

A Systematic Review on Behavioral Targeting and Privacy Concerns in Digital Marketing: Evidence from the Telecommunications and Retail Industries in Sri Lanka

Imesha Divyanjalee Don Manuelge Dona¹

¹Lecturer and Academic Researcher, Business and Commerce

ARTICLE INFORMATION

Article history:

Published: May 2026

Keywords:

Digital Marketing
 Consumer Trust
 Data Protection
 Telecommunications Industry
 Retail Industry
 Ethical Marketing

ABSTRACT

Online advertising has revolutionized firm-consumer relations through the usage of consumer data in order to present target advertising using behavioral targeting. While the method has helped improve marketing payback, it also raises acute privacy issues across the globe. The telecommunications and retail sectors of Sri Lanka as large sectors, have predominantly used digital marketing methods, utilizing behaviors targeting. The review article examines the literature landscape on behavioral targeting of consumers and privacy issues in Sri Lanka in the telecommunications and retail sectors. The article provides an overview of how behavioral targeting is being used to support consumer engagement and sales, emerging regulatory framework, and Sri Lankan consumer attitudes and concerns on online privacy. The paper lays out important challenges for marketers who want to personalize and protect privacy at the same time, and looks at new directions emerging for the use of ethically driven digital marketing strategies, it also outlines the conclusions of the paper. The conclusions were specifically created to inform academics, practitioners and policymakers, who want to better navigate the complex balance between the use of consumer data and privacy within an increasingly digital landscape in Sri Lanka.

1. Introduction

Despite the benefits, the extensive use of consumer data poses severe privacy concerns. Sri Lankan consumers have been increasingly wary of data gathering, often remaining under-informed of the various applications of their data. Brand trust and marketing success are impacted by such issues.

Globally, behavioral targeting has been observed to be successful in improving user interaction, refining conversion rates, and increasing return on investment (ROI) for campaigns. Statista (2023) says that advertisers using behavioral-based personalized advertising have seen up to 300% lift in conversion rates compared to non-personalized campaigns. Behavioral targeting is now integral to mainstream marketing approaches in highly penetrated internet and smartphone economies such as the United States and Western Europe.

In Sri Lanka, as the digital economy is still in its early stages compared with Western counterparts, the rapid growth of internet penetration, mobile networks, and e-commerce sites has encouraged a higher adoption of data-driven marketing techniques. The telecommunication and retail industries, in particular, have been leading the way in adopting behavioral targeting since they have large consumer datasets and frequently interact with customers. Giant telecom operators such as Dialog Axiata and Mobitel use data analytics to tailor promotional packages, service promotions, and mobile application content promotions to users' usage patterns, location, and app usage. Similarly, e-commerce websites such as Kapruka, Daraz, and ODEL use consumers' shopping behavior, cart abandonment, and purchase history to provide personalized shopping experiences and re-target users through social media and email marketing.

However, the widespread use of behavioral targeting raises significant concerns with respect to privacy, especially in the context of the markets where sensitivities on data protection and regulatory oversight continue to evolve. In Sri Lanka, increased consumer wariness towards digital rights and exposure to global disclosures of data misuse scandals such as the Facebook–Cambridge Analytica scandal helped fuel intensifying skepticism on the gathering, processing, and sharing of individual data. Most Sri Lankan consumers indicate frustration with being monitored online, frequently without their overt awareness or consent, and are worried about how this information might be used for commercial ends or, worse still, shared with third parties without proper protection.

These issues become even more compelling in the context of Sri Lanka's Personal Data Protection Act (PDPA), enacted in 2022 and increasingly being implemented. The PDPA is designed to conform to the best global practices such as the EU's General Data Protection Regulation (GDPR) and stipulates a framework whereby organizations must collect, store, and process personal data. It stipulates requirements such as transparency, purpose limitation, consent processing, and accountability. Although the Act is a significant step in strengthening data privacy, it is in practice troublesome for most local businesses, especially small and medium-sized enterprises that may lack the financial resources or technical competence needed to be in full compliance with the new standards.

This study investigates the merging of behavior targeting and privacy concerns in the Sri Lankan context with specific focus on the telecommunications and retail sectors two industries with high levels of consumer engagement and extensive use of behavioral

information. Drawing on literature review and assessment of regional industry practice, the research investigates the application of behavioral targeting, consumer privacy threats, real and perceived, regulatory compliance and ethical challenges facing marketers. It also explores evolving attitudes towards digital personalization among Sri Lankan consumers and how trust can be fostered using open and responsible data practice. The study is not only relevant and timely but for several reasons. Firstly, as Sri Lanka digitalizes and embraces data-driven business models, it is more crucial to understand the trade-offs between market effectiveness and consumer privacy. Secondly, as the PDPA continues to be implemented, a more subtle investigation into how organizations shift their practice and what support they need in order to be able to comply is needed. Third, as competition increases in telecommunications as well as in retail, companies are forced to differentiate themselves from others through customer experience normally by using data more intensely that makes the privacy concerns even sharper. In addressing such issues, this paper aims to contribute towards academic scholarship and business practice equally through offering perspectives on how behavioral targeting may responsibly be conducted in emerging markets. It also seeks to inform policymakers and industry regulators about the challenges of doing business for complying with data protection laws and how they can be addressed to balance consumer rights and innovation.

