfy those requirements; yet COPPA predates immersive virtual reality and offers no guidance on avatars, biometric tracking, or the anonymous, multi-user interactions typical of virtual worlds. Age-misrepresentation (e.g., a child using a parent headset or a teenager claiming to be an adult) undermines parental-consent mechanisms, and COPPA's upper age limit leaves adolescents (13–17) a core metaverse demographic outside its protection. Moreover, because the law is territorial, global platforms must layer COPPA compliance onto a patchwork of foreign regulations. Thus, COPPA touches only one pillar of the ethical framework proposed in this paper (Fig. 2) which is about the protection of vulnerable users while real-time biometric data, reliable age verification, and the orchestration of multiple actors remain largely unregulated. Its limitations, viewed alongside GDPR [13], (privacy and consent), the EU AI Act [14], (harmful AI practices), and the Digital Services Act [15], (transparency and accountability), underscore the need for updated legislation, industry standards, and best-practice codes that explicitly address data-intensive, immersive marketing environments.

Table 2. Detailed coverage of major regulations for metaverse marketing gaps.

Regulation	Scope & objectives	Key provisions	Metaverse relevance	Potential gaps	Enforcement complexity
GDPR (EU)	Comprehensive data protection; applies to all entities processing personal data of EU residents	Data minimization (Art.5), Lawful basis & consent (Art. 6–7), Special category data (Art.9), Data subject rights (Art.12–23), Privacy by design (Art.25)	Metaverse often involves continuous biometric/behavioural data, Real-time tracking for AR/VR marketing is "personal data," but not explicitly addressed	Lacks explicit guidelines on real time VR data, Cross border enforcement tricky with decentralized platforms, Handling "sensitive biometric data" in continuous streams remains ambiguous	Multinational Enforcement (EDPB & national DPAs) with potential conflicts of jurisdiction

(*continued*)

Table 2. (*continued*)

Regulation	Scope & objectives	Key provisions	Metaverse relevance	Potential gaps	Enforcement complexity
AI Act (EU)	Risk-based regulation of AI systems (covering mainly, transparency, oversight, compliance)	Classification of AI use cases (unacceptable/high risk), High-risk AI: rigorous obligations, Transparency & human oversight requirements	Immersive marketing can involve emotional recognition AI or real-time personalization, could be deemed "high-risk" if it threatens autonomy/safety	Not all VR/AR engines or marketing algorithms are labelled "AI", Lacks direct mention of immersive content, Unclear if emotional analysis ads are "high-risk" under the AI Act's definitions	Will likely require "conformity assessments" for certain AI systems; enforcement reliant on national & EU bodies
Digital Services Act (DSA) / Digital Markets Act (DMA)	DSA: Platform liability & content moderation, DMA: Competition rules for "gatekeeper" platforms	DSA: Transparency for targeted ads, "very large online platform" obligations, DMA: Gatekeeper platforms must allow fair competition, data portability	If metaverse platform is large enough, might be subject to DSA obligations, Ad transparency and content moderation extend to 3D immersive user-generated content	Geared towards 2D social media; not specifically addressing immersive ads, "Gatekeeper" designations might not clearly apply to decentralized metaverse solutions	Enforcement led by EU Commission for gatekeepers; national regulators for other aspects
COPPA (US)	Protects children <13 in online environments	Requires verifiable parental consent, Limits data collection from minors, Mandates privacy notices & safe harbours	Key reference for child protection in digital marketing, potentially relevant if US-based metaverse or under US user base	Does not apply globally, Avatar-based age verification is very difficult, no mention of real-time biometrics, Over-13 adolescences remain unprotected by COPPA	Enforced by US FTC; limited effect outside US jurisdiction

