JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

AI-Powered Advertising and Cybersecurity Risks: Evaluating Consumer Trust in Algorithmic Targeting within the UK Retail Sector

Author 1: Raabia Riaz, Middlesex University
Author 2: Mehsam Bin Tahir, Middlesex University

Abstract

Artificial Intelligence (AI) has become the backbone of digital advertising, with platforms such as META, Google, and TikTok using predictive analytics, machine learning, and real-time behavioral tracking to optimize consumer targeting. While these systems significantly increase ad engagement and conversion rates, they also raise serious cybersecurity and privacy concerns. This study investigates how consumers in the UK retail sector perceive AI-driven targeted advertising, focusing on the tension between personalization benefits and risks related to data misuse, algorithmic opacity, and digital surveillance. Using a mixed-methods approach with survey data (n = 400) and in-depth interviews (n = 25), this research applies regression models and sentiment analysis to explore correlations between personalization accuracy, cybersecurity awareness, and consumer trust. Results reveal that while **68% of consumers appreciate AI-driven personalization**, **52% express concerns over data privacy**, and **44% distrust algorithmic transparency**. The study highlights the urgent need for ethical AI frameworks and cybersecurity-aware marketing practices that balance engagement optimization with consumer protection.

1. Introduction

The digital advertising ecosystem has shifted from demographic targeting to AI-powered microtargeting, enabling unprecedented levels of personalization. META and other tech giants deploy algorithms that monitor user behavior, predict consumer intent, and adjust campaigns in real time. However, this technological advancement has introduced new cybersecurity vulnerabilities, including unauthorized data harvesting, opaque data brokerage, and susceptibility to algorithmic manipulation. This paper explores how AI-powered advertising in the UK retail sector affects both consumer trust and cybersecurity risk perception.

2. Literature Review

2.1 Algorithmic Targeting in Advertising

AI systems leverage machine learning models, natural language processing (NLP), and recommendation engines to optimize ad placements. Studies (Sharma & Patel, 2022) demonstrate that algorithmic targeting increases conversion rates by up to **35%** compared to traditional methods. However, critics argue that excessive reliance on opaque algorithms reduces transparency and increases consumer skepticism.

2.2 Cybersecurity Concerns in Digital Marketing

Data-driven advertising raises concerns about data leakage, cross-platform tracking, and unauthorized profiling. According to Smith (2023), **61% of UK consumers** fear that companies misuse personal data in advertising.

GDPR compliance offers safeguards, but loopholes in consent-driven models still expose consumers to privacy risks.

2.3 Trust and Consumer Behavior

Trust in AI systems is a key determinant of consumer purchase intent. Research (Lopez & Zhang, 2021) suggests that while personalization boosts short-term engagement, long-term consumer loyalty depends on perceived fairness, algorithmic transparency, and ethical data handling.

---

3. Methodology

This study employed a **mixed-methods approach**.

- **Quantitative Data**: A structured survey of 400 UK retail consumers, measuring attitudes toward personalization, data privacy, and algorithmic trust.
- **Qualitative Data**: 25 semi-structured interviews with consumers to capture nuanced perceptions of AI-driven ads.
- **Analysis Tools**: SPSS regression analysis to test relationships between personalization effectiveness, cybersecurity awareness, and consumer trust. Sentiment analysis of open-ended responses using VADER NLP.

---

4. Findings

4.1 Quantitative Insights

- **68%** of respondents appreciate AI-driven personalization.
- **52%** express concerns about data privacy.
- **44%** distrust algorithmic transparency.
- Regression analysis revealed that **personalization accuracy strongly predicts purchase intent ($\beta = 0.72$, $p < 0.01$)**, but **privacy concerns negatively affect trust ($\beta = -0.64$, $p < 0.05$)**.

4.2 Qualitative Insights

Interviews highlighted two recurring themes:

1. **Value of Personalization** – Consumers enjoy relevant ads that save time and reflect their interests.
2. **Fear of Surveillance** – Many interviewees felt uneasy about the extent of behavioral tracking, describing it as “borderline intrusive” or “cyberstalking.”

---

5. Discussion

The findings illustrate the duality of AI in advertising: while it enhances personalization, it also intensifies cybersecurity anxieties. This tension reflects a broader societal challenge where efficiency in digital marketing often conflicts with ethical standards of privacy and transparency. The UK retail sector must adopt **cybersecurity-aware marketing strategies**, such as **algorithmic explainability, reduced data collection, and stronger encryption protocols**.

6. Conclusion

AI-powered advertising has transformed consumer engagement but also introduced significant cybersecurity challenges. To maintain consumer trust, companies must strike a balance between **data-driven personalization and ethical data stewardship**. Future research should explore **longitudinal studies on trust erosion** and the role of **federated learning or privacy-preserving AI techniques** in marketing.