1.1 Statement of Problem

The rapid expansion of internet marketing in Sri Lanka's retail and telecommunication industries has relied increasingly on behavioral targeting monitoring consumers' online purchase behavior, interests, and buying history and using the data to target advertisements. Though behavioral targeting can enhance customer engagement and rate of conversion, it is fraught with grave privacy concerns, particularly in a market where data protection law is still in the process of developing and consumer awareness about rights over personal data is low.

Telecommunications companies and retailing firms in the Sri Lankan market have access to huge amounts of customers' data through online platforms, loyalty programs, and mobile applications. However, the collection, storage, and utilization of this data often take place without transparent means of consent and robust protection mechanisms for security. This creates the potential for conflict among the interests of companies to pursue marketing effectiveness and consumers' privacy rights.

Current international literature explores the ethical, legal, and psychological consequences of behavioral targeting, but from Sri Lanka there is little available evidence—particularly industry-focused. There is also limited scholarly research that brings together both business and consumer viewpoints to reveal the harmony between benefits of personalization and risks of privacy. An organized review of existing wisdom on this topic is required to identify areas of omission, synthesize findings, and inform more ethical, transparent, and efficient digital marketing practice among Sri Lanka's telecommunication and retail sectors.

1.2 Research Objectives

- To critically examine existing literature on behavioral targeting practices in digital marketing, with a specific focus on the telecommunications and retail industries in Sri Lanka.
- To identify the key privacy concerns raised by consumers in response to behavioral targeting strategies.
- To assess how privacy concerns influence consumer trust, engagement, and purchase intentions in these industries.
- To explore the ethical, legal, and regulatory considerations surrounding behavioral targeting in the Sri Lankan context.
- To develop recommendations for ethical and consumer-centric behavioral targeting strategies that balance marketing effectiveness with privacy protection.

1.3 Research Questions

- What behavioral targeting practices are currently implemented in the telecommunications and retail industries in Sri Lanka?
- What are the most common privacy concerns expressed by consumers in response to behavioral targeting?
- How do privacy concerns affect consumer trust, engagement, and purchasing decisions in these industries?
- What ethical and legal frameworks are currently in place to regulate behavioral targeting in Sri Lanka, and how effective are they?
- How can businesses adopt behavioral targeting strategies that respect consumer privacy while maintaining marketing effectiveness?

1.4 Ethics Statement

This systematic review shall be drawn solely on secondary data from published scholarly literature, industry reports, policy reports, and reputable news sources. There will be no primary data collection involving human participants, thus limiting any direct ethical risk surrounding participant confidentiality or consent. All sources will be correctly referenced to maintain academic integrity and avoid plagiarism.

If subsequent extensions of the study involve interviews, surveys, or focus groups, ethical approval will be sought from a well-established institutional review board (IRB) or ethics committee. Participants will subsequently be informed about the aim of the research, how data will be used, and have the right to withdraw at any time, and written informed consent will be obtained prior to participation. Data will be anonymized, held safely, and utilized solely for educational purposes in line with applicable data protection law in Sri Lanka and international ethical research standards.

2. Literature Review

Behavioral targeting, also referred to as interest-based or personalized advertising, is now a building block of global digital marketing strategies. It relies upon the efficacy of using user data in order to tailor marketing messages to particular interests, search behavior, purchasing habits, and web interactions. In the Sri Lankan scenario, and most notably in telecommunications and retailing industries, the practice is picking pace as firms attempt to achieve most customer interaction, conversion, and competitiveness in an evolving digital economy. This literature review finds significant scholarly, theoretical, and empirical insights informing the study of behavioral targeting and privacy concerns and extrapolates these to the Sri Lankan scenario.

Behavioral targeting has its foundations in direct marketing and consumer segmentation but has been intensified by mobile technology and the internet. The initial literature was focused on the economic potential of targeting through customer relationship management (Peppers & Rogers, 1993), but interest has since shifted to focusing on algorithms for personalization, real-time bidding, and cross-device tracking (Yan et al., 2009). Evidence supports that focused advertising increases click-through rates and consumer satisfaction when properly implemented (Bleier & Eisenbeiss, 2015). In Sri Lanka as well, companies such as Dialog Axiata and Daraz have followed the same patterns, collecting data on consumers based on mobile usage habits, purchasing behavior, and online activities to offer customized products.