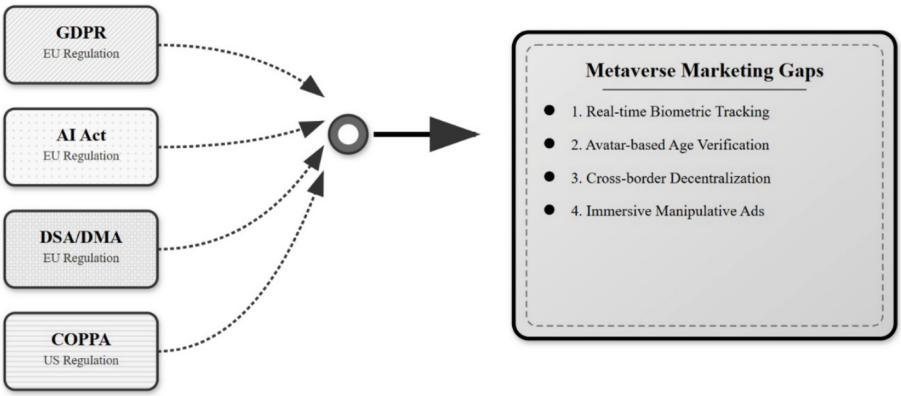

Fig. 1. Existing regulatory landscape vs. metaverse marketing gaps.

5 Proposed Solution: Five-Pillar Ethical Framework

We proposed a five-pillar ethical framework for metaverse marketing gaps as illustrated in Fig. 2. This framework directly responds to the specific gaps and calls for action identified in the existing literature as specified in Fig. 1, and Tables 1 and 2. While previous studies have identified various ethical concerns in isolation, our framework synthesizes these findings into a coherent, actionable model.

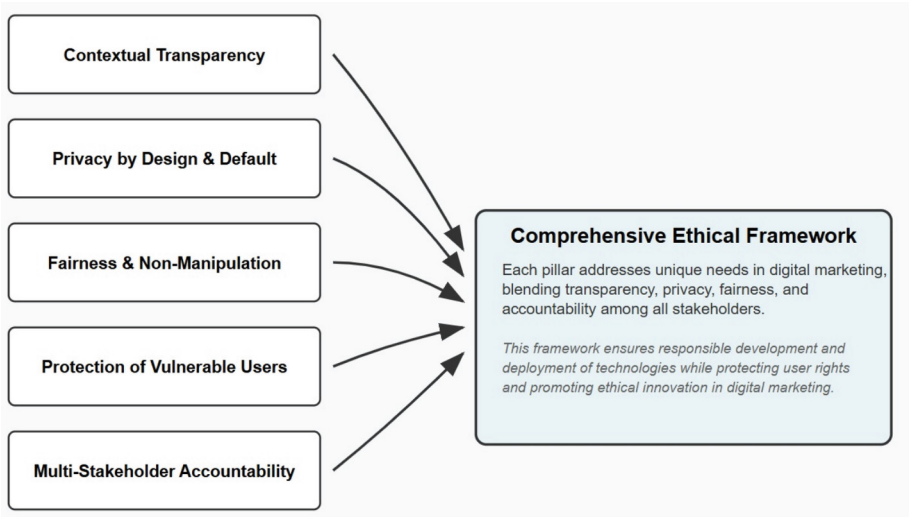

Fig. 2. Five-pillar ethical framework for metaverse marketing.

5.1 Contextual Transparency

The first pillar, contextual transparency, directly responds to Cox et al.'s [23] emphasis on transparent controls and Rosenberg's [19] concern about the difficulty of detecting commercial intent in immersive environments. While Rosenberg [19] identified the problem of brand messages embedded as dynamic billboards, branded quests, or conversational non-player characters, our framework provides the theoretical foundation for solving this challenge through immersive disclosure mechanisms. This pillar extends beyond traditional transparency requirements by addressing the unique challenge that Rosenberg [19] highlighted such as unlike clearly labeled sponsored posts on 2D screens, metaverse marketing blurs commercial intent.

Our theoretical contribution lies in proposing context-aware transparency mechanisms that maintain user awareness without breaking immersion, which is a gap that existing literature identified but did not resolve. Advertising and data practices must be transparent within the users immersive context. Users should clearly know when they are interacting with marketing content or when their data is being collected, even if they are captivated by a virtual experience. In practice, this could mean in-world indicators. For example, subtle labels or visual cues attached to virtual objects that are paid placements, or pop-up notifications that appear in the VR environment to inform a user that certain interactions are being tracked. The goal is to ensure that the immersive nature of the metaverse does not obscure disclosure. Just as websites have cookie notices or ads marked as ads, virtual environments need intuitive mechanisms to maintain honesty with the user. This pillar upholds user awareness and informed consent at all times.