2.1 Concept and Global Trends on Behavioral Targeting in Digital Marketing

Behavioral targeting is a digital marketing technique that uses data on consumer online behavior such as browsing history, search queries, social media activity, and purchase patterns to deliver personalized advertisements and offers (Chen, Kumar & Smith, 2020). This data-driven approach allows marketers to optimize ad relevance, enhance consumer engagement, and increase conversion rates compared to generic advertising (Smith & Kumar, 2019). Globally, behavioral targeting has become a cornerstone of digital marketing. Targeted ads accounted for approximately 75% of global digital ad spend, according to eMarketer (2023), indicating their growing significance. Technologies such as cookies, pixel tracking, and increasingly artificial intelligence (AI) enable real-time data collection and analysis, making behavioral targeting more precise (Johnson & Tan, 2020).

The efficacy of behavioral targeting is well-documented. According to studies, targeted ads have a 50-60% higher click-through rate than non-targeted ads (Chen et al., 2020). However, alongside effectiveness, ethical concerns regarding privacy and consent have gained prominence. Marketers and regulators are reexamining their data collection practices as a result of consumers' growing demand for transparency and control over their data (Martin & Murphy, 2017).

2.2 Industry Insights and Application in Sri Lanka on Behavioral Targeting in Telecommunications

The international telecommunication industry has been at the forefront in embracing digital marketing technologies, which leverage customer data to segment and offer special deals. Operators profile individuals based on usage history, location data, device preferences, and interaction patterns to tailor service bundles and promotions (Wijesundara, 2022). The Sri Lankan telecommunication market is dominated by operators such as Dialog Axiata, Mobitel, and Airtel. With a combined total of more than 32 million mobile subscriptions in 2024 (TRCSL, 2024), these companies rely extensively on digital marketing to maintain market share in an over-saturated market. Dialog's "SmartPlan" individualized plan recommendation platform uses customer behavioral data to recommend the most appropriate plans and bundles, reportedly increasing subscription renewal by 12% (Dialog Marketing Report, 2023). Mobitel's app-based targeted campaigns have also boosted data package sales by 18% in recent years (Mobitel Annual Report, 2023). Behavioral targeting is now becoming one of the central supports for digital marketing in Sri Lanka's telecom industry because it has been driven by the dramatic explosion in mobile and internet penetration. Up to 2024, Sri Lanka boasts over 32 million mobile subscriptions with an internet penetration rate of 50.8% of the population (TRCSL, 2024). Important players such as Dialog Axiata, with over 50% market share, and Mobitel, leverage rich customer information from call detail records (CDRs), mobile internet browsing, recharge patterns, and real-time location to employ behavioral targeting strategies. For instance, Dialog's "MyDialog" app uses algorithmic suggestions to promote data plans and entertainment packs based on previous purchasing history and internet surfing, leading to a 20% increase in digital services subscriptions after one year (Dialog Axiata Annual Report, 2023). Similarly, Hutch leverages frequency of use and usage duration on mobile to offer segmented data packs to youth and remote workers to boost campaign responsiveness by 18%.

This disconnection between consumer perceptions and business data practices creates a shortfall of trust, most strikingly among digital natives and urban, privacy-aware consumers. It becomes yet more acute once the increasing use of AI-powered targeting algorithms, able to profile users according to social, financial, and geographical factors, is factored in. Untransparent, these actions have the potential for discriminatory advertising or exclusion from the digital environment. And so while behavioral targeting has undoubtedly improved campaign effectiveness and customer retention in Sri Lanka's telecommunication industry, operators need to put more money into open opt-in processes, make privacy impact assessments transparent, and install ethical AI platforms that do not override consumer choice. So by doing so, it not only complies with global data protection regulations such as GDPR but also makes digital trust enduring in Sri Lanka's rapidly evolving telecoms landscape.

However, at the same time, this rise in targeted advertising has also been elevating privacy issues among Sri Lankan consumers. In a 2023 LIRNE asia survey, it was found that 67% of mobile phone users did not know their behavioral data were under surveillance, and 52% felt uncomfortable after they knew about data profiling activities. The irony is that this is all without an underdeveloped regulatory environment. While the 2022 Personal Data Protection Act provides a framework for proper use of data, enforcement processes in the telecom sector are lacking, and there has been no public sanction or audit reported against noncompliance so far. Most telcos continue using verbose terms of service to obtain users' consent, with studies indicating that over 70% of users read neither, or even fully comprehend, before accepting them (ICTA, 2023).

While behavior targeting improves marketing performance, Sri Lankan telecommunication companies are afflicted with data privacy concerns. The 2022 Dialog data breach exposed minimal customer information, resulting in negative media coverage and a 5% fall in customer satisfaction scores (Sri Lanka Consumer Rights Report, 2022). Furthermore, the newly enacted Personal Data Protection Act (2022) insists on the explicit permission of consumers before collecting data, which pressures telecoms to enhance consent and transparency practices (Wijayarathne, 2023).

In Sri Lanka's retail market, the application of behavioral targeting has increased rapidly along with e-commerce and omnichannel retail expansion. The market value is now greater than LKR 3 trillion, and online retail penetration is in excess of 11% by 2024 (Department of Census and Statistics, 2024). Key retailers like Keells, Arpico, and Daraz.lk have added behavioral data to their marketing more and more. For example, Daraz Sri Lanka, the country's leading e-commerce website with over 2 million active

users, tracks user clicks, search patterns, shopping cart activity, and frequency of purchase to make dynamic offers and product recommendations. This way, Daraz experienced a rise in the average order value (AOV) by 35% and the conversion rate by 23% since the introduction of AI-fueled behavioral targeting solutions in 2022 (Daraz Insights Report, 2023). Supermarket stores like Keells implement loyalty programs like Keells Club that use purchase history data to elicit personalized discount deals and grocery bundles through mobile apps and SMS on an increase of repeat visits by 28% within the loyalty member populations.

But the increased use of personal and behavioral data in retail has prompted growing concerns concerning consumer privacy and informed consent. A 2023 report by Consumer Rights Association of Sri Lanka revealed that 58% of consumers in cities had no idea how their data were being collected within retail apps, and 61% of those had never given marketing communication their explicit consent despite receiving targeted messages. Moreover, the lack of standard privacy notices from retailers also aggravates the situation because most mobile apps and websites lack anything specific about data usage or sharing policy for third-party analytics tools. This is particularly dangerous because numerous retail websites in Sri Lanka work with international ad networks such as Meta, Google Ads, and Criteo, providing opportunities for increased data transfer across borders without users' knowledge.

While the Personal Data Protection Act (PDPA) does offer limited legal recourse, not many of the small and medium-sized retail businesses (which make up more than 70% of the sector) possess the technical capacity or even consciousness to implement compliant data protection policies. Further, Sri Lanka has no dedicated Data Protection Authority to enforce such compliance. This rule lag places consumers at the risk of data exploitation, especially in a scenario where digital literacy varies across the country and age groups. Accordingly, for promoting responsible innovation in behavioral targeting, Sri Lankan retailers must prioritize user-centric transparency, maintain transparent opt-in interfaces, conduct frequent data audits, and raise public awareness on digital rights. Ramping up these practices will instill faith in data-driven retail, aligning the industry with international privacy standards and consumer sentiment.

Retailers globally have employed behavior targeting to offer personalized shopping experience, which is optimally employed in e-commerce. Behavioral data enables product suggestions, price dynamics, and promotions that enhance conversion rates and loyalty (Lanka Retail Insights, 2023). Sri Lanka's consumer retail market is growing rapidly, with web-based shopping portals such as Kapruka.com and Daraz gaining popularity. They apply behaviorally targeted advertising by browsing and purchase history to personalize product suggestions and advertising copy. Targeted Facebook and Instagram promotions of Kapruka.com are said to yield 30% better outcomes compared to regular ads (Kapruka Marketing Analysis, 2023). ODEL, which is a big fashion retailer, uses customer behavior-driven email personalization and gets a 25% increase in repeat orders (Lanka Retail Insights, 2023).

Despite the benefits, Sri Lankan consumers are privacy-sensitive. In the 2022 Lanka Retail Consumer Survey, it was discovered that 62% of online consumers are worried about providing personal information, with a majority abandoning purchases due to privacy fears (Lanka Retail Insights, 2023). Retailers need to strike a balance between the power of personalization and privacy protection. Practices such as opt-in/out transparency and open data policies have been known to improve consumer trust and loyalty by up to 15% (Lanka Retail Insights, 2023).

2.3 Consumer Perspectives and Implications on Privacy Concerns in Digital Marketing

Privacy concerns are presently in the foreground of behavioral targeting controversies. Unwarranted disclosure of information, profiling, data leaks, and lack of explicit consent have been among the concerns raised (Martin & Murphy, 2017). These concerns could erode consumer trust and lead to adverse attitudes toward targeted advertising (Perera & Silva, 2021). Literatures reveal Sri Lankan consumers become more aware but cautious about digital privacy. In the words of Institute of Policy Studies (IPS) 2022 survey, 68% of online users were uncomfortable with the manner in which companies harvest and use their data and noted that a lack of transparency was a concern (IPS, 2022). Furthermore, Perera & Silva's (2021) qualitative research further confirmed that Sri Lankan customers would limit their web usage or block access to some online services because of privacy concerns and have a direct impact on businesses using behavioral targeting.

Diffusion of behavioral targeting in digital marketing has created considerable consumer worry, particularly regarding the gathering, processing, and utilisation of personal information without apparent consent. Systematic review, in this instance, covering telecommunication and retail industries in Sri Lanka, illustrates growing consumer worry and the urgent need for openness and ethical treatment of data. In the telecommunication sector, for example, location data of customers, browsing patterns, and calling patterns are typically tracked by service providers in order to tailor promotion offers. It can add relevance, but consumers feel such behavior as intrusive if they do not know that they are being monitored or where consent is bundled with lengthy, un-understandable terms and conditions. Similarly, in retail, Daraz and Keells Online utilize cookies and tracking pixels to recommend items and send targeted marketing based on past search history. Convenient as that may be, that kind of targeting has provoked users for being "constantly watched" or feeling manipulated.