5.2 Privacy by Design and Default

The second pillar builds directly on the privacy-focused proposals throughout the literature, particularly Nair et al.'s [24, 26], urgent calls for new safeguards against intrusive data-harvesting. While Nair et al., in [26] demonstrated 94% accuracy in re-identifying users from motion data, our framework provides the theoretical bridge between identifying privacy risks and implementing systematic protection measures. This pillar synthesizes the privacy-by-design approaches advocated by Dwivedi et al., in [25] Wang et al., in [27], and Peukert et al., in [21], but extends their technical focus by providing a comprehensive framework for embedding privacy into marketing practices specifically.

Unlike previous work that focused on general data protection, our theoretical model addresses the unique challenge of continuous biometric data streams in marketing contexts which basically is a gap that Nair et al., in [24], identified as requiring unprecedented privacy safeguards. Metaverse platforms and marketing tools should prioritize user privacy from the ground up. This principle, rooted in GDPR's philosophy, means that systems should collect the minimum data necessary, protect any data they do collect, and give users control over their personal information by default. For metaverse marketing, "privacy by design" entails technical measures like local processing of sensitive data. It also means data minimization. If a virtual store can achieve its marketing goals without recording every eye gaze or heartbeat of the consumer, then it should avoid collecting those streams. By embedding privacy features into the very architecture of

immersive experiences (for instance, giving users privacy settings or "incognito modes" in VR), this pillar pursues to prevent abuse before it can happen. Privacy isn't an afterthought [31]; rather it is a prerequisite for any metaverse marketing initiative.

5.3 Fairness and Non-manipulation

The third pillar responds directly to Peukert et al., [21] concern about the blurred line between legitimate persuasion and covert psychological manipulation when AI personalizes content using behavioral signals. While Lim et al., [9] identified both bright and dark sides of metaverse marketing, our framework provides specific theoretical guidance for navigating this duality ethically. This pillar reports the manipulative potential that Rosenberg [19] warned regarding intensified, yet poorly governed, marketing influences, particularly for vulnerable users. Our theoretical contribution extends to existing fairness concepts by specifically addressing the immersive context where traditional advertising ethics may not apply.

Unlike general AI ethics guidelines, our framework provides specific guidance for the intersection of AI personalization and immersive marketing, which is a gap that existing literature consistently identified but did not resolve. It is essential that marketing campaigns in the metaverse strive for fair persuasion rather than covert influence. Also, no subliminal advertising marketers should hide messages or stimuli in the virtual environment that affect users subconsciously. Also, any use of AI for personalization should be audited for fairness. For example, an AI model that detects if a user is frustrated might helpfully offer a solution, but it should not capitalize on the emotion of selling an irrelevant product. This pillar echoes principles from existing advertising laws such as the EU's Unfair Commercial Practices Directive [32], which outlaws aggressive and misleading tactics and familiarizes them to the immersive context. This states that marketing should inform and persuade, not deceive.

5.4 Protection of Vulnerable Users

The fourth pillar directly addresses the protection gaps identified across multiple studies. Wilkerson & Dailey in [21] highlighted how teenagers fall outside COPPA's protection, while Rosenberg in [19] noted that vulnerable users are exposed to intensified, yet poorly governed, marketing influences. Our framework provides the theoretical foundation for comprehensive protection that extends beyond existing regulatory frameworks. This pillar synthesizes the child protection concerns raised throughout literature but provides a more comprehensive approach to existing work. While Cox et al., in [23] called for responsible identity representation and existing regulations focus on under-13 protection, our theoretical model extends protection to all vulnerable users in immersive environments by addressing the regulatory gap that multiple studies identified.

Given the difficulty of age verification in a world of avatars, extra effort is needed to prevent harm to minors. This pillar calls for age-appropriate design in metaverse environments. For example, if a user is likely a child, certain advertising features could be turned off or restricted. Metaverse platforms need to implement avatar age verification tools, which could involve analyzing speech or behavior patterns with privacy in mind in order to understand if a user is a child. Marketers should also expand the scope of

"child" protections to include teenagers just because youth above 13 are not covered by COPPA [22], which does not mean they aren't vulnerable. We advocate extending some protections such as limits on targeted advertising or explicit content to all minors under 18 as best practice. Beyond children, "vulnerable users" could include those with certain disabilities or those susceptible to addiction; experiences should be designed so as not to misuse these vulnerabilities.