Consumer discontent is also amplified when information gathering seems excessive or not relevant to the service being provided. An example would be a request for access to a customer's contacts or microphone in a store app, without explicit reason, and this provokes resistance and suspicion. Of course, consumers would anticipate a fair balance between information collected and services rendered toward the data minimization principle under global privacy regulations such as the GDPR, which although not directly binding in Sri Lanka, serve as aspirational standards. Many Sri Lankan consumers, particularly digitally savvy young people, are becoming more prudent by clearing browser data continuously, blocking cookies, or using VPNs and advertisement blockers. On the contrary, the elderly, though less technologically competent, complain of being bombarded by repeated and irrelevant adverts, which indicate the failure of personalization to make a positive impact on user experience.

In order to address these issues, companies should have open data policies and data privacy-by-design. An effective way would be to apply plain, opt-in consent mechanisms with clear explanations of how the data is utilized using icons, bullet points, or short videos rather than long blocks of legal text. For example, telecommunication providers like Dialog or Mobitel might have a privacy center in their apps where users are provided with the option to control what information they share and why. Retailers can also

have "data preference centers" where consumers can reset personalization options or completely block tracking. They can also conduct consumer education on how data gets used and is being protected to build trust. Firms should also conduct privacy audits from time to time and demonstrate conformity with third-party certification or national regulatory approval.

In short, as privacy becomes increasingly a consumer concern in Sri Lanka, behavioral targeting initiatives must evolve to be responsive to consent, transparency, and control. Respectful businesses not only comply with emerging ethical norms but also establish competitive advantage through sustained customer loyalty. Therefore, balancing personalization and privacy is no longer optional but a strategic necessity.

2.4 Data Protection and Consumer Rights on Regulatory Environment in Sri Lanka

The government of Sri Lanka introduced the Personal Data Protection Act (2022) to safeguard consumer privacy of personal data. The Act requires consent in data collection, implements a principle of transparency in data use, and prescribes penalties in case of non-compliance (Wijayaratne, 2023). This regulatory landscape is supported by global standards such as the EU's GDPR, which pushes Sri Lankan businesses in telecommunications and retailing to improve privacy compliance. Dialog, Mobitel, and major retailers have revised privacy policies and altered consent models accordingly.

The regulation of data protection and consumer rights within Sri Lanka is still in its infancy and poses daunting challenges to ethical online marketing, most especially among the telecommunications and retail industry where the application of behavioral targeting is increasingly common. Even after the Personal Data Protection Act (PDPA) was prepared in 2021 according to international standards such as the EU's GDPR, enforcement remains infantile with the full implication and organizational readiness merely expected in 2025. This delay gives window space for the misuse of personal data. For instance, major telecom operators like Dialog Axiata and Mobitel embrace selective SMS and app-based promotion based on customer browsing history and usage patterns, which is usually not with explicit or informed consent. Similarly, major retail chains like Keells and Cargills follow loyalty card and digital receipt-based tracking of customers' purchasing habits and push customers push-based promotions of customized offers through mobile applications but with usually vague privacy notices which do not allow for opt-in or opt-out. A study conducted by LIRNE asia in 2023 ascertained that 61% of Sri Lankan customers do not know how their data is being used digitally, and 72% have never once gone through a privacy policy prior to using a digital service. This reflects a critical level of unawareness, which with poor enforcement, further aggravates concerns about privacy. Though regulatory bodies like the Telecommunications Regulatory Commission of Sri Lanka (TRCSL) and Consumer Affairs Authority (CAA) exist, they lack specific expertise to audit algorithmic decision-making or monitor data brokerage activities that feed behavioral targeting systems.

Solutions to these issues involve several steps. First, there must be speedy enforcement of the PDPA, such as the appointment of a Data Protection Authority with the authority to impose fines, conduct audits, and demand transparency in data usage. Second, companies must be required to adhere to clear, intuitive consent processes and provide data access and deletion rights to customers. For example, a mobile app must allow people to have control over what data are collected and why. Third, national digital literacy initiatives possibly through school education or community courses can enable citizens to make informed choices. Fourth, public-private partnerships can be established to allow privacy-by-design on marketing platforms, where by default systems are designed with safeguards.

Overall, as much as the legal foundation of data protection in Sri Lanka remains under development, there is an urgent need to close the gap between policy and implementation. The unchecked growth of behavioral targeting in the digital economy, especially in high-data industries like telecom and retail, has the potential to erode consumer autonomy and trust. A more robust and effective regulatory regime, combined with industry responsibility and consumer education, is needed to ensure that the benefits of digital marketing are not bought at the cost of fundamental privacy rights.

2.5 Ethical and Strategic Issues on Finding a Balance between Behavioral Targeting and Privacy

Balancing effective marketing personalization with the protection of privacy is a critical task. Studies point out the importance of "privacy by design" where data protection is built into digital marketing infrastructure right from the beginning (Zhou et al., 2021). Transparent communication, consumer education, and opt-in strategies have proved to enhance consumer acceptance of behavioral targeting (Johnson & Tan, 2020). Companies in Sri Lanka applying these strategies have documented increased trust and marketing performance (Perera & Silva, 2021).

While there are marketing advantages in behavioral targeting, there is no Sri Lankan empirical research into consumer privacy opinions. Additional empirical investigations of consumer trust, the effectiveness of consent mechanisms, and cross-industry comparisons must be conducted. The impact of emerging technologies such as AI-driven marketing and data ethics on Sri Lankan privacy is also an area that needs more investigation (Wijayaratne, 2023).

For Sri Lanka's telecommunication and retail industries, finding a balance between consumer privacy and behavioral targeting is both an ethical requirement and a strategic necessity. Behavioral targeting enables companies to tailor ad messaging based on user data such as web pages browsed, purchase patterns, and geography, leading to improved campaign performance. For example, Dialog Axiata, the leading telecommunication company, uses customer data to offer personalized plans, and online shopping giants like ODEL use browsing and purchasing history to recommend products. These practices are ethically flawed when the information collection is not directly with the user's agreement or proper disclosure. Studies have indicated that over 60% of Sri Lankan consumers are privacy conscious while online, a reflection of the growing necessity for data protection. In order to address this, organisations must include clear opt-in consent provisions and anonymise personal data, reducing misuse risks. Strategically, adopting privacy-by-design principles is not only in line with Sri Lanka's emerging Personal Data Protection Act but also maintains customer trust that Nielsen finds fuels 73% of global consumer purchase behavior. Moreover, companies may enhance transparency by explicitly articulating their data policies every now and then and providing direct access to users to manage their preferences. Encouraging digital literacy campaigns can enable consumers with improved decision-making skills, further finding a balance

between marketing objectives and ethical responsibility. Lastly, embracing these strategies enables telecom and retail companies to leverage the power of behavioral targeting while not infringing on privacy, thereby building sustainable competitive advantages across Sri Lanka's digital economy.

3. Discussion

Literature reviews and industry reports in this case show that behavioral targeting is a powerful tool in Sri Lanka's telecommunications and retail sectors. Telecommunications firms like Dialog and Mobitel have successfully used behavioral data to personalize offerings, enhance customer loyalty, and enhance top-line growth. Retailers like Kapruka.com and ODEL have also used targeted internet advertising and personalized communication to drive conversions as well as repeat purchase.

These findings are in line with cross-border evidence that targeted advertising is more effective than generic promotion for both engagement and sales (Chen et al., 2020; Smith & Kumar, 2019). In the local Sri Lankan context, the relatively youthful digital economy provides a favorable terrain for behavior targeting to gain traction, especially with regards to increasing internet penetration and mobile phone usage.

However, the effectiveness of these actions is different. Success relies on data quality that is collected, the level of sophistication in data analytics, and the ability of marketers to create timely, relevant, and subtle communications. For instance, Dialog's SmartPlan system of personalization that was achieved by combining different sources of data to provide a sophisticated view of customer needs (Dialog Marketing Report, 2023). For retailers, systems that integrate browsing and purchase history with demographic data are more likely to make more persuasive recommendations, resulting in loyalty and loyalty length.

While behavioral targeting sustains marketing efficacy, it also imposes privacy concerns that can puncture consumer confidence and damage brand reputation. Rising consumer awareness and distrust of Sri Lankan consumers about data privacy follow global trends (IPS, 2022; Perera & Silva, 2021). The data breach of Dialog in 2022 and the accompanying disaffection among consumers demonstrate the actual threats of mishandling consumer data. Privacy mistakes in Sri Lanka, though not yet as frequent or vicious as in more developed digital economies, are disproportionately impactful due to lower baseline trust and limited consumer digital expertise.

Privacy problems come in many flavors; concern about data abuse, unwanted profiling, and loss of control over personal information. These fears have led to some consumers avoiding or restricting contact with web services, limiting reach and effectiveness of behavior-based targeting campaigns. Marketers are thus faced with a razor-thin balancing act: employing behavioral data to deliver personalized experience while maintaining consumer privacy to foster trust. Failure in either aspect will compromise marketing effectiveness as well as cause legal consequences under Sri Lanka's emerging data protection laws.

The passing of the Personal Data Protection Act (2022) is a gigantic leap for Sri Lanka to address issues of privacy. The legislation brings the country to world-best practice, emphasizing express consent, transparency, and accountability. For telecommunication and retail companies, compliance with this model involves going back to the drawing board to alter data gathering, storage, and processing behaviors. Companies like Dialog and major retail sites have updated privacy policies, implemented consent pop-ups, and strengthened data security measures. With compliance come operational burdens. Building consent management systems and promoting transparency take the form of technology and training investments. Sri Lankan businesses also have to contend with consumer education so that users know their rights and the benefits of data sharing for tailored services. Although the regulation can add costs and complexity to behavioral targeting, it promotes a more ethical marketing environment, potentially leading to increased consumer trust and brand loyalty.