5.5 Multi-Stakeholder Accountability

The metaverse ecosystem is complex; it includes platform developers, advertisers, content creators, third-party AI vendors, and even users themselves who might create content. This pillar emphasizes clear allocation of roles and responsibilities among these actors. This pillar responds to Dwivedi et al., in [25] call for cross-stakeholder governance and Peukert et al., in [21] emphasis on coordinated frameworks. While existing literature identified accountability gaps, our framework provides the theoretical structure for multi-party responsibility in complex metaverse ecosystems. This pillar addresses the governance challenges that Wang et al., in [27] identified regarding harmonized standards and Cox et al., in [23] call for coordinated ethical guidelines.

For example, if a virtual platform and an advertiser collaborate on a campaign, they should outline who is the data "controller" versus "processor" and agree on standards for protecting user data. Joint accountability agreements, possibly in the form of contracts or codes of conduct, can guarantee that if something goes wrong, such as a data breach or an unethical ad slip through, no one can simply point fingers at others. Additionally, multi-stakeholder accountability involves cross-border cooperation. Metaverse worlds are not confined to one country, so regulators will need to collaborate internationally for enforcement. In essence, this pillar is about building an accountable governance structure for the metaverse, so that ethical norms are upheld collectively and transparently.

6 Discussion

The proposed theoretical framework directly responds to the calls for action identified throughout the literature review as reported in Tables 1 and 2 & Fig. 1. Dwivedi et al., [25] called for coordinated norms, Cox et al. [23] advocated for ethical guidelines, and Rosenberg [19] demanded regulatory responses. Our five-pillar framework provides theoretical foundation for systematic, coordinated action. The framework's significance lies not only in addressing individual concerns raised by previous studies but in synthesizing these concerns into a coherent theoretical model. By connecting the privacy imperatives identified by Nair et al., in [24, 26], the manipulation concerns raised by Peukert et al., in [21], the transparency needs highlighted by Rosenberg in [19], and the governance gaps noted by Wang et al., in [27] and Dwivedi et al., in [25], this paper provides the theoretical bridge between problem identification and systematic solution development that the literature has been calling for as described in Table 1.

6.1 Theoretical and Practical Implications:

These five pillars form a comprehensive ethical framework. They are interrelated (for instance, transparency and privacy by design both contribute to user trust, and protecting vulnerable users is a facet of fairness), and together they address the core challenges outlined in our research questions. By adopting this framework, industry players can proactively self-regulate to some extent, and policymakers can identify where guidance or new rules are needed. Table 3 provides a clear mapping of each discussed regulation to our five-pillar ethical framework, identifying key gaps for both metaverse technology development communities and businesses seeking to use these technologies for marketing purposes.

This framework makes several key theoretical contributions that directly address gaps identified in existing literature. While technical studies like Nair et al., in [24, 26] and Wang et al., in [27] focused on identifying privacy and security risks, and ethical studies like Rosenberg in [19] and Cox et al., [23] called for regulatory responses, our framework provides the missing theoretical link between risk identification and practical ethical implementation. Our framework also addresses Dwivedi et al., [25] observation that ethical issues outpace existing policy. The literature consistently identified problems such as Peukert et al., in [21] noted blurred manipulation lines, Rosenberg in [19] highlighted disclosure challenges, Nair et al., demonstrated privacy vulnerabilities but provided limited theoretical guidance for systematic solutions [24].

These gaps have been filled by our coherent theoretical model that addresses these identified problems comprehensively. Lim et al., in [9], recognition of both bright and dark sides of metaverse marketing highlighted the need for balanced approaches. Our framework provides the theoretical foundation for this balance, unlike previous work that focused primarily on restrictions or purely on opportunities. While existing regulations like GDPR [13] and COPPA [22] provide important foundations, the literature consistently noted their inadequacy for immersive environments. Our framework extends regulatory theory by providing principles specifically designed for the unique characteristics of metaverse marketing that Rosenberg [19] and Cox et al., [23] identified as inadequately addressed.

The proposed ethical framework, while conceptual, can be practically implemented through collaboration among regulatory bodies, marketing organizations, and technology companies. Companies could integrate privacy-by-design principles, offering users granular control over their data, particularly biometric and behavioral data. Real-world testing, such as in virtual marketplaces, could assess how the framework's principles, like contextual transparency and user protection, work in practice, including age-gating mechanisms for vulnerable users. To validate the framework empirically, real-time data collection and user feedback could be used to track key performance indicators like consent rates and transparency scores, while longitudinal studies could provide insights into the long-term impacts of responsible marketing in the metaverse.