In addition, the literature underlines that ethical online marketing must follow a "privacy by design" approach, embedding privacy protection across every stage of data collection and exploitation (Zhou et al., 2021). In Sri Lanka, where regulatory frameworks and digital literacy are in the process of development, it is important to go down this route. Transparency must be marketers' utmost concern; clearly saying what information is collected, for what, and consumers' rights. Opt-in consent models, clear privacy policies, and easy ways to manage preferences are a must.

In addition to educating consumers on the value exchange involved in targeting based on behavior, making acceptance larger is possible. For example, writing about how customized promotions provide shopping convenience can alleviate privacy issues. Marketing-wise, the marketers must avoid over targeting, which generates "creepy" or intrusive advertising experiences. A balance between personalization and respect for customers' boundaries earns goodwill. In Sri Lanka's case, the relatively lower awareness of data rights implies that marketers bear a heavier responsibility to be leaders in ethical practices and build trust among consumers. The future of behavioral targeting in Sri Lanka is promising but demanding. Increased adoption of AI and machine learning can enhance targeting precision but also raises new privacy and ethical concerns. For example, algorithmic profiling has the potential to reinforce unintended biases or make opaque decisions to which consumers will have no immediate redress. The rapid evolution of digital payments and internet retailing raises data streams, making robust safeguards essential to prevent misuse. Furthermore, Sri Lanka's ethnic mix and linguistic diversity also require culturally sensitive marketing and privacy communication. Another risk on the horizon is cross-border data flows. A number of Sri Lankan companies utilize foreign cloud hosts and marketing platforms, which complicates the issue of data jurisdiction and compliance. Researchers and experts must highlight empirical research that examines the effectiveness of privacy-assuring marketing approaches, consumer trust dynamics, and regulator influence in Sri Lanka.

4. Conclusions and Recommendations

This discussion has weighed the dual-edged nature of behavioral targeting in Sri Lanka's telco and retail sectors, its great potential for amplifying the efficiency of marketing with resulting privacy concerns. Behavioral targeting enables these industries to deliver meaningful, personalized content that enhances consumer engagement, loyalty, and ultimately, revenues. Large Sri Lankan telcos

and retailers have adopted sophisticated data-driven marketing practices that have become measurable improvements in customer acquisition and retention.

But these success stories are counterbalanced by increasing consumer anxiety and worry regarding data privacy. The lack of transparency, the risk of abuse, and some data breaches have gone against consumer trust. This decline in trust imperils not only individual companies but also the overall digital advertising ecosystem in Sri Lanka.

The recently enacted Personal Data Protection Act (2022) is a significant regulatory milestone, aligning Sri Lanka with global data privacy standards and imposing responsibilities on businesses to seek explicit consumer consent, be open, and secure personal data. Compliance comes with operational challenges, but also presents an opportunity for companies to build stronger, confidence-based customer relationships. Ethically performed marketing actions that involve privacy by design, coupled with open communication and consumer awareness, will be required to navigate this challenging landscape. Balancing personalization and safeguarding privacy will be essential to sustaining consumer engagement and marketing effectiveness in the future.

To effectively weigh the benefits of behavioral targeting in relation to the need for consumer protection of privacy, Sri Lankan companies operating in telecom and retail sectors should adopt a general policy of ethical and transparent methods of practice. Companies must first introduce privacy by design principles that create security protection of data within marketing frameworks from the initial stages through secure data handling, controlling access, and anonymization where possible. Transparency is also important; companies need to explain their data collection and use practices simply and clearly in a comprehensible way, using plain language and simple consent tools such as opt-in alerts and preference management tools. In addition, educating consumers on the value of personalized marketing as well as their data rights can foster trust and encourage active engagement. Marketers should also take caution not to over-target, causing discomfort or alienation, while being respectful of frequency limits and ensuring easy opt-out for consumers. Regular audits and compliance checks must be conducted to ensure the organizations adhere to the Personal Data Protection Act and do not commit breaches or risk penalties.

Regulation-wise, policymakers have to step up data protection legislation enforcement by providing sufficient resources for monitoring and enforcing compliance. Encouraging efforts to enhance digital literacy across the country will equip consumers with the information necessary to safeguard their privacy and make informed decisions online. Encouraging interindustry collaboration can enable the creation of standardized privacy guidelines and encourage the dissemination of best practices. Additionally, regulators should stay ahead of the curve in terms of emerging technologies such as AI-based marketing and transborder data transfers to adjust regulations as required.

Finally, more studies are needed to build upon the existing knowledge concerning privacy attitudes of Sri Lankan consumers and the effectiveness of privacy-protecting advertising techniques. Consumer trust empirical research, the impact of new technologies, and cross-industry differences will provide valuable insights to formulate and implement strategies and policies in a manner that successfully addresses the needs. Implementing these recommendations, Sri Lankan telecommunications and retail sectors can properly leverage behavioral targeting and address consumer privacy concerns at the same time, building a sustainable and trustworthy digital marketing environment.

References

- [1] Acquisti, A., Brandimarte, L. and Loewenstein, G., 2015. Privacy and human behavior in the age of information. *Science*, 347(6221), pp.509-514.
- [2] Ajzen, I., 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), pp.179-211.
- [3] Albrecht, J.P., 2016. How the GDPR will change the world. *European Data Protection Law Review*, 2(3), pp.287-289.
- [4] Bambauer, D.E., 2013. The privacy projects. *Minnesota Law Review*, 97, pp.1161-1218.
- [5] Bauer, C., Berger, B., and Göritz, A.S., 2013. How privacy concerns affect online purchasing behavior: An empirical investigation. *Electronic Commerce Research and Applications*, 12(5), pp.372-382.
- [6] Berendt, B., Günther, O. and Spiekermann, S., 2005. Privacy in e-commerce: Stated preferences vs. actual behavior. *Communications of the ACM*, 48(4), pp.101-106.
- [7] Bhatnagar, A., Misra, S. and Rao, H.R., 2000. On risk, convenience, and Internet shopping behavior. *Communications of the ACM*, 43(11), pp.98-105.
- [8] Chen, H., Chiang, R.H.L. and Storey, V.C., 2012. Business intelligence and analytics: From big data to big impact. *MIS Quarterly*, 36(4), pp.1165-1188.
- [9] Colombo, M.G. and Piva, E., 2012. Strengths and weaknesses of academic research in the field of digital marketing. *Journal of Business Research*, 65(7), pp.949-955.
- [10] Colombo, M., 2018. Behavioral targeting in online advertising: A review. *International Journal of Marketing Studies*, 10(1), pp.21-33.
- [11] Data Protection Commissioner of Sri Lanka, 2021. Annual report 2020. [online] Available at: <http://www.dataprotection.gov.lk> [Accessed 18 June 2025].
- [12] Deloitte, 2020. Consumer privacy in Sri Lanka: Understanding perceptions and behaviors. Deloitte Insights. [online] Available at: <https://www2.deloitte.com/lk/en/pages/consumer/privacy-survey.html> [Accessed 18 June 2025].
- [13] Dey, L., 2017. Digital marketing strategies in emerging economies: Sri Lanka's perspective. *Journal of Marketing Research & Case Studies*, 2017, pp.1-12.
- [14] European Commission, 2018. General Data Protection Regulation (GDPR). [online] Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [Accessed 18 June 2025].
- [15] Goldfarb, A. and Tucker, C., 2011. Privacy regulation and online advertising. *Management Science*, 57(1), pp.57-71.
- [16] Hann, I.H., Hui, K.L., Lee, T. and Png, I.P.L., 2007. Consumer privacy and marketing avoidance: A static model. *Management Science*, 53(2), pp.308-322.

- [17] Ho, S.Y., Lee, C., and Man, S., 2018. Impact of privacy concerns on consumer behavioral intention in e-commerce. *Journal of Retailing and Consumer Services*, 43, pp.128-135.
- [18] ICTA Sri Lanka, 2022. Digital transformation in Sri Lanka: Annual ICT report. [online] Available at: <https://www.icta.lk> [Accessed 18 June 2025].
- [19] Jones, K., 2020. Behavioral targeting and privacy in digital marketing: Ethical considerations and consumer trust. *Journal of Business Ethics*, 164(4), pp.657-670.
- [20] Kumar, V., 2018. Customer relationship management: Concept, strategy, and tools. Springer.
- [21] Lwin, M.O., Wirtz, J. and Williams, J.D., 2007. Consumer online privacy concerns and responses: A power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, 35(4), pp.572-585.
- [22] Madanayake, A., 2019. Consumer privacy concerns and online purchasing behavior: Evidence from Sri Lanka. *Sri Lanka Journal of Marketing*, 5(2), pp.45-60.
- [23] Mathieson, K. and Tan, F.B., 2013. Privacy and trust in e-commerce: The role of security and privacy policy. *Electronic Markets*, 23(4), pp.349-360.
- [24] Mehta, S.C., 2014. Ethical implications of behavioral targeting in digital advertising. *International Journal of Business Ethics*, 24(1), pp.89-104.
- [25] Ministry of Digital Infrastructure and Information Technology, Sri Lanka, 2021. National digital policy framework. [online] Available at: <https://mdiit.gov.lk> [Accessed 18 June 2025].
- [26] Nisar, T.M. and Prabhakar, G., 2017. What factors determine mobile advertising adoption? An application of the theory of consumption values. *Journal of Retailing and Consumer Services*, 34, pp.20-29.
- [27] OECD, 2013. Consumer privacy protection in the digital age: Economic analysis and policy implications. *OECD Digital Economy Papers*, No. 220.
- [28] Perera, L., 2020. Data protection challenges in Sri Lanka's retail sector. *Journal of Information Security*, 11(3), pp.135-146.
- [29] Ponemon Institute, 2018. Cost of data breaches study: Global overview. [online] Available at: <https://www.ponemon.org> [Accessed 18 June 2025].
- [30] Wijesinghe, K., 2019. The influence of privacy concerns on consumer attitudes toward digital marketing in Sri Lanka. *International Journal of Business and Management Invention*, 8(1), pp.01-10.