Table 3. Mapping regulations to the proposed five-pillar ethical framework.

Ethical pillar	Relevant regulations	How they currently address (or don't) this pillar	Key gaps & opportunities
Contextual Transparency	GDPR (Art. 13–14: information duties) DSA (ad labelling)	GDPR requires transparent data collection notices, DSA mandates ad disclosure for large platforms	Immersive disclaimers not clearly defined, need "in-world" real-time notices in VR/AR, Opportunity to develop standardized UX for consent in 3D environments
Privacy by Design & Default	GDPR (Art. 25), e-Privacy Directive	Foundational in GDPR, but typically oriented toward web/app contexts	Requires continuous data approach for VR/AR, Guidance or best practices for on-device or localized biometric processing
Fairness & non-manipulation	AI Act (transparency, oversight), Unfair Commercial Practices Directive (UCPD)	AI Act references avoiding manipulative AI, UCPD prohibits misleading or aggressive commercial practices	Subliminal AR/VR ads not explicitly covered, Real-time emotional recognition for marketing might not be classified as "high-risk AI", Clear definition of "manipulation" in VR needed
Protection of Vulnerable Users	COPPA, GDPR child-specific recitals, National child protection laws	COPPA is a main child privacy standard in the US, GDPR calls for special data protection for children, Some EU states have age-appropriate design codes	Avatar identity complicates age checks, no robust system for verifying minors in VR, Over-13 teens remain a grey zone in both EU & US regulations
Multi-Stakeholder Accountability	GDPR (joint controllers), DSA (platform liability)	GDPR acknowledges joint liability among controllers/processors, DSA focuses on platform responsibilities	Metaverse often decentralized: roles for platform operators, marketers, AI providers, content creators, etc., Mechanisms for cross-border user complaints still underdeveloped

7 Conclusion

This paper analyzes how the metaverse enables new forms of immersive brand engagement while creating privacy and manipulation risks that current regulations inadequately address. We develop a five-pillar ethical framework for metaverse marketing, implemented through transparent interface design, systematic AI ethics audits, and comprehensive child protection measures. This framework requires coordinated regulatory oversight and industry self-regulation via enforceable conduct standards. Such dual governance can transform the metaverse from an unregulated domain into a managed environment where immersive marketing coexists with robust consumer protection.

Acknowledgments. This research was funded by the European Union's Horizon Europe research and innovation programme "Training Young Researchers on Shaping Metaverse for Business and Social Value (AGORA)" under the Marie Skłodowska-Curie grant agreement No 101119937.

References

1. Dolata, M., Schwabe, G.: What is the Metaverse and who seeks to define it? Mapping the site of social construction. J. Inf. Technol. **38**(3), 239–366 (2023)
2. Stephenson, N.: Snow Crash. Bantam Books, New York (1992)
3. Polyviou, A., Pappas, I.O.: Metaverses and business transformation. In International Working Conference on Transfer and Diffusion of IT, pp. 314–319. Springer International Publishing, Cham (2022)
4. Nike: Nike acquires RTFKT. Nike Press Release (2021). https://about.nike.com/en/newsroom/releases/nike-acquires-rtfkt/1000
5. The Fashion Law: A digital-only gucci bag sold for $4,115 on roblox, as brands continue to look to gaming to reach gen-z (2022). Accessed 18 April 22. https://www.thefashionlaw.com/a-digital-only-gucci-bag-sold-for-4115-on-roblox-as-brands-continue-to-look-to-gaming-as-reach-gen-z/
6. Business Insider: Luxury nft could become a $56 billion market by 2030 (2022). https://markets.businessinsider.com/news/currencies/luxury-nfts-metaverse-56-billion-market-revenue-2030-morgan-stanley-2021-11.
7. Al-Kfairy, M., Alomari, A., Al-Bashayreh, M., Alfandi, O., Tubishat, M.: Unveiling the Metaverse: A survey of user perceptions and the impact of usability, social influence and interoperability. Heliyon (2024)
8. Su, Y., Wang, E.J., Berthon, P.: Ethical marketing AI? A structured literature review of the ethical challenges posed by artificial intelligence in the domains of marketing and consumer behavior (2023)
9. Lim, W.M., Bansal, S., Nangia, P., Singh, S.: The bright and dark side of metaverse marketing. Glob. Bus. Organ. Excell. **44**(2), 58–82 (2025)
10. Zhuk, A.: Ethical implications of AI in the Metaverse. AI and Ethics, 1–12 (2024)
11. Sharma, S., et al.: User safety and security in the metaverse: a critical review. IEEE Open Journal of the Communications Society (2024)
12. Kumar, D., Suthar, N.: Ethical and legal challenges of AI in marketing: an exploration of solutions. J. Inf. Commun. Ethics Soc. **22**(1), 124–144 (2024)
13. Voigt, P., Von dem Bussche, A.: The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Springer International Publishing, Cham **10**(3152676), 10–5555 (2017)

14. European Union: AI Act (Regulation (EU) 2024/1689). Available via https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689
15. Chiarella, M.L.: Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment. Athens JL **9**, 33 (2023)
16. Dwivedi, Y., Hughes, L.: In search of a head start: marketing opportunities in the metaverse. NIM Marketing Intelligence Review **15**(2), 18 (2023)
17. Rosenberg, L.: Marketing in the metaverse and the need for consumer protections. In: 2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0035–0039. IEEE (2022)
18. Rosenberg, L.B.: The growing need for metaverse regulation. In: Proceedings of SAI Intelligent Systems Conference, pp. 540–547. Springer International Publishing, Cham (2022)
19. Rosenberg, L.: Marketing in the metaverse: emerging risks. In: Future of Information and Communication Conference, pp. 41–51. Springer Nature Switzerland, Cham (2023)
20. Dwivedi, Y.K., et al.: Metaverse marketing: How the metaverse will shape the future of consumer research and practice. Psychol. Mark. **40**(4), 750–776 (2023)
21. Peukert, C., Weinhardt, C., Hinz, O., van der Aalst, W.M.: Metaverse: How to approach its challenges from a BISE perspective. Bus. Inf. Syst. Eng. **64**(4), 401–406 (2022)
22. Wilkerson, J., Dailey, M.: Protecting Child Online Data Privacy in the Age of AI: A COPPA Theoretical and Policy Analysis (2024)
23. Cox, S., Kadlubsky, A., Svarverud, E., Adams, J., Baraas, R.C., Bernabe, R.D.: A scoping review of the ethics frameworks describing issues related to the use of extended reality. Open Research Europe **4**, 74 (2025)
24. Nair, V., Garrido, G.M., Song, D.: Exploring the unprecedented privacy risks of the metaverse. CoRR (2022)
25. Dwivedi, Y.K., et al.: Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. Int. J. Inf. Manage. **66**, 102542 (2022)
26. Nair, V., et al.: Unique identification of 50,000+ virtual reality users from head & hand motion data. In: 32nd USENIX Security Symposium (USENIX Security 23), pp. 895–910 (2023)
27. Wang, H., et al.: A survey on the metaverse: The state-of-the-art, technologies, applications, and challenges. IEEE Internet Things J. **10**(16), 14671–14688 (2023)
28. Soliman, M.M., Ahmed, E., Darwish, A., Hassanien, A.E.: Artificial intelligence powered Metaverse: analysis, challenges and future perspectives. Artif. Intell. Rev. **57**(2), 36 (2024)
29. Eder, N.: Making systemic risk assessments work: how the DSA creates a virtuous loop to address the societal harms of content moderation. German Law Journal **25**(7), 1197–1218 (2024)
30. Cabral, L., et al.: The EU digital markets act: a report from a panel of economic experts. In: Cabral, L., Haucap, J., Parker, G., Petropoulos, G., Valletti, T., Van Alstyne, M., (eds.) The EU Digital Markets Act. Publications Office of the European Union, Luxembourg (2021)
31. Balebako, R., Cranor, L.: Improving app privacy: Nudging app developers to protect user privacy. IEEE Secur. Priv. **12**(4), 55–58 (2014)
32. Howells, G., Micklitz, H.W., Wilhelmsson, T.: European fair trading law: the unfair commercial practices directive. Routledge (2016)